UNIVERSITÀ DEGLI STUDI DI TRENTO
FACOLTÀ DI GIURISPRUDENZA
Dottorato in Studi Giuridici
Comparati ed Europei

Corso di Dottorato in Studi Giuridici Comparati ed Europei

XXVI ciclo

Tesi di Dottorato

Prova informatica e diritti fondamentali della persona nel processo penale

Relatore *Dottoranda*

Prof. Renzo Orlandi *Federica Iovene*

anno accademico 2012-2013

UNIVERSITÀ DEGLI STUDI DI TRENTO
FACOLTÀ DI GIURISPRUDENZA
Dottorato in Studi Giuridici
Comparati ed Europei

Candidata: Federica Iovene

PROVA INFORMATICA E DIRITTI FONDAMENTALI DELLA PERSONA NEL PROCESSO PENALE

Relatore Prof. Renzo Orlandi

Anno Accademico 2012-2013

Indirizzo specialistico in Diritto e procedura penale e filosofia del diritto

XXVI ciclo

Esame finale: 06/03/2014

Commissione esaminatrice:

Prof. Mauro Catenacci, Università degli Studi Roma Tre
Prof. Daniele Negri, Università degli Studi di Ferrara
Prof. Antonia Menghini, Università degli Studi di Trento

Ai miei genitori

RINGRAZIAMENTI

Un sentito ringraziamento al Professor Renzo Orlandi, per avermi guidata in questo percorso. Al Professor Marcello Busetto e alla Dottoressa Gabriella Di Paolo che mi hanno sostenuta durante l'esperienza trentina.
Al Professor Michael Corrado per l'esperienza alla University of North Carolina.
Al Max Planck Institut di Freiburg.

Alla mia famiglia, per esserci sempre.

Grazie all'Aula Dottorandi, a "Berlino Est" e "Berlino Ovest", e ai suoi occupanti, legittimi e…abusivi! Alla mia "classe": Daria, Carlos, Betty, Rossana, Alvise e Ilaria, il mio punto di contatto 24/7. A Magì, la mia Louise. A Marta, per la pazienza. A Roberto, per i preziosi consigli.

Agli amici di sempre, e a quelli che ci sono sempre.

Naturalmente, non era possibile sapere se e quando si era sotto osservazione. Con quale frequenza, o con quali sistemi, la Psicopolizia si inserisse sui cavi dei singoli apparecchi era oggetto di congettura. Si poteva persino presumere che osservasse tutti continuamente. Comunque fosse, si poteva collegare al vostro apparecchio quando voleva. Dovevate vivere (e di fatto vivevate, in virtù di quella abitudine che diventa istinto) presupponendo che qualsiasi rumore da voi prodotto venisse ascoltato e qualsiasi movimento - che non fosse fatto al buio - attentamente scrutato.

G. Orwell, 1984

INDICE

CAPITOLO II

MEZZI DI RICERCA DELLA PROVA TIPICI E NUOVE TECNOLOGIE INFORMATICHE

ABSTRACT

La tesi si propone di approfondire il tema dell'incidenza che le innovazioni in campo tecnologico e informatico hanno sui mezzi di ricerca della prova.

Preliminare all'esame della disciplina positiva è una riflessione sui diritti fondamentali – costituzionali e convenzionali (CEDU e CDFUE) - che le indagini informatiche sono suscettibili di comprimere e limitare. A tal fine vengono esaminati innanzitutto i "classici" diritti fondamentali alla libertà personale, all'inviolabilità del domicilio, alla libertà e segretezza delle comunicazioni e alla libertà di circolazione, inoltre diritti di "nuova generazione", come i diritti di *privacy* - riservatezza e tutela dei dati personali -. Infine, prendendo spunto dall'esperienza comparata, e in particolare dalla giurisprudenza costituzionale tedesca, si vaglia l'opportunità di creare nuovi diritti fondamentali, in grado di tutelare la persona di fronte alle sfide poste dal progresso tecnologico.

Una volta delineata la cornice costituzionale di riferimento, vengono presi in considerazione i mezzi di ricerca della prova informatici tipici, così come disciplinati a seguito della ratifica della Convenzione *Cybercrime* e vengono messe in luce le carenze dell'intervento legislativo che lasciano aperte alcune questioni fondamentali: la natura giuridica dell'attività di clonazione dell'*hard disk*, cui è strettamente collegato il problema dell'attuazione del contraddittorio con la difesa, le conseguenze derivanti dall'inosservanza delle *best practices* nel condurre le indagini informatiche, la persistenza dell'interesse al riesame del decreto di sequestro di *computer*, restituito dopo la clonazione dell'*hard disk*, il rischio di perquisizioni esplorative, che muovono alla ricerca della *notitia criminis*. Per quanto riguarda quest'ultimo aspetto, si suggerisce una possibile soluzione, che prende spunto dalla ricerca comparata, ed in particolare dal sistema statunitense. Vengono poi esaminate altre questioni lasciate irrisolte dal legislatore, quali la captazione di comunicazioni vocali effettuate con sistemi *VoIP* e l'apprensione in tempo reale della posta elettronica. Infine, viene approfondita la complessa tematica della conservazione dei dati di traffico telefonico e telematico – c.d. *data retention*.

Sul versante delle indagini informatiche non disciplinate dalla legge – pedinamento satellitare e c.d. perquisizioni *online* – il quesito centrale cui si è cercato di dare risposta è se, allo stato, si tratti di prova atipica oppure piuttosto di prova incostituzionale, propendendo per quest'ultima conclusione.

Da ultimo si sono presi in considerazione i delicati profili di cooperazione giudiziaria, con particolare attenzione alla tutela dei diritti fondamentali della persona. Una cooperazione giudiziaria in materia di acquisizione probatoria che sia rispettosa dei diritti fondamentali dei soggetti coinvolti e che porti a risultati utilizzabili e ammissibili in giudizio presuppone, infatti, l'esistenza di *standards* investigativi comuni. Con l'entrata in vigore del Trattato di Lisbona, l'Unione europea possiede gli strumenti per dettare disposizioni comuni agli Stati membri in materia di acquisizione probatoria (art. 82 TFUE). A tal fine, riteniamo che la giurisprudenza della Corte di Strasburgo relativa in particolare all'art. 8 CEDU possa costituire una buona base giuridica da cui prendere le mosse.

INTRODUZIONE

1. Il complesso rapporto tra accertamento penale e nuove tecnologie informatiche

L'avvento di *Internet* e delle nuove tecnologie informatiche ha determinato una rivoluzione copernicana dei sistemi di comunicazione e delle relazioni interpersonali.[1] *Computer*, *tablets*, *smartphones* sono al giorno d'oggi i mezzi più usati per comunicare, in quanto, mettendo a disposizione strumenti diversi quali *e-mail*, *sms*, *chat*, *VoIP*, sono in grado di soddisfare le più diverse esigenze dell'utente. I dispositivi informatici sono diventati a tal punto essenziali per lo svolgimento di attività lavorative e ricreative, di natura personale o sociale, da costituire una sorta di «"corpo elettronico" che ciascuno di noi possiede e che lascia tracce ovunque»[2].

Evidenti sono i riflessi sul piano del diritto e dell'accertamento penale: da un lato, infatti, ci si avvale di strumenti informatici nella commissione di reati, dall'altro, le potenti memorie dei *computers* costituiscono altrettanti archivi di informazioni, di cui autorità giudiziaria e di polizia possono ormai raramente fare a meno per l'accertamento di qualsiasi reato. Le c.d. indagini informatiche, infatti hanno carattere trasversale, non riguardano solo i delitti che abbiano ad oggetto, o la cui commissione avvenga per mezzo di, sistemi informatici o dati informatici (c.d. reati informatici in senso stretto e in senso ampio)[3], ben potendo i dati digitali essere rilevanti per l'accertamento di illeciti privi di una dimensione tecnologica, come l'omicidio o la violenza sessuale[4].

Al tempo stesso occorre riconoscere la peculiarità della realtà digitale come oggetto di indagine. La natura ontologicamente volatile e alterabile dei dati digitali fa

---

[1] Secondo J. RUX*, Ausforschung privater Rechner durch die Polizei-und Sicherheitsbehörden - Rechtsfragen der "Online-Durchsuchung"*, in *JZ*, 2007*,* p. 285 ss. «dall'invenzione della ferrovia nessun'altra rivoluzione tecnologica ha prodotto un cambiamento così rapido e radicale nei comportamenti umani come *Internet* e la tecnologia».

[2] P. G. MONATERI, *Diritti senza tempo né spazio*, Sole24ore, 23 dicembre 2012, p. 33.

[3] Si vedano L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, p. 86 ss.; C. SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale*, 3ª ed., Milano, 2010, p. 61 ss.

[4] Si pensi a titolo esemplificativo al caso di Garlasco, dove la prova d'alibi si basava essenzialmente sull'utilizzo del *computer* in una fascia oraria, oppure al c.d. stupro della Caffarella, in cui i due rumeni inizialmente arrestati sono stati liberati perché scagionati dal test del *DNA* e dalla mappatura del traffico telefonico.

sorgere delicate questioni circa la loro acquisizione, conservazione e presentazione in sede processuale. I dati digitali sono immateriali, si risolvono in *informazioni* espresse in codice binario (c.d. *bit*, sequenze di 0 e 1), ma per essere fruibili e intellegibili hanno bisogno di un supporto fisico, di una *res* in cui essere incorporati. Essi sono, tuttavia, indipendenti e scindibili dal supporto informatico che li contiene, possono essere duplicati un'infinità di volte su supporti diversi e rimangono sempre uguali a se stessi[5]. Non va trascurato però che lo stato del dispositivo su cui i dati sono registrati può, anche inavvertitamente, essere modificato da colui che l'ha formato o da altre persone, con alterazione o perdita dei dati stessi.

Fondamentale, quindi, affinché l'accertamento possa dirsi attendibile è garantirne la genuinità, adottando particolari cautele nella ricerca, raccolta e analisi dell'evidenza elettronica. Ciò richiede l'adozione di specifici strumenti di *computer forensics* e pone il problema di come bilanciare il contributo degli esperti con l'attività del giudice[6].

Le innovazioni in campo informatico hanno altresì permesso di sviluppare nuove tecniche d'indagine: si tratta da un lato della possibilità di svolgere indagini tradizionali con l'ausilio di nuovi strumenti tecnologici – è il caso ad esempio del

[5] Molto opportunamente, la legge di ratifica della Convenzione di Budapest ha abrogato l'art. 491 *bis* c.p. che considerava documento informatico «qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli». Accoglie positivamente tale scelta del legislatore L. PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, p. 701 ss., il quale ritiene la definizione dell'art. 491 *bis* c.p. inadeguata all'evoluzione tecnologica e in particolare alla c.d. "immaterialità" dei dati digitali, in quanto incentrata sul supporto contenente i dati. Attualmente, l'unica definizione legislativa di documento informatico è contenuta nell'art. 1 del Codice dell'amministrazione digitale (d.lgs. 82/2005), dove esso è descritto come «la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti» (lett. p). Tuttavia, c'è chi dubita che la definizione contenuta nel Codice dell'amministrazione digitale e gli altri requisiti strutturali richiesti per garantire stabilità e identificabilità del documento informatico siano vincolanti nell'ordinamento processuale penale, dove è lo stesso art. 324 c.p.p. a fissare la nozione di documento processualmente rilevante e le relative condizioni di utilizzo. Cfr. P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, p. 401 ss.; F. ZACCHÉ, *La prova documentale,* Milano, 2012, p. 36. Questa impostazione può essere fuorviante; infatti, se è vero che l'art. 324 c.p.p., per il richiamo in esso contenuto a «qualsiasi altro mezzo», è una norma a struttura aperta, idonea a ricomprendere anche i documenti informatici (ciò è sostenuto, tra gli altri, anche da F. CORDERO, sub *art. 234*, in *Codice di procedura penale commentato*, 2ª ed., Torino, 1992), bisogna fare attenzione a non confondere il contenuto con il contenitore: i dati digitali non sono prove documentali e non seguono le regole di ammissione per questi dettate dagli artt. 495, co. 3 e 515 c.p.p., valgono per essi, in considerazione della loro natura volatile e modificabile, regole di raccolta e utilizzo dibattimentale diverse.

[6] Sulla necessità di ripensare tutte le comuni regole probatorie, originariamente concepite per le prove tradizionali, si veda O. S. KERR, *Digital Evidence and the New Criminal Procedure*, in *105 Colum. L. Rev.*, 2005, p. 290 ss. Cfr. anche U. SIEBER, *Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag*, München, 2012.

pedinamento satellitare –; dall'altro di inediti mezzi di ricerca della prova, come l'infiltrazione in un sistema informatico ai fini dell'installazione di un particolare *software* di indagine che permette agli investigatori di esplorare il contenuto di un *computer* e monitorarne l'uso da parte dell'utente, ogni qualvolta questi si connetta ad *Internet* – c.d. perquisizione *online* -. In entrambi i casi, si pongono delicati problemi di bilanciamento tra le esigenze di indagine penale e tutela dei diritti fondamentali: la libertà personale (art. 13 Cost.), l'inviolabilità del domicilio (art. 14 Cost.), la libertà e segretezza delle comunicazioni (art. 15 Cost.), la libertà di circolazione (art. 16 Cost.), il diritto al rispetto della vita privata e familiare (art. 8 CEDU, art. 7 Carta dei Diritti Fondamentali dell'Unione Europea – di seguito CDFUE), il diritto alla protezione dei dati a carattere personale (art. 8 CDFUE).

Non solo, ma le innovazioni tecnologiche sono in grado di minare le fondamenta dei classici diritti costituzionali, tanto che in ordinamenti non distanti dal nostro si è avvertita l'esigenza di coniare nuovi diritti della personalità, in grado di fronteggiare e arginare l'invasività di strumenti d'indagine che si avvalgono delle nuove tecnologie. Si fa riferimento alla creazione da parte della Corte costituzionale tedesca (*Bundesverfassungsgericht*, di seguito *BVerfG*) dell'*informationelle Selbstbestimmungsrecht* – il diritto all'autodeterminazione informativa[7] - e del *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, ossi il diritto alla "garanzia della segretezza e integrità dei sistemi informatici"[8].

Ciò impone di aggiornare la nozione di riservatezza, cui non sembra più possibile negare il rango di diritto fondamentale (art. 2 Cost., artt. 8 CEDU e 117 Cost.), per offrire protezione a quello che appare essere un unico oggetto di tutela: «la persona nelle sue diverse considerazioni, via via determinate dal suo rapporto con le tecnologie, che non sono solo quelle elettroniche»[9]. Caratteristica tipica della prova digitale è la sua promiscuità: dati rilevanti per le indagini sono spesso mescolati a dati di carattere personale, irrilevanti per le indagini. Le indagini

[7] *BVerfG*, 15 dicembre 1983, in *BVerfGE* 65, 1 ss.
[8] *BVerfG*, 27 febbraio 2008, in *BVerfGE* 120, 274 ss.
[9] S. RODOTÀ, *Il diritto di avere diritti*, Roma, 2012, p. 317.

informatiche sono quindi sempre potenzialmente in grado di pregiudicare la riservatezza degli individui[10].

Infine, va considerato un ulteriore aspetto problematico: lo spazio informatico è globale e refrattario a limitazioni nazionali. I dati digitali sono spesso salvati su *servers* o *personal computers* dislocati in Paesi diversi da quello in cui le indagini vengono svolte[11]. Si pongono al riguardo problemi seri di cooperazione giudiziaria, soprattutto in considerazione del forte rischio che ogni Stato svolga investigazioni informatiche anche oltre i confini della propria sovranità, fino a dove la tecnologia lo consenta, dando vita a quello che è stato efficacemente descritto come «un "*far-west* tecnologico", in cui il diritto soccombe alla tecnologia»[12].

Compito del diritto è quindi quello di aggiornare, attraverso l'evoluzione normativa e giurisprudenziale, le tradizionali categorie concettuali in modo da non lasciare i singoli sprovvisti di tutela.

Il presente lavoro prenderà le mosse dall'analisi dei diritti fondamentali della persona suscettibili di essere limitati dalle indagini informatiche, al fine di metterne in evidenza i connotati essenziali e indefettibili che devono ritenersi esclusi da un'opera di bilanciamento con esigenze altrettanto rilevanti, quali quelle d'indagine in vista della repressione (e in ipotesi anche della prevenzione) di reati (capitolo I). Alla luce di questi primi risultati, verranno quindi esaminate le diverse misure investigative che sfruttano la tecnologia informatica, distinguendo tra mezzi di ricerca della prova tipici (capitolo II) e indagini informatiche non disciplinate dalla legge (capitolo III). Infine, si prenderanno in considerazione i profili di cooperazione giudiziaria (capitolo IV).

[10] F. RUGGIERI, *Profili processuali nelle investigazioni informatiche*, in L. PICOTTI (a cura di), *Il diritto penale*, cit., p.158 ss.
[11] Sempre più diffuso è l'utilizzo di servizi di *cloud computing*, in cui i dati sono salvati in una "nuvola", e non su un supporto fisico.
[12] L'espressione è ripresa da M. PANZAVOLTA, *Intercettazioni e spazio di libertà, sicurezza e giustizia*, in F. RUGGIERI, L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, p. 69.

2. Chiarimento sulla nozione di prova informatica ai fini del presente studio

Come si è già avuto modo di accennare, il processo di informatizzazione e digitalizzazione che sta interessando la società moderna ha inevitabili e significativi riflessi anche sul terreno dell'accertamento penale, al punto che si è preconizzato un mutamento «della stessa essenza epistemologica del giudizio penale»[13]. Informatica e processo penale interagiscono a diversi livelli. Rimanendo in ambito probatorio, il materiale informatico può venire innanzitutto in rilievo come oggetto di indagine – è il caso ad esempio di ispezioni e perquisizioni di sistemi informatici o telematici -; inoltre, le nuove tecnologie sono sfruttate come strumento di indagine – si pensi all'utilizzo della tecnica della *bit stream image* per clonare e quindi sequestrare la memoria di un *computer* – o come mezzo dell'operazione probatoria – per esempio nell'ipotesi dell'esame a distanza -; infine, lo strumento informatico può servire a ricostruire dinamiche fattuali – si pensi alle simulazioni di disastri aerei, incidenti automobilistici – o semplicemente a documentare l'attività d'indagine.

Si rende pertanto necessaria qualche distinzione preliminare ai fini della individuazione della nozione di prova informatica oggetto del presente lavoro, soprattutto in considerazione del rischio di ipertrofia cui essa è esposta.

Già i concetti di "*electronic evidence*" e "*digital evidence*", spesso usati come sinonimi, non sono in realtà perfettamente sovrapponibili. Infatti, la *digital evidence* è un sottosistema della *electronic evidence*, la quale si presta a ricomprendere oltre ai dati in formato digitale anche quelli in formato analogico (come quelli contenuti in audio e video cassette o su una pellicola fotografica) i quali possono essere digitalizzati, ma non nascono in formato digitale[14].

---

[13] Così L. LUPARIA, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007, p. 134, il quale si richiama a G. ALESSI, *Il processo penale. Profilo storico*, Roma-Bari, 2001, p. 180, che fa un interessante parallelismo tra la "rivoluzione" prodotta dalla nascita dell'inchiesta medioevale e quella che si determinerà con la diffusa applicazione delle tecniche informatiche all'accertamento del reato. V. anche R. ORLANDI, *Questioni attuali in tema di processo penale ed informatica*, in *Riv. dir. proc.*, 2009, p. 129.

[14] Tale distinzione è ben colta da S. MASON, *Electronic Evidence: Disclosure, Discovery and Admissibility*, Londra, 2007, p. 22 ss. che adotta la seguente definizione di "*electronic evidence*": «*data (comprising the out put of analogous device or data in digital format) that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the process of adjudication*». Per quanto riguarda la definizione di "*digital evidence*", essa si identifica secondo E. CASEY, *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet*, *2° ed.*, Elsevier, 2004, p. 14, in «*any data stored*

Si può in via di prima approssimazione definire la prova informatica come quella consistente in informazioni in formato digitale, contenute in dispositivi informatici o circolanti nella rete[15]. Ciò tuttavia ancora non è sufficiente. Infatti, occorre ulteriormente distinguere tra *computer-derived evidence* ed "*electronic evidence* a genesi procedimentale"[16]. La prima fa riferimento ai casi in cui l'elaboratore o la rete costituiscono l'oggetto dell'attività probatoria; la seconda comprende le ipotesi in cui l'apparecchiatura informatica è lo *strumento di redazione* e/o *conservazione* di atti processuali oppure il *mezzo* dell'operazione probatoria, o ancora divenga il *soggetto* dell'attività probatoria. Ciò che accomuna tali variegate ipotesi è per l'appunto il fatto che i dati digitali siano generati nel corso del procedimento dagli *electronic devices* in dotazione degli organi inquirenti e altri soggetti processuali (e loro ausiliari) per lo svolgimento delle proprie funzioni[17].

La *computer-derived evidence*, invece, si caratterizza per avere ad oggetto dati digitali a genesi extra-procedimentale, i quali possono essere precostituiti ed acquisiti *ex post*, come quelli salvati nell'*hard disk* del *computer* o in altro dispositivo di memoria, o i dati di traffico telematico che i fornitori di servizi di telecomunicazione sono tenuti a conservare per dodici mesi, oppure circolare nella rete ed essere captati in tempo reale, come i flussi informatici. Quest'ultima è la nozione di prova informatica adottata nel presente lavoro.

Tenendo ferma la distinzione tra modalità statiche e modalità dinamiche di apprensione dei dati digitali, verranno esaminati mezzi di ricerca della prova che insistono su dati precostituiti (ispezione, perquisizione, sequestro di sistemi informatici o telematici, conservazione e acquisizione di dati di traffico telematico) e

---

or transmitted using a computer that support or refuse a theory of how an offence occurs or that address critical elements of the offence such as intent or alibi». V. anche G. VACIAGO, Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, 2012, p. 1 ss., per un quadro delle diverse definizioni di *electronic evidence* e *digital evidence*.

[15] G. DI PAOLO, (voce) *Prova informatica (diritto processuale penale)*, in *Enc. dir.,* Annali VI*,* Milano, 2013, p. 736 ss., in particolare, p. 739.

[16] Tradizionalmente, e secondo il paradigma di matrice anglosassone, si distingue tra *computer-derived evidence* e *computer-generated evidence*. La definizione "*electronic evidence* a genesi procedimentale" è ripresa da G. DI PAOLO, (voce) *Prova informatica*, cit., p. 740, la quale fa rientrare in tale categoria oltre alla *computer-generated evidence* – ossia i casi in cui gli strumenti informatici (*computer*, schermi, telecamere, proiettori, connessioni *Internet*) siano installati nelle aule di giustizia per consentire la redazione di atti processuali, la realizzazione di videoconferenze, la presentazione delle prove, *etc.* – anche gli strumenti che fanno capo alla *electronic surveillance*, ossia quelli a disposizione degli inquirenti nella fase investigativa, come le video riprese.

[17] *Ibidem*, p. 740.

strumenti di indagine che consentono la captazione in tempo reale del flusso di dati scambiato tra sistemi informatici e telematici (intercettazioni di comunicazioni telematiche, localizzazione tecnologicamente assistita). Menzione a parte merita l'accesso ad un sistema informatico che avviene tramite installazione, in locale o in remoto, di uno specifico *software* di *computer forensics*. Tale strumento di indagine, generalmente denominato "perquisizione *online*" – dal tedesco *Online Durchsuchung* [18] – particolarmente invasivo della sfera privata dell'individuo, permette sia di acquisire dati già salvati sul *computer* oggetto di indagine (documenti, immagini, video), sia di acquisire dati in tempo reale (captazione di comunicazioni che avvengano via *Skype*, o di *e-mail* non scaricate sul *computer*).

Esulano invece dal presente studio, in quanto appartenenti alla categoria della "*electronic evidence* a genesi procedimentale" innanzitutto le ipotesi in cui lo strumento informatico è utilizzato per documentare l'attività d'udienza (redazione del verbale mediante *computer*) o l'espletamento di un atto del procedimento (assunzione di una testimonianza o di un interrogatorio). Si tratta infatti, di raffigurare in formato digitale una realtà storica che non ha natura digitale; i dati informatici sono in questo caso generati dagli apparecchi in dotazione dei soggetti processuali. In secondo luogo, i casi in cui la tecnologia informatica rappresenta la modalità di compimento di un atto di indagine che però non insiste su una realtà digitale (intercettazioni di comunicazioni *ex* art. 266 c.p.p., video-riprese investigative). Infine, le ipotesi in cui il sistema informatico sia il mezzo dell'operazione probatoria, ossia lo strumento attraverso cui raccogliere dichiarazioni procedimentali (esame a distanza) oppure il *soggetto* dell'operazione dimostrativa[19] (utilizzo di *computer* e *software* per la ricostruzione e/o simulazione della dinamica fattuale).

[18] Il *Land Nordrhein Westfalen* ha per primo introdotto tale strumento investigativo nella Legge sulla protezione della Costituzione del *Land*, oggetto della sentenza del *Bundesverfassungsgericht* del 27 febbraio 2008 che ne ha dichiarato l'illegittimità costituzionale, previa creazione del *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. *Infra*, capitolo I, par. 5.1 e capitolo III, par. 4.1.

[19] Tale definizione è ripresa da L. LUPARIA, *Processo penale*, p. 145.

CAPITOLO I
PROVA INFORMATICA E DIRITTI FONDAMENTALI DELLA PERSONA

SOMMARIO: *1. La libertà personale e le sue manifestazioni 1.1 Il diritto all'inviolabilità del domicilio (art. 14 Cost.) 1.2 Libertà e segretezza delle comunicazioni (art. 15 Cost.) 1.3 Libertà di circolazione (art. 16 Cost.) 2.* Privacy *e riservatezza. Alcune distinzioni preliminari 2.1 Fonte del diritto alla riservatezza 3. Il diritto alla vita privata nella Convenzione Europea dei Diritti dell'Uomo e delle Libertà Fondamentali 3.1 Valore della CEDU nell'ordinamento interno 4. Diritto alla vita privata e alla tutela dei dati personali nella Carta dei Diritti Fondamentali dell'Unione Europea 5. Verso la creazione di nuovi diritti* 5.1 *L'esperienza tedesca: dall'*informationellen Selbstbestimmungsrecht *al* Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme *5.2 Le nuove dimensioni della* privacy *nell'ordinamento italiano: verso la creazione di nuovi diritti fondamentali?*

1. La libertà personale e le sue manifestazioni

«*Attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito*»[20].

Alla luce di tale insegnamento della Corte costituzionale, è opportuno affrontare il tema della prova informatica muovendo dalla cornice costituzionale in cui si iscrivono le diverse attività di indagine.

Viene in rilievo innanzitutto il diritto alla libertà personale (art. 13 Cost.) che, assumendo una posizione prioritaria tra i diritti inviolabili dell'uomo, riconosciuti e garantiti dall'art. 2 Cost. a salvaguardia del pieno svolgimento della personalità di ciascuno, funge da «presupposto di tutti gli altri diritti di libertà, in quanto logicamente li precede e li condiziona a livello operativo, rendendone possibile la piena esplicazione»[21]. Per quanto interessa ai fini del presente lavoro, evidente è il

[20] C. cost., 6 aprile 1973, n. 34, in *Giur. cost.*, 1973, p. 316, con nota di V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*.
[21] V. GREVI, *Libertà personale dell'imputato e costituzione*, Milano, 1976, p. 1. Si veda anche il fondamentale studio di G. VASSALLI, *La libertà personale nel sistema delle libertà costituzionali*, in *Scritti giuridici in memoria di P. Calamandrei*, V, Padova, 1958, p. 355 ss.

legame innanzitutto con la libertà domiciliare (art. 14 Cost.) e la libertà e segretezza delle comunicazioni (art. 15 Cost.) che, anch'esse inviolabili, si pongono come ampliamento e precisazione del principio di libertà personale[22]. Inoltre, con la libertà di circolazione, cui parte della dottrina costituzionalistica addirittura nega autonomia rispetto al diritto tutelato dall'art. 13 Cost.[23].

I diritti di libertà garantiscono all'individuo indipendenza e capacità di autodeterminarsi nella vita di relazione, sottraendo al controllo e all'interferenza da parte di terzi determinati aspetti della vita privata[24]. Essi, tuttavia, non sono diritti assoluti, ma suscettibili di bilanciamento con altri diritti e valori costituzionalmente protetti. Eventuali limitazioni devono però rispettare le garanzie poste dalla Costituzione: riserva di legge, riserva di giurisdizione, obbligo di motivazione.

La libertà personale, nata come garanzia dell'*habeas corpus*, e quindi inizialmente concepita come assenza di coercizioni fisiche, viene poi interpretata dalla Corte costituzionale anche come libertà morale, a condizione che il provvedimento coercitivo provochi una "degradazione giuridica", ossia «*una menomazione o mortificazione della dignità o del prestigio della persona,* [tale] *da poter essere equiparata a quell'assoggettamento all'altrui potere in cui si concreta la violazione del principio dell'*habeas corpus»[25]. Su posizioni simili anche la

[22] P. BARILE, E. CHELI, voce *Corrispondenza (libertà di), Enc. dir.*, vol. X, Milano, 1962, p. 744. Tutte le libertà costituzionali si manifestano come conseguenza della tutela della libertà personale, ma la libertà di domicilio e quella di corrispondenza più di ogni altra «integrano e specificano la sfera normativa dell'art. 13 Cost.: l'una garantendo alla persona un certo àmbito spaziale, l'altra garantendo una delle forma più dirette di collegamento della persona con il mondo esterno». Si veda anche A. PACE, *Art. 15*, in A. BRANCA (a cura di), *Commentario alla costituzione*. *Rapporti civili*, Bologna, 1975, p. 80 ss., il quale dà atto dell'originaria intenzione del legislatore costituente di introdurre una disciplina unitaria dei tre aspetti «inviolabili» della persona umana. La successiva scelta di prevedere distinte norme sarebbe tuttavia ispirata a intenti garantistici: quanto alla libertà di domicilio, si possono così tutelare anche luoghi non destinati all'abitazione, quanto alla libertà di comunicazione, si esclude in tal modo che questo diritto possa subire limitazioni legittime da parte di autorità pubbliche diverse da quella giudiziaria.

[23] I rapporti tra art. 13 e art. 16 Cost. sono stati al centro di un acceso dibattito. Ci si è domandati, infatti, «se si tratti di situazioni giuridiche corrispondenti a facoltà o interessi realmente distinti o di due aspetti di un'unica libertà», così G. AMATO, *Art. 16*, in A. BRANCA (a cura di), *Commentario alla costituzione*. *Rapporti civili*, Bologna, 1975, p. 114 ss. *Infra*, par. 1.3.

[24] A. BALDASSARRE, *Diritti della persona e valori costituzionali*, Torino, 1997, p. 275 ss.

[25] C. cost., 31 maggio 1995, n. 210, in *Dir. pen. proc.*, 1996, p. 703 ss. Nella prima decisione in materia, sentenza 14 giugno 1956, n. 2, in *Giur. cost.*, 1956, p. 561, la Corte costituzionale ha accolto una nozione di libertà personale come libertà fisica, dichiarando incostituzionali, per violazione dell'art. 13 Cost., le norme del T.U. delle leggi di pubblica sicurezza che permettevano l'accompagnamento e la traduzione coattiva al comune di provenienza, senza autorizzazione o convalida da parte dell'autorità giudiziaria. Con una sentenza di poco successiva, n. 11 del 3 luglio 1956, in *Giur. cost.*, 1956, p. 612 ss., la Corte ammette che anche l'ammonizione, pur non

dottrina costituzionalistica: se quella più risalente interpretava la libertà personale come un potere di libera disposizione del proprio corpo, seppur nei limiti e con l'osservanza degli obblighi posti dall'ordinamento[26], quella successiva vi fa rientrare anche la libertà morale[27]. La libertà personale viene in particolare concepita come pretesa al libero sviluppo della persona umana, rispetto al quale la libertà fisica è strumentale. L'art. 13 Cost. sarebbe quindi «privo di un contenuto determinato, apparterrebbe al novero delle fattispecie c.d. a schema aperto o variabile, pur essendo in funzione di una costante: la persona umana»[28]. Nell'individuare il contenuto della libertà personale, pertanto, occorre fare continuo riferimento ai valori del sistema costituzionale nel suo complesso e, in particolare, «ai *Grundwerte* che informano talune libertà, cioè i valori della persona»[29]. La tutela della libertà personale acquisisce così quell'elasticità necessaria a garantire protezione all'individuo di fronte all'evoluzione della società e alla nascita di nuove forme di limitazione.

Simile interpretazione dell'art. 13 Cost. si rivela particolarmente appropriata in materia di prove atipiche che, ai sensi dell'art. 189 c.p.p., possono essere ammesse dal giudice solo se non pregiudichino la *libertà morale* della persona. Infatti, nel verificare se un mezzo di ricerca della prova non disciplinato dalla legge limiti o meno la libertà di autodeterminazione, occorre fare riferimento alla libertà personale nella sua più ampia accezione e nei suoi rapporti con altri principi costituzionali. Ciò soprattutto considerando che strumenti di indagine che sfruttano le innovazioni tecnologiche in campo scientifico e informatico possono dar vita a limitazioni della

---

comportando alcuna forma di coercizione fisica, restringa il diritto di libertà personale costituzionalmente garantito, poiché «*si risolve in una sorta di "degradazione giuridica" in cui taluni individui, appartenenti a categorie di persone che la legge presume socialmente pericolose, magari designati come tali dalla pubblica voce, vengono a trovarsi per effetto di una pronuncia della pubblica Autorità*». L'ambito di applicazione dell'art. 13 Cost. viene ulteriormente esteso con la sentenza n. 30 del 27 marzo 1962, in *Giur. cost.*, 1962, p. 240, con cui la Corte vi ricomprende anche la menomazione della libertà di autodeterminazione «*quando* [essa] *implichi un assoggettamento totale della persona all'altrui potere* […] *tale da poter essere equiparata all'arresto*».

[26] S. GALEOTTI, *La libertà personale*, Milano, 1953 p. 6; F. CARNELUTTI, *Principi del processo penale*, Napoli, 1960, p. 175 ss.

[27] A. BARBERA, *I principi costituzionali della libertà personale*, Milano, 1967, *passim*; P. BARILE, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, p. 111 ss.

[28] Così A. BARBERA, *I principi costituzionali*, cit., p. 196.

[29] *Ibidem*, p. 48.

libertà personale magari meno evidenti, ma comunque altrettanto insidiose rispetto alla privazione della libertà fisica[30].

1.1 Il diritto all'inviolabilità del domicilio (art. 14 Cost.)

Nel sistema delle libertà fondamentali, la libertà domiciliare si presenta strettamente collegata alla libertà personale e alla libertà di comunicazione[31]. Sotto il primo profilo, il domicilio viene in rilievo come proiezione spaziale della persona ossia come sfera di estrinsecazione della propria personalità. Sotto il secondo, come luogo nel quale è garantito il diritto alla riservatezza[32].

Oggetto di tutela non è quindi la proprietà o altro diritto reale, ma il rapporto persona-ambiente, ossia «la persona riflessa in una certa sfera spaziale volta a preservare il carattere intimo, domestico, o quanto meno privato di determinati comportamenti soggettivi»[33].

Tuttavia, come chiarito dalle Sezioni Unite della Cassazione, la libertà domiciliare non deve essere confusa con il diritto alla riservatezza[34]. Infatti, da un lato non tutti i luoghi in cui si manifesta la personalità dell'individuo rientrano nell'ambito di applicazione dell'art. 14 Cost., dall'altro, il particolare rapporto che si instaura tra persona e domicilio fa sì che esso venga tutelato anche se la persona è

[30] È questo ad esempio il caso del pedinamento satellitare che, permettendo di seguire costantemente gli spostamenti dell'individuo nello spazio, si traduce in una forma di controllo e quindi limitazione della libertà personale. Il tema sarà oggetto di specifica trattazione nel prosieguo del presente lavoro. Si veda *infra*, Capitolo III, par. 2 ss.

[31] La protezione costituzionale del domicilio risulta tuttavia più debole di quella degli altri diritti di libertà (libertà personale, libertà e segretezza delle comunicazioni). Infatti, l'art. 14 comma 2 Cost. ammette che leggi speciali consentano di eseguire accertamenti e ispezioni domiciliari anche per motivi di sanità e di incolumità pubblica o a fini economici e fiscali.

[32] La tutela del domicilio è inoltre strumentale all'esercizio di altre libertà costituzionali: riunione (art. 17 Cost.), associazione (art. 18 Cost.), culto (art. 19 Cost.), insegnamento (art. 33 Cost.), iniziativa economica (art. 41 Cost.), organizzazione politica e sindacale (artt. 49 e 39 Cost.) possono svolgersi all'interno dell'area tutelata dall'art. 14 Cost. P. BARILE, E. CHELI, voce *Domicilio (libertà di)*, in *Enc. dir.*, vol. XIII, Milano, 1964, p. 859 ss.

[33] *Ibidem*, p. 861. Si veda anche G. AMATO, *Art. 14*, in A. BRANCA (a cura di), *Commentario alla costituzione*. *Rapporti civili*, Bologna, 1975, p. 54 ss.; C. cost., 24 aprile 2002, n. 135, in *Giur. cost.*, 2002, p. 1062 ss., con osservazioni di F. CAPRIOLI, *Riprese visive nel domicilio e intercettazioni «per immagini»*; C. cost., 7 maggio 2008, n. 149, in Giur. cost., 2008, p. 1832 ss., con osservazioni di F. CAPRIOLI, *Nuovamente al vaglio della Corte costituzionale l'uso degli strumenti investigativi di ripresa visiva*.

[34] Cass., sez. un., 28 marzo 2006, Prisco, con nota di M. L. DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni Unite*, e di F. RUGGIERI, *Riprese visive e inammissibilità della prova*, in *Cass. pen.* 2006, p. 3937 ss.; e di A. CAMON, *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento ed alcuni dubbi nuovi*, in *Riv. it. dir. e proc. pen.* 2006, p. 1550 ss.

assente, cosa che non accade per altri luoghi riservati. Ciò che distingue il domicilio dai luoghi riservati è, per tale giurisprudenza, la *stabilità* della relazione tra la persona e il luogo, che fa ad esso acquistare autonomia rispetto alla persona che ne ha la titolarità. Tale differenza si ripercuote evidentemente in ambito processuale: le intromissioni nel domicilio devono rispettare, per espressa previsione costituzionale, le garanzie previste per la limitazione della libertà personale, mentre per quelle nei luoghi riservati, tutelati dall'art. 2 Cost. sarebbe sufficiente un provvedimento motivato del pubblico ministero.

Quale sia il significato da attribuire alla nozione costituzionale di domicilio è controverso sia in dottrina che in giurisprudenza. Ciò dipende dal fatto che nell'ordinamento vigente non esiste una nozione unitaria di domicilio, ma molteplici nozioni, ciascuna elaborata nell'ambito di un diverso settore normativo.

La questione centrale è se l'art. 14 Cost. rinvii alla nozione di domicilio elaborata nel diritto penale, oppure se ricomprenda una sfera di interessi più ampia di quella tutelata dalla norma penale[35].

Secondo un primo orientamento, l'art. 14 Cost. farebbe sì rinvio alla norma penale, ma non si tratterebbe di un rinvio formale ad una fonte extra-costituzionale, ma di un rinvio recettizio, o presupposizione. Pertanto, oggetto di tutela sarebbero l'abitazione, i luoghi di privata dimora e le loro pertinenze (art. 614 c.p.). Conferma di tale impostazione si troverebbe nel fatto che la tutela costituzionale, identificandosi nell'esistenza di un collegamento necessario e indefettibile tra domicilio e persona, viene a coincidere con la *ratio* ispiratrice della tutela penale, che correttamente colloca il delitto di violazione di domicilio tra i delitti contro la libertà individuale[36].

Altra dottrina sostiene al contrario che la nozione di domicilio accolta dalla Costituzione faccia sì riferimento a quella penalistica, ma non si esaurisca in essa,

[35] Non sono mancati tentativi di elaborare un'autonoma nozione costituzionale di domicilio, in base all'argomento che non sarebbe corretto desumere da fattispecie particolari o extra-costituzionali l'oggetto e il contenuto di una nozione posta nella norma costituzionale. Si veda G. MOTZO, *Contenuto ed estensione della libertà domiciliare*, in *Rass. dir. pubbl.*, 1954, II, p. 507 ss.
[36] P. BARILE, E. CHELI, voce *Domicilio*, cit., p. 859 ss.

ricomprendendo «qualunque luogo di cui si disponga a titolo privato, anche se non si tratta di privata dimora»[37].

Simile contrasto si rinveniva anche in giurisprudenza prima dell'intervento delle Sezioni Unite nel 2006, che tra l'altro mettono in evidenza come la tendenza giurisprudenziale sia nel senso di ampliare il concetto di domicilio in funzione della tutela penale e di circoscriverlo quando l'ambito domiciliare rappresenta un limite allo svolgimento delle indagini. A fronte di decisioni in cui per stabilire se un luogo rientrasse o meno nella tutela dell'art. 14 Cost. si faceva prevalentemente riferimento alla utilizzazione dello stesso per lo svolgimento di manifestazioni della vita privata e alla durata del rapporto tra il luogo e la persona, ve ne erano altre in cui si poneva l'accento sul carattere esclusivo (lo *ius excludendi alios*) e sulla difesa della *privacy*.

Esemplificative di tale contrasto giurisprudenziale sono le sentenze relative alla possibilità di qualificare l'automobile come domicilio, e quindi di farla rientrare nell'àmbito di tutela dell'art. 14 Cost.[38]. Muovendo dall'identificazione del concetto di domicilio con quello penalistico di privata dimora, la giurisprudenza maggioritaria esclude che tale qualifica spetti all'abitacolo di un autoveicolo, in quanto spazio nel quale non si compiono, di norma, atti caratteristici della vita domestica[39]. Poiché, tuttavia, rientra tra le libertà individuali la facoltà di scegliere lo spazio più congeniale alla propria personalità in cui dimorare, l'abitacolo di un'autovettura può essere considerato luogo di privata dimora qualora venga sin dall'origine adibito a luogo di abitazione[40].

Non mancano decisioni in cui si estende la tutela dell'art. 14 Cost. anche all'automobile, sulla base dell'assunto per cui rientrerebbero nel concetto di privata dimora tutti quei luoghi che «*oltre all'abitazione, assolvano la funzione di*

[37] G. AMATO, *Art. 14*, cit., p. 61. In questo senso, in giurisprudenza, Cass., sez. IV, 16 marzo 2000, Viskovic, in *C.E.D. Cass.*, n. 217688, secondo cui «*la nozione di domicilio accolta dall'art. 14 Cost. è diversa e più ampia di quella prevista dall'art. 614 c.p., finendo per coprire tutti i luoghi, siano o meno di dimora, in cui può aver luogo il conflitto di interessi che essa regola*».

[38] Si veda a tal proposito la ricostruzione fatta da Cass., sez. un., 31 ottobre 2001, Policastro, in *Cass. pen.*, 2002, p. 944 ss., che, tuttavia, non ha potuto dare soluzione alla questione perché priva di rilevanza nel caso concreto.

[39] Cass., sez. VI, 18 febbraio 2003, Palumbo, in *C.E.D. Cass*., n. 223960. In senso conforme, *ex multis*, Cass., sez. I, 29 luglio 2003, Faraci, in *C.E.D. Cass*., n. 225141; Cass., sez. VI, 4 febbraio 2003, Brozzu, in *C.E.D. Cass*., n. 226149; Cass., sez. VI, 14 gennaio 2003, Barilari, in *C.E.D. Cass.*, n. 223682.

[40] Cass., Sez., I, 29 gennaio 2001, Galli, in *C.E.D. Cass*., n. 218042. È il caso di *camper* o *roulotte*.

proteggere la vita privata e siano perciò destinati al riposo, all'alimentazione, alle occupazioni professionali e all'attività di svago»[41].

In questo senso è anche parte della dottrina che, partendo dal presupposto che il domicilio sia la "proiezione spaziale della persona"[42], pone l'accento non tanto sull'astratta abitabilità del luogo, bensì sullo svolgimento al suo interno delle attività in cui si svolge la sua personalità[43], riconoscendo all'autovettura la natura di spazio chiuso in cui l'individuo può preservare i propri effetti personali da ingerenze esterne, anche quando non sia materialmente presente all'interno dell'abitacolo[44].

La questione dell'ampiezza della nozione costituzionale di domicilio si avverte anche nello specifico ambito della criminalità informatica.

Infatti, con la legge n. 547 del 23 dicembre 1993, che ha introdotto nel codice penale le fattispecie di accesso abusivo ad un sistema informatico o telematico (art. 615 *ter*) e di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater*), il legislatore intendeva tutelare i sistemi informatici e telematici quali «espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti essenziali agli articoli 614 e 615 del codice penale»[45]. Tuttavia, come evidenziato da acuta dottrina «il parallelismo con il domicilio, bene eminentemente privato e personale, coglie solo parzialmente il contenuto dell'interesse all'*esclusione di terzi* da determinate "sfere di disponibilità e rispetto", create e rese fruibili dalla tecnologia informatica»[46].

Questa tensione è colta anche dalla giurisprudenza di legittimità, che in una recente pronuncia ha riconosciuto che il codice penale tutela il c.d. domicilio

[41] Cass., Sez. II, 10 giugno 1998, Zagaria, in *C.E.D. Cass*., n. 211142. In tal senso anche Cass., Sez. I, 10 agosto 2000, Nicchio e altri, in *C.E.D. Cass.*, n. 216749. La stessa Corte costituzionale in una risalente pronuncia relativa al potere dell'autorità amministrativa di intimare l'apertura di mezzi di trasporto, ha configurato l'autovettura come «*luogo di privata dimora sia pure esposto al pubblico dal quale il titolare ha il diritto di escludere ogni altro*»; C. cost., sentenza 25 marzo 1987, n. 88, in *Giur. cost.*, 1987, p. 682 ss., con nota di G. PAGANETTO, *Libertà domiciliare nelle autovetture e limiti alla tutela dell'ambiente*.

[42] La definizione si deve a A. AMORTH, *La Costituzione italiana*, Milano, 1948, p. 62.

[43] A. LARONGA, *L'utilizzabilità probatoria del controllo a distanza eseguito con sistema satellitare g.p.s.*, in *Cass. pen.*, 2002, p. 3050 ss.

[44] M. STRAMAGLIA, *Il pedinamento satellitare: ricerca ed uso di una prova "atipica"*, in *Dir. pen. proc.*, 2011, p. 213 ss.

[45] Così, la Relazione ministeriale al disegno di legge, p. 9. Sul punto, si veda L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, p. 80 ss.

[46] Testualmente, L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 80.

informatico «*quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto*»[47].

Il discorso si sposta quindi dal domicilio alla riservatezza, ma non per arrivare ad una distinzione, quanto a copertura costituzionale, circa limiti e presupposti di ingerenza da parte degli investigatori, come hanno fatto le Sezioni Unite in materia di videoriprese, bensì per teorizzare, assieme alla più attenta dottrina penalistica[48], l'esistenza di un diverso bene giuridico tutelato, quello alla riservatezza informatica. Tale diritto nasce come espansione del domicilio per acquistare autonomia in un ambito, quello digitale, in cui non ci sono confini, non ci sono luoghi *fisici* che possano riflettere il carattere privato o riservato delle attività che ivi si svolgano o di ciò che vi sia custodito. Il problema diviene allora quello dell'individuazione della fonte di tale diritto alla riservatezza informatica, che è cosa diversa dal diritto alla riservatezza *tout court*. Sul punto si avrà modo di tornare nel prosieguo della trattazione[49], ciò che preme fin da ora sottolineare è, ancora una volta, come le nuove tecnologie informatiche siano in grado di mettere in crisi non solo i tradizionali diritti fondamentali, come quello all'inviolabilità del domicilio, ma anche diritti relativamente nuovi, come quello alla riservatezza[50].

1.2 Libertà e segretezza delle comunicazioni (art. 15 Cost.)

L'art. 15 Cost. tutela la libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione, sancendone l'inviolabilità. Eventuali limitazioni possono avvenire solo «per atto motivato dell'autorità giudiziaria con le garanzie

[47] Cass., Sez. V, 26 ottobre 2012, n. 42021, inedita.
[48] L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 87 ss.; ID., *I diritti fondamentali nell'uso ed abuso dei* social network. *Aspetti penali*, in *Giur. merito*, 2012, p. 2532; R. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di* Internet, *in www.penalecontemporaneo.it*; ID., *Verso una rivalutazione dell'art. 615* ter *c.p.?,* in *Riv. trim. dir. pen. cont.*, 2012, n. 2, p. 126 ss.; ID., *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di "domicilio informatico" e lo* jus excludendi alios, in *Dir. pen. proc.*, 2005, p. 81 ss.
[49] *Infra*, par. 5.2.
[50] Di ciò è ben consapevole la Corte costituzionale tedesca che, nella nota sentenza sulla *Online Durchsuchung* ha ritenuto insufficiente la tutela offerta dall'*informationellen Selbstbestimmungsrecht*, da lei stessa elaborato nella sentenza sul censimento nel 1983, e ha coniato il nuovo diritto *auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. Si veda, *infra*, par. 5.1.

stabilite dalla legge». Non sono previsti, diversamente dagli artt. 13 e 14 Cost., casi eccezionali in cui la limitazione può essere disposta in via d'urgenza direttamente dall'autorità di pubblica sicurezza, salvo successiva convalida da parte dell'autorità giudiziaria[51].

Occorre fin da subito precisare che la corrispondenza viene considerata una *species* del più ampio *genus* comunicazione. È questo pertanto il concetto da chiarire per stabilire la portata della norma costituzionale. A tal proposito, si intende tradizionalmente per comunicazione uno scambio di idee o notizie tra mittente e destinatario – c.d. intersubiettività o personalità della corrispondenza che vale a distinguerla dalla libertà di manifestazione del pensiero[52] – che abbia carattere di attualità[53].

Non sono invece rilevanti né i mezzi usati per la comunicazione, né l'oggetto in cui si concreti il suo contenuto[54]. Ciò acquista particolare importanza proprio di fronte al progresso tecnologico e conferisce alla protezione costituzionale il necessario carattere di elasticità che consente di non lasciare prive di tutela nuove forme di comunicazione. Infatti, se la scelta del mezzo di comunicazione dovesse dipendere dal tipo di tutela che la costituzione riconosce, si assisterebbe ad una sostanziale violazione della libertà di comunicare e più in generale della libertà di

[51] P. BARILE, E. CHELI, voce *Corrispondenza*, cit., p. 749.

[52] Secondo P. BARILE, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, p. 163, diversi sarebbero gli scopi degli artt. 15 e 21 Cost.: tutela della riservatezza della comunicazione tra soggetti determinati nel primo caso, diffusione del pensiero senza confini né segreti nel secondo. Infatti, mentre l'art. 15 Cost. costituisce un diritto fondamentale che completa il diritto della persona umana (libertà personale, libertà domiciliare, libertà di corrispondenza, libertà di circolare e soggiornare ovunque), l'art. 21 Cost. costituisce anch'esso un diritto individuale, ma che pone le basi della comunità politica moderna.

[53] Non c'è unanimità di vedute in dottrina sull'individuazione del momento in cui la comunicazione cessa di essere attuale. Secondo taluno, l'attualità verrebbe meno nel momento in cui il destinatario prende conoscenza della comunicazione, dopodiché subentrerebbe la tutela di altre disposizioni costituzionali, come quelle a presidio della libertà personale, domiciliare, del diritto di proprietà. A. PACE, *Problematica delle libertà costituzionali, Lezioni, Parte Speciale II*, Padova, 1985, p. 232. Diversamente, P. BARILE, E. CHELI, voce *Corrispondenza*, cit., p. 745, ritengono necessaria un'indagine caso per caso del momento in cui, venendo meno l'attualità viene meno anche la tutela dell'art. 15 Cost., e che tenga conto del valore della comunicazione.

[54] P. BARILE, E. CHELI, voce *Corrispondenza*, cit., p. 744. *Contra*, A. PACE, *Art. 15*, in A. BRANCA (a cura di), *Commentario alla costituzione. Rapporti civili*, Bologna, 1975, p. 82 ss., secondo cui, una volta individuata la matrice del diritto all'inviolabilità delle comunicazioni nella libertà di espressione, logica conseguenza sarebbe la sua attitudine a tutelare le sole forme espressive, riconoscibili come tali esteriormente. L'art. 15 Cost. non si estenderebbe quindi alle «comunicazioni di non pensieri», come ad esempio alla corrispondenza non epistolare.

autodeterminazione. Logica conseguenza è che messaggi di posta elettronica, *chat*, servizi *VoIP* rientrano nell'ambito di tutela dell'art. 15 Cost.

La Costituzione tutela l'interesse di chi comunica alla segretezza della comunicazione, ossia ad impedire che altri percepiscano l'atto comunicativo in sé considerato, e non l'interesse al segreto sull'oggetto della comunicazione, che può anche non consistere in una notizia privata o riservata. Controverso è, invece, se rientri nell'ambito applicativo dell'art. 15 Cost. anche l'interesse a mantenere *riservato* l'atto stesso del comunicare, ossia il fatto che una determinata comunicazione, intesa come fatto storico, sia avvenuta[55]. Ci si domanda se sia coperta dalla doppia riserva, di legge e di giurisdizione, anche l'acquisizione dei c.d. dati esteriori di una comunicazione, quali ad esempio numero chiamato, durata, ubicazione, etc.

La Corte costituzionale, chiamata a pronunciarsi in merito, ha affermato che l'ampiezza della tutela accordata dall'art. 15 Cost. «*è sicuramente tale da ricomprendere fra i propri oggetti anche i dati esteriori di individuazione di una determinata conversazione telefonica*»[56]. Infatti, la Costituzione tutela non solo la segretezza, ma anche la libertà delle comunicazioni, offrendo così una protezione molto ampia al diritto dei singoli di intrattenere relazioni riservate. Anzi, secondo autorevole dottrina, tra libertà e segretezza, è senz'altro la prima che caratterizza la tutela costituzionale: la segretezza sarebbe uno strumento volto a garantire la libertà[57]. La libertà di comunicare viene quindi concepita come «*parte necessaria di*

[55] Così, F. CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2002, p. 66.
[56] C. cost., 11 marzo 1993, n. 81, in *Cass. pen.*, 1993, p. 2744. Conforme, C. cost., 17 luglio 1998, n. 281, in *Giur. cost*., 1998, p. 2721 ss. Anche la Corte Europea dei Diritti dell'Uomo ha riconosciuto che l'utilizzazione come mezzo di prova dei tabulati telefonici integra un'ingerenza nella *privacy* e incide pertanto sul diritto al rispetto della vita privata, tutelato dall'art. 8 CEDU. Cfr. Corte europea dei diritti dell'uomo, *Heglas v. Czech Republic*, in *Cass. pen.*, 2007, p. 3947 ss., con nota di L. DE MATTEIS. Si veda anche A. BALSAMO, A. TAMIETTI, *Le intercettazioni, tra garanzie formali e sostanziali*, in A. BALSAMO, R. E. KOSTORIS (a cura di), *Giurisprudenza europea e processo penale italiano*, Torino, 2008, p. 464. Anche la Corte costituzionale tedesca, nell'importante sentenza sulla legge di attuazione della direttiva *data retention*, ha ritenuto che i dati c.d. esterni di una comunicazione rientrino nell'ambito di tutela dell'art. 10, comma 1 GG, che garantisce la segretezza delle comunicazioni (*Fernmeldegeheimnis*). *BVerfG*, 2 marzo 2010, *1BvR 256/08*, *1 BvR 263/08*, *1 BvR 586/08*, in *www.bundesverfassungsgericht.de*. *Infra*, capitolo II, par. 7.5. In dottrina, si veda, *ex multis*, A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. e proc. pen.*, 2005, p. 594 ss.; F. CAPRIOLI, *Colloqui riservati*, cit.
[57] P. BARILE, *Diritti dell'uomo*, cit., p. 164.

quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana»[58].

Parte della dottrina non condivide simile approdo interpretativo, pur apprezzandone l'ispirazione garantistica[59]. Presupposto di tale impostazione è il riconoscimento del fatto che l'art. 15 Cost. assicuri, assieme all'art. 14 Cost., il diritto dell'individuo «all'inaccessibilità (o intimità) della propria sfera privata, da intendersi come diritto a coltivare la propria personalità in ambiti spirituali (la comunicazione riservata) e spaziali (il domicilio) sottratti all'ascolto e all'osservazione di estranei»[60]. In quest'ottica, l'interesse a non rendere noto il fatto che una comunicazione è avvenuta (quando e dove), presenta maggiore affinità con il diritto alla riservatezza, inteso come interesse al controllo sulla circolazione e sull'uso delle notizie personali, «del quale condividerebbe il (limitato) regime di tutela costituzionale»[61], ed esula dalla tutela che l'art. 15 cost. accorda alla sfera privata.

Pur aderendo all'orientamento in forza del quale i dati esterni rientrano nell'ambito dell'art. 15 Cost., resta il problema del se per la loro acquisizione sia necessario un provvedimento del giudice, come per le intercettazioni[62], o se sia sufficiente un provvedimento del pubblico ministero[63].

Il legislatore, intervenuto a disciplinare la materia della conservazione e acquisizione dei dati di traffico telefonico con il decreto legislativo 196/2003, c.d. codice *privacy*, dopo aver inizialmente attribuito al giudice competenza ad emettere il provvedimento acquisitivo, ha successivamente ritenuto sufficiente un decreto del pubblico ministero, da adottare *ex* art. 256 c.p.p.[64]

---

[58] C. cost., 11 marzo 1993, n. 81, cit.
[59] Così, F. CAPRIOLI, *Colloqui riservati*, cit., p. 68.
[60] *Ibidem*, p. 56. Tanto è vero che, parafrasando la definizione di domicilio come proiezione spaziale della persona, (*supra* nota 24), autorevole dottrina penalistica ha parlato della comunicazione riservata come di una «proiezione spirituale» del soggetto che la pone in essere. F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. e proc. pen.*, 1967, p. 1120.
[61] F. CAPRIOLI, *Colloqui riservati*, cit., p. 70. Sul diritto alla riservatezza si veda *infra*, par. 2.
[62] In questo senso, Cass., sez. un., 13 luglio 1998, Gallieri, in *Giust. pen.*, 1999, III, c. 614 ss.
[63] Così, allineandosi all'orientamento della Corte costituzionale che aveva escluso l'applicabilità della disciplina delle intercettazioni, Cass., sez. un., 23 febbraio 2000, D'Amuri, in *Giur. it.*, 2001, p. 1707 ss.
[64] Sulle vicende relative alla disciplina della conservazione e acquisizione dei dati di traffico, si rinvia a *infra*, capitolo II, par. 7 ss.

Ciò è compatibile con l'art. 15 Cost., che richiede che la limitazione del diritto ivi garantito avvenga per mezzo di un provvedimento dell'autorità giudiziaria, sia essa il giudice o il pubblico ministero[65]. L'idea, condivisibile, è che, pur essendo unico il diritto che viene in considerazione, i presupposti per l'adozione di limitazioni dello stesso varino a seconda dell'intensità dell'intromissione nella sfera privata. Il tutto nel rispetto del dettato costituzionale[66].

Per quanto riguarda quindi, il rapporto tra nuovi strumenti di indagine informatica e art. 15 Cost., è bene tenere a mente l'insegnamento della Corte costituzionale, in forza del quale l'attinenza della libertà e segretezza delle comunicazione «*al nucleo essenziale dei valori della personalità,* […] *comporta un vincolo interpretativo diretto a conferire a quella libertà, per quanto possibile, un significato espansivo*»[67].

1.3 Libertà di circolazione (art. 16 Cost.)

L'utilizzo di nuove tecnologie per condurre classiche attività di indagine impone di prendere in considerazione anche diritti di libertà che a prima vista poco hanno a che vedere con i mezzi di ricerca della prova. Il riferimento è all'uso del *GPS* per seguire e monitorare gli spostamenti della persona nello spazio e, quindi, all'art. 16 Cost. che garantisce la libertà di circolazione e soggiorno.

Tale diritto è strettamente connesso alla libertà personale, tanto che non è mancato chi ne ha negato autonomia rispetto alla sfera di tutela offerta dall'art. 13 Cost.[68]. Diversamente, altra parte della dottrina, muovendo dal dato costituzionale, riconosce che si tratta di due libertà distinte, ancorché strettamente connesse: la libertà personale attiene alla persona in sé, mentre quella di circolazione e soggiorno

[65] La stessa Corte costituzionale, nella sentenza n. 81 del 1993, aveva precisato che spettava al legislatore l'individuazione dell'autorità giudiziaria (giudice o pubblico ministero) competente ad emanare il provvedimento acquisitivo dei tabulati telefonici.

[66] Similmente a quanto afferma la Corte di Strasburgo con riferimento all'art. 8 CEDU. Contra, F. CAPRIOLI, *Colloqui riservati*, cit., p. 71. Sul punto si tornerà nel prosieguo della trattazione, *infra*, par. 3 ss.

[67] C. cost., 11 marzo 1993, n. 81, cit.

[68] V. CRISAFULLI, *Libertà personale, costituzione e passaporti*, in *Arch. pen.*, 1955, II, p. 117 ss.; M. GALIZIA, *La libertà di circolazione e soggiorno (dall'Unificazione alla Costituzione repubblicana)*, in P. BARILE (a cura di), *La pubblica sicurezza*, Vicenza, 1967, p. 545 ss.; U. DE SIERVO, voce *Soggiorno, circolazione, emigrazione (Libertà di)*, in *Novissimo digesto italiano*, vol. XVII, Torino, 1970, p. 822 ss.

riguarda la vita di relazione, presuppone un rapporto tra persona e territorio[69]. Secondo questo diverso orientamento, la libertà tutelata dall'art. 16 Cost. atterrebbe ad un momento cronologicamente successivo a quello della libertà personale, presupponendola e sviluppandola[70]. Entrambe sarebbero dunque espressione della più ampia libertà di autodeterminazione della persona[71].

Non tutte le restrizioni alla libertà di circolazione e soggiorno rientrerebbero quindi nell'art. 16 Cost., ma «solo quelle che non tocchino direttamente ed immediatamente la persona in qualcuno dei suoi attributi essenziali, [ossia] la sua dignità sociale e la sua personalità morale»[72].

In quest'ottica e alla luce del progresso tecnologico, l'art. 16 Cost. avrebbe la funzione di tutelare l'individuo da forme di controllo dei suoi movimenti che non raggiungono la soglia della restrizione della libertà personale, ma che sono comunque in grado di comprimere la sua libertà di autodeterminazione, fungendo da remora a determinati spostamenti[73]. Il riferimento è al c.d. pedinamento satellitare o al tracciamento del cellulare, su cui si tornerà approfonditamente nel prosieguo della trattazione[74].

Così concepito, il diritto alla libertà di circolazione, si arricchirebbe di una nuova componente: il diritto a non essere localizzati[75].

In realtà, con specifico riferimento al controllo dei movimenti della persona al fine di acquisire elementi utili per un procedimento penale, il confine tra limitazione della libertà personale e restrizione della libertà di circolazione è labile. Infatti, già autorevole dottrina distingueva tra libertà di locomozione, intesa come possibilità di disporre dei propri movimenti, e quindi come una delle facoltà in cui si esplica il godimento della libertà personale, tutelata dall'art. 13 Cost. e libertà di circolazione e soggiorno in senso stretto che costituiscono manifestazioni della libertà personale

[69] A. BARBERA, *I principi costituzionali*, cit., p. 146 ss.; P. BARILE, *Diritti dell'uomo*, cit., p. 172.
[70] P. BARILE, *Diritti dell'uomo*, cit., p. 172. Secondo G. VASSALLI, *La libertà personale*, cit., p. 405, ne deriverebbe un concetto unitario di libertà personale, intesa come «l'interesse di ogni individuo a non essere in nessun modo turbato nella propria attività esterna in sé e per sé considerata». La questione dell'ambito di applicazione delle due norme costituzionali, si era posta con riferimento alle misure di prevenzione. Cfr. G. AMATO, *Art. 16*, cit., p. 114 ss.
[71] S. GALEOTTI, *La libertà personale*, Milano, 1953 p. 12.
[72] A. BARBERA, *I principi costituzionali*, cit., p. 200.
[73] A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. e proc. pen.*, 2005, p. 633.
[74] Capitolo III, par. 2 ss.
[75] A. CAMON, *L'acquisizione dei dati*, cit.

«sotto il particolare riflesso della possibilità di spostarsi da una località all'altra e di fissare liberamente la propria dimora»[76]. Più di recente è stato per l'appunto sostenuto che il c.d. pedinamento *GPS* costituirebbe una limitazione della libertà personale[77].

Le conseguenze rilevano sotto il profilo dei presupposti di adozione di simili strumenti investigativi, diversi a seconda che l'attività di indagine si iscriva nell'art. 13 o nell'art. 16 della Costituzione[78].

Gli effetti che strumenti di controllo come il *tracking* GPS o le videoriprese possono avere sulla libertà di autodeterminazione della persona, nella sua duplice espressione di libertà morale e libertà di circolazione e movimento, sono ben esemplificati in una sentenza della Corte Suprema dell'Oregon del 1988 in cui si afferma che ogni strumento che consenta alla polizia di localizzare rapidamente una persona o un oggetto per un periodo prolungato, costituisce una significativa limitazione della libertà personale, intesa come libertà dal controllo – *freedom from scrutiny* -[79]. Si ammette inoltre che la libertà di autodeterminazione possa essere limitata in misura uguale, se non maggiore, dalla minaccia del controllo rispetto al controllo effettivo. Sulla base di queste premesse, la Corte teorizza quindi l'esistenza di un *constitutional right to freedom from technologically advanced scrutiny*, ricavabile dall'art. 1, par. 9 della Costituzione dello Stato dell'Oregon, che al pari del IV Emendamento alla Costituzione americana, tutela la libertà personale degli individui.

2. Privacy *e riservatezza. Alcune distinzioni preliminari*

La *privacy* nasce come libertà borghese, come privilegio di pochi[80]. L'originaria elaborazione del *right to privacy* si fa risalire all'omonimo e celebre

[76] G. VASSALLI, *La libertà personale*, cit., p. 384.
[77] L.FILIPPI, *Il GPS è una prova incostituzionale? Domanda provocatoria, ma non troppo, dopo la sentenza* Jones *della Corte Suprema* U.S.A., in *Arch. pen.*, 2012, n.1. *Infra*, capitolo III, par. 2.1.
[78] *Infra*, capitolo III, par. 2.1.
[79] *State v. Campell*, 759 P.2d 1040, 1048-1049 (Or. 1988). In merito si veda D. J. GLANCY, *Privacy on the Open Road*, *30 Ohio N. U. L. Rev. 295 (329)*.
[80] Sostiene, infatti, S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, p. 24, che storicamente la *privacy* può essere riportata al disgregarsi della società feudale e all'affermarsi della classe borghese. A livello sociale e istituzionale, la nascita della *privacy* non si presenta quindi come un'esigenza "naturale"

saggio di Samuel Warren e Louis Brandeis, del 1890[81]. I due studiosi americani (Brandeis sarà futuro giudice della Corte Suprema degli Stati Uniti), avvertendo l'esigenza di tutelare la vita privata da nuove forme di violazione, teorizzano il *right to be let alone*, nucleo primigenio del diritto alla *privacy*, come proiezione del diritto di proprietà. Ci si muove ancora nell'ambito delle libertà da – *liberty from* -.

Significativo il momento storico in cui lo scritto vede la luce, che coincide con i primi sviluppi dell'era tecnologica[82]. Vi è d'altronde una costante relazione tra *privacy* e mutamenti determinati dalle tecnologie dell'informazione[83]. Ciò che fa della *privacy* una nozione dinamica e poliedrica, posta a tutela di diversi interessi, orientati a difesa della libertà individuale e dell'autodeterminazione[84]. La *privacy* comprende un fascio di diritti, tra cui: riservatezza, identità personale, protezione dei dati personali, vita privata, diritto all'immagine, alla reputazione[85]. Appare quindi più corretto parlare di diritti di *privacy*[86].

Nella sua iniziale accezione di *right to be let alone*, il *right to privacy* può essere inteso innanzitutto come diritto all'inviolabilità della sfera privata o diritto alla riservatezza.

Giova a questo punto richiamare la nota *Sphärentheorie* – teoria delle sfere -, elaborata dalla dottrina tedesca verso la metà del secolo scorso[87]. Tale dottrina esemplifica i rapporti tra individuo e società facendo ricorso all'immagine di tre sfere concentriche, di diametro progressivamente minore, contenenti ognuna informazioni che il soggetto vuole mantenere *lato sensu* riservate. La sfera più ampia è quella privata (*Privatsphäre*) e comprende tutte quelle notizie, quei comportamenti, quei

---

dell'uomo, ma come l'acquisizione di un privilegio da parte di un gruppo. Come è stato correttamente affermato, «*poverty and privacy are simply contradictory*», A. M. BENDICH, *Privacy, Poverty and the Constitution*, *Report for the Conference on the Law of the Poor*, *University of California at Berkeley*, p. 7.

[81] S. D. WARREN, L. D. BRANDEIS, *The Right to Privacy*, in *Harv. L. Rev.*, 4 (1890), p. 193 ss.

[82] G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Milano, 1983, p. 1. L'invenzione del telefono e della fotografia istantanea è degli anni '80 dell'Ottocento.

[83] S. RODOTÀ, *Tecnologie*, cit., p. 101.

[84] G. ILLUMINATI, *La disciplina processuale*, cit., p. 3.

[85] F. CAPRIOLI, *Colloqui riservati*, cit., p. 16 riconduce nell'alveo dei diritti di *privacy* anche il diritto alla inaccessibilità della sfera privata, a sua volta comprensivo del diritto alla inviolabilità domiciliare e del diritto alla segretezza delle comunicazioni.

[86] S. CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in D. NEGRI (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 16.

[87] H. HUBMANN, *Das Persönlichkeitsrecht*, Münster-Köln-Böhlau, 1953, p. 17. Teoria ripresa da Bricola nel noto scritto *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. e proc. pen.*, 1967, p. 1083 ss.

discorsi che il soggetto non vuole divengano di pubblico dominio. La sfera confidenziale (*Vertrauenssphäre*) riguarda informazioni di cui solo determinate persone sono a conoscenza e che non si vuole vengano ulteriormente divulgate. Infine, la sfera del segreto (*Geheimnisphäre* o *Intimsphäre*) comprende «notizie o fatti che per interessi o ragioni particolari sono inaccessibili a chiunque non sia titolare del segreto»[88].

Il diritto all'inviolabilità della sfera privata, o diritto alla riservatezza[89], può essere quindi definito come «l'interesse alla conoscenza esclusiva delle notizie inerenti alla propria sfera personale»[90].

Con l'avvento della tecnologia informatica si creano anche le prime banche dati. Il reperimento, la raccolta, la conservazione di dati personali diviene più rapida. Le tracce elettroniche che ognuno lascia dietro di sé nell'agire quotidiano consentono di creare profili della personalità, e fanno divenire urgente l'esigenza di avere il controllo sulla diffusione e sull'uso delle proprie informazioni personali. La *privacy* acquista dunque una dimensione collettiva, l'attenzione si sposta dalla segretezza al controllo[91]. Non più solo *right to be let alone*, ma anche *right to control of the information about oneself*, da *liberty from* a *liberty to*.

In questa seconda accezione, la *privacy* acquista un significato assimilabile a quello di autodeterminazione informativa[92], di tutela dei dati personali.

L'ulteriore affermarsi delle c.d. tecnologie del controllo, che consentono di sorvegliare e localizzare l'individuo fa riemergere l'esigenza di tutela della sfera privata, che assume connotazioni nuove[93]. Infatti, come autorevolmente rilevato, «la tecnologia contribuisce a far nascere una sfera privata più ricca, ma più fragile,

[88] F. BRICOLA, *Prospettive e limiti*, cit., p. 1087. Tale distinzione corrisponde a quella tra notizie private, notizie confidenziali e notizie segrete. Così, F. CAPRIOLI, *Colloqui riservati*, cit., p. 17.
[89] L'espressione diritto alla riservatezza è entrata nel linguaggio giuridico italiano per opera soprattutto di Ravà (*Istituzioni di diritto privato*, Padova, 1938) e De Cupis (*I diritti della personalità*, Padova, 1942). Così, G. PUGLIESE, *Il diritto alla "riservatezza" nel quadro dei diritti della personalità*, in *Riv. dir. civ.*, 1963, p. 608.
[90] F. CAPRIOLI, *Colloqui riservati*, cit., p. 13.
[91] S. RODOTÀ, *Tecnologie*, cit., p. 29 ss.
[92] Sulla creazione di questo diritto ad opera della Corte costituzionale tedesca, si veda *infra*, par. 5.2.
[93] Si pensi solo al telefono cellulare, che è ormai divenuto imprescindibile, tanto da essere considerato una sorta di «protesi della persona», un «guinzaglio elettronico», che consente di seguire ogni movimento dell'individuo. Discorso del Presidente Stefano Rodotà, Relazione 2002, Garante per la protezione dei dati personali, Roma 20 maggio 2003; S. NIGER, *Le nuove dimensioni della* privacy*: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, p. 74.

sempre più esposta a insidie. Da qui una sempre più forte necessità di rafforzamento della protezione giuridica, e quindi, un allargamento delle frontiere della *privacy*»[94].

Si assiste oggi ad una duplice tendenza evolutiva del concetto di *privacy*: da un lato ad una ridefinizione della nozione, da potere di esclusione a potere di controllo, dall'altro ad un ampliamento dell'oggetto del diritto alla riservatezza, determinato dall'ampliamento della sfera privata. Essa comprende tutto quell'insieme di azioni, comportamenti, opinioni, preferenze, informazioni personali, su cui l'interessato intende mantenere un controllo esclusivo[95].

La *privacy* può quindi essere definita come il diritto di mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera privata[96]. In quest'ottica, la riservatezza diviene strumentale alla *privacy*[97]. Infatti, sebbene una definizione di *privacy* come diritto di essere lasciato solo abbia da tempo perso valore generale, essa continua a cogliere un aspetto essenziale del problema. Non può quindi trascurarsi il nucleo primigenio della riservatezza, soprattutto quando si fa riferimento alle indagini informatiche che consentono agli investigatori intromissioni sempre più insidiose nella sfera privata.

Il settore delle innovazioni scientifiche è magmatico; si pone pertanto la necessità di individuare principi generali, che delineino i binari entro cui dovranno di volta in volta iscriversi gli interventi legislativi, in modo che il diritto sia in grado di garantire tutela agli individui, senza soccombere di fronte alla tecnologia. Le difficoltà nell'individuare tali principi risiedono non solo, e non soltanto, nel fatto che si tratta di una realtà in costante e rapida evoluzione, ma soprattutto nella molteplicità di interessi e valori, spesso tra loro confliggenti, che caratterizzano i diversi ambiti coinvolti[98]. Di qui l'importanza di riconoscere rango di diritti fondamentali ai diritti di *privacy*.

---

[94] S. RODOTÀ, *Tecnologie*, cit., p. 104 ss.
[95] *Ibidem*, p. 101 ss. individua quattro tendenze nell'evoluzione del concetto di *privacy*: «dal diritto ad essere lasciato solo al diritto di mantenere il controllo sulle informazioni che mi riguardano; dalla *privacy* al diritto all'autodeterminazione informativa; dalla *privacy* alla non discriminazione; dalla segretezza al controllo».
[96] *Ibidem*, p. 122.
[97] F. CAPRIOLI, *Colloqui riservati*, cit., p. 16.
[98] S. RODOTÀ, *Tecnologie*, cit., p. 42.

2.1 Fonte del diritto alla riservatezza

Riconoscere valore costituzionale ai diritti di *privacy* è particolarmente importante perché significa che eventuali limitazioni, in un'ottica di bilanciamento, si giustificano solo se poste a tutela di altri diritti dello stesso rango[99].

Per quanto riguarda il fondamento costituzionale del diritto alla riservatezza, diverse sono le alternative prospettate dalla dottrina.

Innanzitutto si sono richiamate le disposizioni in materia di libertà personale – intesa come libertà morale e di autodeterminazione – libertà e segretezza delle comunicazioni, inviolabilità del domicilio (artt. 13, 14, 15 Cost.). Tali norme, interpretate estensivamente (alla luce del progresso tecnologico), si presterebbero infatti a garantire la necessaria protezione alla vita privata dell'individuo, della quale ciascuna tutela un aspetto specifico[100].

Si è inoltre fatto riferimento all'art. 21 Cost., sul presupposto che la libertà di manifestazione del pensiero comprendesse anche il suo opposto, ossia l'interesse a non manifestarlo[101]. Così interpretata, tale norma consentirebbe di tutelare l'individuo di fronte a forme di apprensione e divulgazione di notizie che si vogliono mantenere riservate. I limiti di tale impostazione risiedono, tuttavia, nell'affidare alla stessa disposizione la tutela di interessi contrapposti, spesso da bilanciare tra loro, «con possibile insorgenza di conflitti "interni" di difficile composizione»[102].

Si è quindi ritenuto di poter rinvenire la fonte costituzionale del diritto alla riservatezza nell'art. 3 Cost., inteso come "clausola generale della dignità". La

[99] A. PACE, *Diritti «fondamentali» al di là della Costituzione*, in *Pol. dir.*, 1993, p. 4, invece, nega rango costituzionale al diritto alla riservatezza proprio perché questo determinerebbe un aumento dei conflitti con diritti costituzionali espressamente riconosciuti.

[100] P. BARILE, *Diritti dell'uomo*, cit., p. 61. Cfr. T. A. AULETTA, *Riservatezza e tutela della personalità*, Milano, 1978, p. 43, il quale precisa che, se in passato si tendeva a garantire all'individuo un ambito d'intimità privata mediante la tutela del domicilio e della corrispondenza, oggi tali forme di protezione non sono più sufficientemente efficaci. Infatti, la violazione non avviene semplicemente mediante l'apprendimento della notizia segreta, ma più in generale attraverso la pubblicizzazione delle notizie, ciò che «ha fatto sorgere il diritto alla riservatezza». Inoltre, la consapevolezza o anche solo la possibilità del controllo possono ingenerare nell'individuo cambiamenti circa le abitudini di vita, indurlo a non tenere determinati comportamenti, limitando così il libero sviluppo della sua personalità e la sua autodeterminazione. *Contra*, F. BRICOLA, *Prospettive e limiti*, cit., p. 1092, secondo cui «la tendenza a desumere il riconoscimento del diritto alla riservatezza sulla base di disposizioni costituzionali che proclamano diritti affini o che costituiscono manifestazioni parziali del diritto alla riservatezza [pur non essendo] metodologicamente scorretto, […] è insufficiente».

[101] A. CERRI, *Libertà negativa di manifestazione del pensiero e di comunicazione – Diritto alla riservatezza: fondamento e limiti*, in *Giur. cost.*, 1974, p. 610 ss.

[102] S. CARNEVALE, *Autodeterminazione informativa*, cit., p. 17.

dignità umana, proiettata a livello sociale, presupporrebbe infatti il diritto di preservare la propria sfera privata da forme di intromissione[103].

Il fondamento costituzionale del diritto alla riservatezza è stato infine individuato nell'art. 2 Cost., muovendo dalla sua interpretazione come fattispecie "aperta", fonte di nuovi diritti della personalità[104]. Come noto, la discussione sulla natura "aperta" o "chiusa" di questa norma è stata al centro di un acceso dibattito tra i costituzionalisti. Da un lato vi era chi la considerava una clausola riassuntiva di diritti di libertà espressamente tutelati nelle altre norme costituzionali[105], dall'altro si attribuiva all'art. 2 Cost. la funzione di tutela ora di diritti naturali non presenti nel testo costituzionale, ora di quei valori di libertà emergenti a livello di costituzione materiale[106].

Tuttavia, quando si tratta di bilanciare il diritto alla riservatezza con le esigenze di repressione dei reati, il richiamo al solo art. 2 Cost. mostra i suoi limiti. Tale norma, infatti, contrariamente agli artt. 13, 14 e 15 Cost., non individua i presupposti di una limitazione da parte della pubblica autorità dei diritti inviolabili ivi sanciti[107].

---

[103] Nel senso che il mancato riconoscimento «di un certo ambito privato dal quale poter escludere l'altrui ingerenza» finirebbe per «pregiudicare lo stesso valore della persona, e quindi la sua dignità», T. A. AULETTA, *Riservatezza*, cit., p. 36. L'art. 3 Cost. presenta una certa affinità con gli artt. 1 e 2 della Costituzione tedesca (*Grundgesetz*), che tutelano rispettivamente la dignità umana e il libero sviluppo della personalità, e da cui il *Bundesverfassungsgericht* e la dottrina fanno discendere l'affermazione costituzionale del diritto alla vita privata. Cfr. F. BRICOLA, *Prospettive e limiti*, cit., p. 1095 ss., il quale ritiene che la locuzione «dignità sociale» sia tuttavia troppo generica per servire allo scopo di dare fondamento costituzionale al diritto alla riservatezza.

[104] Seppur suggestiva, la tesi dell'esistenza nel nostro ordinamento di un unico diritto della personalità, non può essere accolta. Mosso proprio dall'esigenza di dare solido fondamento costituzionale al diritto alla riservatezza, il Giampiccolo aveva infatti tentato di importare in Italia il modello tedesco, dove la tutela delle diverse manifestazioni della personalità si fa discendere dall'*allgemeine Persönlichkeitsrecht*, che affonda le sue radici negli articoli 1, comma 2 e 2, comma 2 *GG*. G. GIAMPICCOLO, *Scritti giuridici in memoria di P. Calamandrei*, V, Padova, 1958, p. 440 ss. A tale impostazione è stato autorevolmente obiettato che «i beni personali giuridicamente tutelati sono parecchi e dotati ciascuno di proprie peculiarità», e che è quindi più opportuno parlare di una pluralità di diritti della personalità. A. DE CUPIS, *I diritti della personalità*, Padova, 1942, p. 34 ss. In argomento si veda anche G. PUGLIESE, *Il diritto alla "riservatezza"*, cit., p. 607; S. NIGER, *Le nuove dimensioni*, cit., p. 42 ss. Per quanto riguarda invece l'ordinamento tedesco si rinvia a *infra*, par. 5.1.

[105] P. BARILE, *Diritti dell'uomo*, cit., p. 54 ss.; A. PACE, *Diritti «fondamentali»*, cit., p. 4.

[106] A. BARBERA, *Art. 2*, in A. BRANCA (a cura di), *Commentario della Costituzione. Principi fondamentali*, Bologna, 1975, p. 65 ss.. Oltre al diritto alla riservatezza, hanno trovato riconoscimento *ex* art. 2 Cost., tra gli altri: il diritto alla propria immagine, il diritto ai segni distintivi della propria personalità, il diritto alla rettifica delle notizie inesatte, il diritto al libero sviluppo della personalità.

[107] F. B. MORELLI, *La giurisprudenza costituzionale italiana tra diritto alla riservatezza e potere di controllo sulle informazioni personali*, in D. NEGRI (a cura di), *Protezione dei dati personali*, cit., p. 41.

La Corte costituzionale considera la riservatezza come appartenente «*al nucleo essenziale dei valori della personalità, parte necessaria di quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana*»[108]. Tuttavia, consapevole dell'insufficienza dell'art. 2 Cost. a tutelare l'inviolabilità della sfera privata, essa àncora il riconoscimento del diritto alla riservatezza non solo a tale norma, ma anche ai diversi diritti di libertà che di volta in volta vengono in rilievo[109]. Questa impostazione si richiama a quella dottrina che, pur negando all'art. 2 Cost. la natura di fonte di nuovi diritti, ne ammette l'utilizzo strumentale al fine di un'interpretazione espansiva dei singoli diritti di libertà previsti espressamente dalla Costituzione[110].

Questo ragionamento è seguito dalla Consulta nella già menzionata sentenza in materia di intercettazioni telefoniche, dove si riconosce l'appartenenza dell'interesse alla libertà e segretezza delle comunicazioni, tutelato dall'art. 15 Cost., al più ampio *genus* dei diritti della personalità, definiti inviolabili dall'art. 2 Cost. Le due disposizioni sono quindi poste a tutela della riservatezza delle comunicazioni[111].

In una decisione dello stesso anno, chiamata a pronunciarsi sulla legittimità costituzionale delle norme del codice di procedura civile che consentivano di inibire la pubblicazione delle immagini altrui, anche qualora fossero destinate alla stampa, la Corte ha ritenuto prevalente rispetto alla libertà di stampa e di informazione, il diritto alla riservatezza, riconosciuto e garantito dagli artt. 2, 3, comma 2 e 13, comma 1 Cost.[112]

Tuttavia, anche questa impostazione mostra i suoi limiti, non prestandosi a ricomprendere istanze di tutela non riconducibili a diritti espressamente tutelati.

---

[108] C. cost., 11 luglio 1991, n. 366, cit.
[109] F. B. MORELLI, *La giurisprudenza costituzionale*, cit., p. 41.
[110] P. BARILE, *Diritti dell'uomo*, cit., p. 56 ss.; A. PACE, *Problematica delle libertà costituzionali. Parte generale*, 3ª ed., Padova, 2003, p. 25 ss. In quest'ottica, peraltro, la distanza tra la tesi dell'art. 2 Cost. come fattispecie "aperta" o come fattispecie "chiusa" si riduce. Cfr. S. CARNEVALE, *Autodeterminazione informativa*, cit., p. 13.
[111] C. cost., 6 aprile 1973, n. 34, cit. Cfr. anche C. cost. 11 luglio 1991, n. 366, in *Giur. cost.*, 1991, p. 2914 ss.; C. cost., 12 gennaio 1993, n. 10, in *Giur. cost.*, 1993, p. 52 ss.
[112] C. cost., 5 aprile 1973, n. 38, in *Giur. cost.*, 1973, p. 354 ss., con osservazioni di G. PUGLIESE, *Diritto all'immagine e libertà di stampa*. La Corte precisa che tali disposizioni «*riconoscono e garantiscono i diritti inviolabili dell'uomo tra i quali rientra quello del proprio decoro, del proprio onore, della propria rispettabilità, riservatezza, intimità e reputazione sanciti espressamente dagli artt. 8 e 10 della CEDU*».

Occorre quindi elaborare un diritto alla riservatezza che abbia autonomo fondamento, e che stabilisca presupposti e limiti delle intromissioni consentite alla pubblica autorità. A tal fine non si può che volgere lo sguardo oltre i confini nazionali, e guardare in particolar modo alla CEDU e alla Carta dei Diritti Fondamentali dell'Unione Europea[113].

3. Il diritto alla vita privata nella Convenzione Europea dei Diritti dell'Uomo e delle Libertà Fondamentali

La Convenzione Europea dei Diritti dell'Uomo e delle Libertà Fondamentali (d'ora innanzi CEDU) tutela in un'unica norma, l'art. 8, il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza.

La nozione di vita privata, in particolare, «è ampia e non suscettibile di una definizione esaustiva»[114]; essa comprende sia il diritto a godere di una sfera esclusiva di intimità personale (*right to be let alone*), sia il diritto di sviluppare la propria personalità, intrattenendo relazioni sociali con altri individui[115]. L'art. 8 CEDU tutela non solo il diritto alla riservatezza, ma anche quello all'autodeterminazione informativa, ossia al controllo sui propri dati personali[116].

[113] La necessità di fare riferimento anche ai diritti riconosciuti dalle Convenzioni internazionali era stata evidenziata già dalla dottrina più attenta. Si veda per tutti, F. BRICOLA, *Prospettive e limiti*, cit., p. 1097 ss. Tale dottrina attribuiva quindi all'art. 2 Cost. la funzione di recepire nel nostro ordinamento i diritti espressi dall'evoluzione della coscienza sociale, che avessero trovato consacrazione in atti e convenzioni internazionali. A. BARBERA, *Art. 2*, cit., p. 66.

[114] Corte Europea dei Diritti dell'Uomo, *Pretty v. United Kingdom*, 29 aprile 2002, ric. n. 2346/02.

[115] Corte Europea dei Diritti dell'Uomo, *Niemietz v. Germany*, 16 dicembre 1992, ric. n. 13710/88. Si veda anche S. BARTOLE, P. DE SENA, V. ZAGREBELSKY (a cura di), *Art. 8. Commentario breve alla Convenzione Europea dei Diritti dell'Uomo*, Padova, 2012, p. 297 ss.

[116] In quest'ambito, l'art. 8 CEDU va interpretato alla luce della Convenzione del Consiglio d'Europa del 1981 sulla protezione delle persone rispetto al trattamento automatizzato dei dati personali, che all'art. 2, lett. a) definisce dato personale «ogni informazione concernente una persona fisica identificata o identificabile». La stessa Corte di Strasburgo ha precisato poi che il diritto alla protezione dei dati personali costituisce un'applicazione settoriale del diritto al rispetto della vita privata e che l'ingerenza in quest'ultima si realizza già al momento della memorizzazione dei dati, anche se ottenuti grazie all'osservazione di comportamenti tenuti in pubblico. Corte europea dei diritti dell'uomo, *Perry v. United Kingdom*, 17 luglio 2003, ric. n. 63737/00; Corte europea dei diritti dell'uomo, *Rotaru v. Romania*, 4 maggio 2000, ric. n. 28341/95; Corte europea dei diritti dell'uomo, *Amann v. Switzerland*, 16 febbraio 2000, ric. n. 27798/95. Cfr. S. ALLEGREZZA, *Giustizia penale e diritto all'autodeterminazione dei dati personali nella regione Europa*, in D. NEGRI (a cura di), *Protezione dei dati*, cit., p. 65 ss.; G. TIBERI, *Il diritto alla protezione dei dati personali nelle carte e nelle corti sovranazionali (in attesa del Trattato di Lisbona) (I parte)*, in *Cass. pen.*, 2009, p. 4479 ss.

La stessa Corte di Strasburgo evita di dare una definizione di vita privata ma, seguendo un approccio "in negativo"[117] e casistico, si impegna a qualificare le possibili interferenze nel suddetto diritto, fornendone quindi un'interpretazione aperta ed evolutiva. Intercettazioni telefoniche[118], acquisizione dei tabulati[119], intercettazione di *e-mail* e di comunicazioni via *Internet*[120], sorveglianza via *GPS*[121] costituiscono ingerenze nell'art. 8 CEDU.

Tale norma non si limita a sancire il diritto al rispetto della vita privata, ma individua anche le condizioni che devono sussistere affinché un'intromissione da parte della pubblica autorità nell'esercizio dello stesso sia legittima. Si deve trattare di un'ingerenza prevista dalla legge, che costituisca «una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la sicurezza pubblica, 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, per la protezione dei diritti e delle libertà degli altri» (art. 8, par. 2 CEDU)[122].

Affinché un'attività d'indagine sia considerata «prevista dalla legge», occorre, secondo la Corte di Strasburgo, che essa abbia una base nel diritto interno – di creazione legislativa o giurisprudenziale - sia conoscibile dall'interessato e, soprattutto, che questi sia in grado di prevedere le conseguenze derivanti dall'applicazione della misura nei suoi confronti.

Quanto agli interessi a tutela dei quali si possono giustificare limitazioni della vita privata, essi costituiscono sì un elenco tassativo, ma sono al tempo stesso sufficientemente generici da richiedere un'opera di definizione e specificazione. Tale compito è assunto dalla Corte di Strasburgo che opera un costante bilanciamento del diritto alla protezione della vita privata con le esigenze di cui al secondo comma dell'art. 8 CEDU[123]. Le autorità nazionali godono comunque di un margine di

[117] Così, V. ZENO ZENCOVIC, sub *Art. 8*, in S. BARTOLE, B. CONFORTI, G. RAIMONDI (a cura di), *Commentario alla Convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2011, p. 309.
[118] Corte Europea dei Diritti dell'Uomo, *Klass v. Germany*, 6 settembre 1978, ric. n. 5029/71.
[119] Corte Europea dei Diritti dell'Uomo, *Malone v. United Kingdom*, 2 agosto 1984, ric. n. 8691/79.
[120] Corte Europea dei Diritti dell'Uomo, *Copland v. United Kingdom*, 3 aprile 2007, ric. n. 62617/00.
[121] Corte Europea dei Diritti dell'Uomo, *Uzun v. Germany*, 2 settembre 2010, ric. n. 35623/05. *Infra*, capitolo III, par. 2.2 ss.
[122] L'ingerenza, per essere compatibile con la Convenzione deve rispondere a un «bisogno sociale imperativo» ed essere proporzionata al perseguimento di uno scopo legittimo. Corte europea dei diritti dell'uomo, *Leander v. Sweden*, 26 marzo 1987, ric. n. 9248/81.
[123] G. TIBERI, *Il diritto alla protezione dei dati*, cit., p. 4477.

apprezzamento nell'individuare il punto di equilibrio fra obiettivi pubblici e interessi privati tra loro concorrenti. Margine di discrezionalità che diviene particolarmente ampio con riferimento al processo penale, soprattutto per quanto riguarda la tutela offerta all'autodeterminazione sui dati personali. Infatti, assicurare l'effettività della giustizia penale è considerato dalla Corte un compito essenziale dello Stato, che giustifica la compressione delle garanzie individuali in misura maggiore di quanto accada in altri ambiti[124].

Poiché la nozione di vita privata fatta propria dall'art. 8 CEDU e dalla giurisprudenza di Strasburgo è particolarmente ampia, tale norma si presta a fungere da baluardo nei confronti di diverse attività di indagine. A seconda, tuttavia, dell'intensità dell'ingerenza nel suddetto diritto, la Corte EDU tollera una maggiore discrezionalità del legislatore nazionale nel fissare i requisiti del singolo mezzo di ricerca della prova[125].

3.1 Valore della CEDU nell'ordinamento interno

La Convenzione Europea dei Diritti dell'Uomo e delle Libertà Fondamentali, in quanto trattato internazionale, è stata ratificata ed eseguita con legge ordinaria (L. 4 agosto 1955, n. 848). Fin dal suo recepimento si è tuttavia posta la questione del suo valore nell'ordinamento interno, poiché è apparso subito chiaro che, pur trattandosi di legge ordinaria, essa conteneva principi e diritti fondamentali, che meritavano di prevalere rispetto a fonti formalmente equiparate. La stessa Corte costituzionale, fin dalle prime pronunce, si è richiamata ai diritti CEDU, in funzione "integratrice" del parametro nel giudizio di costituzionalità[126].

Mossa dall'intento di valorizzare il contenuto "costituzionale" della CEDU, la dottrina ha elaborato diverse teorie, volte a rinvenire nella Costituzione un fondamento del valore superiore di tale Convenzione rispetto a quello della legge ordinaria.

---

[124] S. ALLEGREZZA, *Giustizia penale e diritto all'autodeterminazione*, cit., p. 74.

[125] Così, ad esempio, la disciplina delle intercettazioni deve essere più stringente di quella del c.d. pedinamento satellitare. *Infra*, capitolo III, par. 2.2.

[126] D. TEGA, *L'ordinamento costituzionale italiano e il "sistema" Cedu: accordi e disaccordi*, in V. MANES, V. ZAGREBELSKY, *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Milano, 2011, p. 199.

Si è innanzitutto richiamato l'art. 10 Cost. che, prevedendo l'adeguamento dell'ordinamento interno ai principi di diritto internazionale generalmente riconosciuti, e tra questi al fondamentale *pacta sunt servanda*, influirebbe sulla collocazione gerarchica delle norme di adattamento al diritto pattizio[127].

In secondo luogo, come si è già avuto modo di precisare nella trattazione relativa all'art. 2 Cost., si è individuata in tale norma la clausola di recepimento «di tutti quei diritti inviolabili non esplicitamente previsti dalla Costituzione, ma emergenti dall'evoluzione della coscienza sociale e proclamati in documenti internazionali», tra cui va senz'altro annoverata la CEDU[128].

Partendo dal presupposto che le Carte dei diritti siano trattati stipulati al fine di stabilire «un ordinamento che assicuri la pace e la giustizia fra e Nazioni», si è inoltre ritenuto di rinvenire nell'art. 11 Cost. la copertura costituzionale della CEDU[129].

Infine, dopo la riforma del Titolo V della Costituzione, parte della dottrina ha ravvisato nell'art. 117, comma 1 Cost., in forza del quale «la potestà legislativa è esercitata […] nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali», il fondamento della copertura costituzionale della CEDU, a cui sarebbe così garantita una particolare capacità di resistenza all'abrogazione. Nel caso in cui vi dovesse essere un conflitto tra una norma interna e la Convenzione, esso andrebbe risolto dalla Corte costituzionale alla luce dell'art. 117, comma 1 Cost., utilizzando come norme interposte quelle della CEDU[130].

Quest'ultima interpretazione è stata accolta dalla Corte costituzionale nelle note sentenze "gemelle" del 2007, laddove si afferma che «*con l'art. 117, comma 1 Cost. si è realizzato un rinvio mobile alla norma convenzionale di volta in volta conferente, la quale dà vita e contenuto a quegli obblighi internazionali*

[127] R. QUADRI, *Diritto internazionale pubblico*, Napoli, 1968, p. 68 ss.; P. BARILE, *Rapporti tra norme primarie comunitarie e norme costituzionali e primarie italiane*, in *La comunità internazionale*, 1966, p. 15 ss.
[128] A. BARBERA, *Art. 2*, cit., p. 66; F. BRICOLA, *Prospettive e limiti*, cit., p. 1097 ss. *Supra*, par. 2.1 (nota 113).
[129] P. MORI, *Convenzione europea dei diritti dell'uomo, Patto delle Nazioni unite e Costituzione italiana*, in *Riv. dir. int.*, 1983, p. 306 ss.
[130] A. BARBERA, *Le tre Corti e la tutela multilivello dei diritti*, in P. BILANCIA, E. DE MARCO (a cura di), *La tutela multilivello dei diritti. Punti di crisi, problemi aperti, momenti di stabilizzazione*, Milano, 2004, p. 89 ss.; B. CONFORTI, *Sulle recenti modifiche della Costituzione italiana in tema di rispetto degli obblighi internazionali comunitari*, in *Foro it.*, 2002, V, c. 229 ss.

genericamente evocati». I diritti fondamentali riconosciuti dalla CEDU, nell'interpretazione fornita dalla Corte di Strasburgo, costituiscono dunque norme interposte nel giudizio di legittimità costituzionale del diritto interno, soggette a loro volta ad una verifica di compatibilità con le norme della Costituzione. Infatti, diversamente da quanto accade per il diritto dell'Unione europea, di cui la Corte riconosce il primato sul diritto interno con conseguente obbligo di disapplicazione delle norme interne contrastanti da parte dei singoli giudici, l'eventuale contrasto con una norma della Convenzione «*non gener[a] problemi di successione delle leggi nel tempo o valutazioni sulla rispettiva collocazione gerarchica delle norme in contrasto, ma questioni di legittimità costituzionale*», che devono essere risolte dal giudice delle leggi[131].

La Corte costituzionale ha mantenuto ferma tale sua impostazione anche dopo l'entrata in vigore del Trattato di Lisbona che, come noto, prevede l'adesione dell'Unione europea alla CEDU, che entra così a far parte dei principi generali del diritto dell'Unione (art. 6 TUE)[132]. Infatti, a prescindere dalla circostanza che tale adesione non è ancora avvenuta, la Corte sottolinea come in ogni caso i principi fondamentali, in quanto diritto dell'Unione, sono soggetti al principio di attribuzione, in base al quale è disciplinata la distribuzione delle competenze tra Unione e Stati membri[133].

Nonostante la mancanza di effetto diretto[134], si può affermare che il diritto alla riservatezza trovi oggi il suo fondamento nell'art. 8 CEDU che, per il tramite

[131] C. cost., 24 ottobre 2007, n. 348, in *Giur. cost.*, 2007, p. 3475, con nota di C. PINELLI, *Sul trattamento giurisdizionale della CEDU e delle leggi con essa confliggenti*; C. cost., 24 ottobre 2007, n. 349, *ivi*, 2007, p. 3535, con nota di M. CARTABIA, *Le sentenze "gemelle": diritti fondamentali, fonti, giudici*.

[132] C. cost., 11 marzo 2011, n. 80, in *Giur. cost.*, 2011, p. 1224 ss.

[133] Ciò che giustificherebbe la diversa giustiziabilità negli Stati membri dei diritti della Carta rispetto a quelli della CEDU "comunitarizzati" sarebbe il fatto che questi ultimi non sono recepiti automaticamente nel diritto dell'Unione, ma presuppongono un'opera di interpretazione e precisazione da parte della Corte di Giustizia. Fino a quel momento, non se ne potrebbe quindi predicare una diretta applicabilità. Così, C. SOTIS, *Convenzione europea dei diritti dell'uomo e diritto comunitario*, in V. MANES, V. ZAGREBELSKY, *La Convenzione europea dei diritti dell'uomo*, cit., p. 110 ss., in particolare, p. 144.

[134] La mancanza dell'effetto di diretta disapplicazione del diritto interno, comporta semplicemente che eventuali contrasti debbano essere risolti dalla Corte costituzionale, adita dal giudice *a quo*, nel caso in cui non sia possibile un'interpretazione convenzionalmente conforme. In questo modo non viene, quindi «mortificato l'operato dei giudici ordinari né tanto meno [essi vengono] emargina[ti] dal sistema "multilivello" della tutela dei diritti fondamentali». Così, M. CARTABIA, *La convenzione europea dei diritti dell'uomo e l'ordinamento italiano*, in A. BALSAMO, R. E. KOSTORIS (a cura di), *Giurisprudenza europea*, cit., p. 54.

dell'art. 117, comma 1 Cost., acquista rango di diritto fondamentale[135]. Questa impostazione, a differenza di quella che ravvisa la fonte di tale diritto nell'art. 2 Cost., ha il pregio di consentire di individuare altresì limiti e presupposti dell'ingerenza da parte della pubblica autorità. Essa dovrà, infatti, rispettare le condizioni previste dal secondo comma dell'art. 8 CEDU.

4. Diritto alla vita privata e alla tutela dei dati personali nella Carta dei Diritti Fondamentali dell'Unione Europea

È espressione ricorrente che la tutela dei diritti fondamentali sia oggi assicurata da un sistema integrato di protezione che si articola su tre livelli: quello nazionale, quello internazionale e quello comunitario (c.d. sistema multilivello). Dopo aver esaminato le disposizioni della Costituzione e della CEDU, non resta ora che fare riferimento alla Carta dei Diritti Fondamentali dell'Unione Europea (d'ora innanzi CDFUE).

Il Trattato di Lisbona ha attribuito alla CDFUE lo stesso valore giuridico dei Trattati, ossia efficacia vincolante per gli Stati membri, seppur nelle sole materie di competenza dell'Unione (art. 6 TUE)[136].

Le norme che vengono in rilievo, ai fini che qui interessano, sono gli articoli 7 e 8 della Carta che tutelano rispettivamente il diritto al rispetto della vita privata e familiare, del domicilio e delle comunicazioni, e il diritto alla protezione dei dati personali. Particolarmente significativa è la circostanza che la Carta, proclamata a Nizza nel 2000, preveda due distinte norme per la tutela della riservatezza e per l'autodeterminazione sui propri dati personali. Ciò è infatti emblematico della maturata consapevolezza circa le nuove dimensioni della *privacy*. Ci si avvede dunque della necessità di dare autonoma rilevanza a quel *right to control of the information about oneself*, già considerato componente essenziale della *privacy*. Tanto è vero che lo stesso Trattato di Lisbona introduce un'apposita base giuridica

[135] Cfr., R. ORLANDI, *Strafverfolgende oder vorbeugende Überwachung des Fernmeldeverkehrs und die Privatsphäre, Einsatz technischer Mittel, online Durchsuchung und das Recht auf informelle Selbstbestimmung*, *Congress on the Criminal Law Reforms in the World and in Turkey, atti del convegno internazionale svoltosi a Istanbul-Ankara dal 26 maggio al 4 giugno 2010, Istanbul 2010*, p. 23 ss. in particolare, p. 30, 31.

[136] Tale norma precisa, infatti, al secondo comma che «le disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati».

per l'azione dell'Unione a tutela del diritto alla protezione dei dati personali (art. 16, comma 2 TFUE)[137].

Ai sensi dell'art. 52, comma 1 CDFUE «eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta 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 terzo comma, inoltre, prevede che «laddove la […] Carta contenga diritti corrispondenti a quelli garantiti dalla [CEDU], il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione» (c.d. clausola di equivalenza). E quindi, gli articoli 7 e 8 CDFUE vanno riempiti di significato alla luce dell'art. 8 CEDU e della relativa giurisprudenza della Corte di Strasburgo, soprattutto per quanto riguarda i presupposti di un'ingerenza legittima negli stessi da parte della pubblica autorità. Ciò tuttavia ancora non significa che il diritto CEDU trovi diretta applicazione negli Stati membri, come accade per le norme della CDFUE che hanno lo stesso valore giuridico dei Trattati. Infatti, la Carta rimane soggetta al sindacato della Corte di Giustizia, che potrà eventualmente operare un diverso bilanciamento degli interessi in gioco[138]. A tal proposito si segnala che, in una recente sentenza in materia di tutela dei diritti d'autore in *Internet*, la Corte di Giustizia facendo proprie le conclusioni dell'avvocato generale, Pedro Cruz Villalòn, ha ribadito l'equivalenza tra art. 8 CEDU e artt. 7 e 8 CDFUE[139].

[137] Tale norma, dopo aver ribadito l'esistenza di un diritto alla protezione dei dati personali, meritevole di tutela, prevede che «il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti». Sul punto si avrà modo di tornare nel prosieguo della trattazione. V. *Infra*, capitolo IV, par. 4 ss.

[138] C. SOTIS, *Convenzione europea*, cit., p. 144.

[139] Corte di Giustizia dell'Unione Europea, 24 novembre 2011 (C-70/10). La Corte ha, infatti, affermato che l'ingiunzione diretta, da parte di un giudice ad un *service provider*, di adottare sistemi di filtro per impedire agli utenti di utilizzare sistemi di *file sharing*, in violazione delle norme in materia di diritto d'autore, comprime in modo sproporzionato i diritti e le libertà tutelati dagli artt. 8 e 11 della CDFUE e dai corrispondenti artt. 8 e 10 della CEDU. Così, R. FLOR, *Lotta alla "criminalità informatica"*, cit. Analoga una sentenza di poco successiva, Corte di Giustizia dell'Unione Europea, 16 febbraio 2012, C 360/10, caso "*SABAM v. Netlog*".

Ciò acquista particolare significato nell'ambito delle indagini informatiche e via *Internet*, dove diviene di fondamentale importanza la valorizzazione del diritto alla tutela dei dati personali, quale filiazione del diritto al rispetto della vita privata. La circostanza che la Corte di Giustizia abbia ricondotto l'art. 8 CDFUE all'art. 8 CEDU fa sì che eventuali ingerenze nel diritto alla tutela dei propri dati personali dovranno essere caratterizzate dal perseguimento di uno scopo legittimo ed essere proporzionate, ossia opportune, idonee e necessarie al suo raggiungimento[140].

Tuttavia, la circostanza che gli articoli 7 e 8 CDFUE, in quanto filiazione dell'art. 8 CEDU, siano tra loro intimamente connessi tanto da integrare un «diritto alla vita privata con riguardo al trattamento dei dati personali»[141], non deve tradursi in una mancata valorizzazione delle differenze. La distinzione in due diverse disposizioni del diritto alla vita privata e di quello alla tutela dei dati personali, infatti, si fa particolarmente apprezzare nell'ambito degli obblighi di *data retention*. Come recentemente messo in luce dall'avvocato generale, Pedro Cruz Villalòn, il legame tra le due norme dipende dal tipo di dati personali che vengono in considerazione[142]. Esistono infatti, «dati personali in quanto tali», come le generalità, e «dati più che personali», ossia quelli che si riferiscono alla riservatezza della vita privata. Con riferimento ai primi, si pone il problema di garantire all'interessato il controllo sulle modalità del trattamento – comunicazione dello scopo della rilevazione, diritto di accesso, di seguito e di cancellazione, etc. – . Per essi l'art. 8 della Carta costituisce una garanzia adeguata. Quanto ai secondi, invece, l'esigenza di tutela riguarda la circostanza che aspetti variegati della vita di una persona si siano tradotti in dati, suscettibili di trattamento informatico. Il rischio in questo caso è che, attraverso la raccolta di tali dati, si ricostruiscano profili della personalità. Sapere con chi una persona comunichi, dove si trovava in un determinato momento, quali siti *Internet* ha visitato negli ultimi due anni, costituisce senza dubbio un'ingerenza nel suo diritto alla riservatezza della vita privata. Pur considerando che tali dati verranno

[140] Non va dimenticato che ai sensi dell'art. 6 TUE la Carta dei diritti fondamentali dell'Unione Europea ha lo stesso valore giuridico dei Trattati, e quindi è direttamente applicabile ed azionabile negli Stati membri.
[141] Corte di Giustizia dell'Unione Europea, 9 novembre 2010, *Volker und Markus Schecke e Eifert,* C-92/09 e C-93/09.
[142] Conclusioni dell'Avvocato Generale, Pedro Cruz Villalòn, presentate il 12 dicembre 2013, nelle cause riunite C-293/12, *Digital Rights Ireland Ltd contro The Minister for Communications, Marine and Natural Resources e altri* e C-594/12, *Kärntner Landesregierung Michael Seitlinger* e *Christof Tschohl*, in *www.curia.europa.eu*.

acquisiti solo se necessari per la repressione di reati gravi, resta il fatto che essi vengono conservati per un apprezzabile lasso di tempo, ingenerando nei cittadini dell'Unione una sensazione di permanente controllo.

Pertanto, la direttiva 2006/24/CE (c.d. *data retention*) costituisce un'interferenza nel diritto alla vita privata (art. 7 CDFUE) e non in quello alla tutela dei dati personali (art. 8 CDFUE)[143].

Costituendo una «limitazione all'esercizio di diritti e libertà riconosciti dalla […] Carta», la direttiva *data retention* deve quindi rispettare le prescrizioni di cui all'art. 52, comma 1 CDFUE, il quale stabilisce che eventuali intromissioni debbano essere previste dalla legge, rispettare il nucleo essenziale dei diritti ed essere proporzionate all'obiettivo da raggiungere, corrispondente o a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Che una direttiva possa essere ascritta al concetto di «legge», non pare potersi dubitare[144]. Ciò che occorre valutare è se si tratti di un atto che indichi in maniera sufficientemente chiara i presupposti della limitazione del diritto fondamentale coinvolto. Trattandosi di una direttiva, spetterà agli Stati membri, nell'ambito della discrezionalità loro riconosciuta, specificare le garanzie che devono accompagnare simile limitazione; tuttavia, compito dell'Unione è quello di individuare i principi-quadro[145]. In quest'ottica, un obbligo di conservazione fino a due anni appare sproporzionato rispetto all'esigenza da soddisfare[146].

---

[143] Secondo l'avvocato generale, «posto che la «sfera privata» costituisce il nocciolo della «sfera personale», non si può escludere che una normativa che restringa il diritto alla protezione dei dati di carattere personale in conformità all'art. 8 della Carta, possa nondimeno essere considerata come recante una lesione sproporzionata dell'art. 7 della Carta». La gravità dell'ingerenza nel diritto al rispetto della vita privata dipenderebbe poi, da un lato dall'importanza che i mezzi di comunicazione, anche informatica, hanno acquisito nella società moderna, e dall'altro dalla circostanza che i dati sono conservati ad opera di soggetti privati, ciò che aumenta il rischio di usi per scopi illeciti. L'art. 8 non sarebbe invece violato perché la direttiva esplicitamente prevede il rispetto della direttiva 95/46/CE (c.d. direttiva madre), della direttiva 2002/58/CE (c.d. *e-privacy*) e della Convenzione del Consiglio d'Europa del 1981 (*consideranda* 15 e 20).

[144] Sull'interpretazione del requisito «prevista dalla legge», l'avvocato generale si richiama, infatti, alla giurisprudenza di Strasburgo, in forza della quale occorre andare oltre un criterio puramente formale, e considerare se, nella sostanza, si tratti di un atto che indichi i presupposti e le garanzie per la limitazione di un diritto fondamentale.

[145] Il legislatore dell'Unione avrebbe dovuto individuare i reati per il perseguimento dei quali si giustifica il ricorso ai dati di traffico, e non limitarsi alla clausola «reati gravi». Inoltre, avrebbe dovuto introdurre il principio dell'obbligo per le autorità nazionali autorizzate ad accedere ai dati di cancellarli una volta utilizzati e di informare le persone interessate di tale accesso, quantomeno a posteriori, una volta eliminato il rischio che tale informazione possa pregiudicare l'efficacia delle

5. Verso la creazione di nuovi diritti

L'esplosione di *Internet* e dei nuovi prodotti tecnologici (*smartphones*, *tablets*, etc.) ha determinato una rivoluzione nel modo di comunicare, e più in generale nelle relazioni sociali, sempre più affidate al mondo virtuale. Ciò espone la vita privata dei singoli a sempre maggiori pericoli di intromissione.

I *tradizionali* diritti fondamentali, nati come baluardo del singolo di fronte ad ingerenze da parte dei pubblici poteri, mostrano i loro limiti. Pur se interpretati estensivamente, essi si rivelano inadeguati a fornire adeguata protezione al bisogno di *riservatezza* dell'utente della rete[147]. Lo stesso può dirsi per diritti di nuova generazione, come i diritti di *privacy*, tra cui quello alla c.d. autodeterminazione informativa. È, infatti, sicuramente meritevole di tutela l'esigenza di controllo sul trattamento dei propri dati personali, ma prima ancora si avverte la necessità di inibire l'accesso a determinate informazioni. Informazioni che, nel mondo 2.0 sono salvate sul *computer* o nella rete, che divengono dunque strumenti attraverso cui si sviluppa la personalità, meritevoli di protezione costituzionale. Riacquista quindi centralità quella sfera di privatezza che costituisce il nucleo primigenio della *privacy*, che va tuttavia calata nel contesto dell'informatica e delle tecnologie.

Di ciò è ben consapevole il *Bundesverfassungsgericht* (d'ora innanzi *BVerfG*), che in una recente sentenza ha coniato un nuovo diritto della personalità, il diritto alla garanzia della riservatezza e integrità del sistema informatico.

---

misure che giustificano l'impiego dei dati di cui trattasi. Così, l'avvocato generale nelle sue conclusioni.

[146] Secondo l'avvocato generale, infatti, la durata della conservazione dei dati (*data retention*), incide sull'intensità dell'ingerenza nella vita privata ed appare sproporzionata rispetto all'esigenza di repressione dei reati cui è preordinata. Ciò anche in considerazione della possibilità di fare ricorso a forme di *data preservation*, o *quick freeze*, ossia alla conservazione di dati a posteriori. Esse rappresentano, infatti, una limitazione minore della vita privata in quanto consistono nella conservazione di dati di soggetti determinati e quanto meno sospettati di aver commesso un reato. Il problema che si pone quindi non è quello di accertare se, al fine della repressione di gravi reati, un periodo più lungo di conservazione e di messa a disposizione dei dati sia preferibile rispetto ad un periodo più breve, bensì se ciò, nell'ottica della proporzionalità, sia necessario. Infatti, la conservazione di dati «in luoghi imprecisati del *cyberspazio* tende sempre ad essere percepita come un'anomalia, a prescindere dalla sua durata, […] e quindi dovrebbe avvenire solo in considerazione di altri imperativi della vita sociale. […] Trattandosi quindi di una situazione eccezionale, essa non può perdurare oltre quanto strettamente necessario». Cfr. conclusioni dell'avvocato generale Pedro Cruz Villalòn del 12 dicembre 2013, cit. Sul tema si avrà modo di tornare approfonditamente nel prosieguo della trattazione, *infra*, capitolo II, par. 7 ss. e capitolo IV, par. 4.1.

[147] Basti pensare al c.d. *cloud computing* che consente di memorizzare, archiviare ed elaborare dati, delocalizzati in rete.

La giurisprudenza della Corte costituzionale tedesca costituisce un esempio particolarmente istruttivo di come il diritto, mediante l'elaborazione di principi (*rectius*: diritti fondamentali), riesca a non soccombere di fronte all'evoluzione tecnologica e a fornire ai singoli tutela nei confronti di nuove forme di limitazione dei loro diritti fondamentali. Inoltre, le sentenze del *BVerfG*, e il riferimento in particolare è a quella sul censimento del 1983 e alla più recente relativa alle perquisizioni *online*, svolgono l'importante funzione di sensibilizzare l'opinione pubblica circa i pericoli derivanti dalle nuove tecnologie.

*5.1 L'esperienza tedesca: dall'*informationellen Selbstbestimmungsrecht *al* Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Nell'ordinamento tedesco esiste un unico diritto della personalità - *allgemeines Persönlichkeitsrecht* – che affonda le proprie radici nella tutela riconosciuta dal *Grundgesetz* alla dignità umana (art. 1, comma 1) e al libero sviluppo della personalità (art. 2, comma 1). Secondo l'interpretazione che ne dà il *BVerfG*, codesto diritto ha diverse espressioni o manifestazioni, elaborate per far fronte alle sfide lanciate dall'evoluzione tecnologica. Nel suo nucleo essenziale, l'*allgemeine Persönlichkeitsrecht* tutela gli aspetti strettamente personali della vita umana, necessari per la sua realizzazione libera e consapevole. La c.d. teoria delle sfere (*Sphärentheorie*), cui già si è fatto riferimento[148], è stata elaborata dal *BVerfG* proprio nell'ambito del generale diritto della personalità. A seconda del grado di intimità delle informazioni, il diritto della personalità oppone una resistenza più o meno maggiore a forme di intromissione da parte dei pubblici poteri. La sfera intima (*Geheimnisphäre* o *Intimsphäre*) costituisce il nocciolo duro, il nucleo inviolabile dell'*allgemeinen Persönlichkeitsrecht* (*unantastbarer Bereich privater Lebensgestaltung*).

La *Sphärentheorie* e l'esistenza di un unico diritto della personalità hanno permesso di dare al *right to be let alone*, già elaborato negli Stati Uniti, un solido fondamento costituzionale nell'ordinamento tedesco. Anche il *Recht an der eigenen*

[148] *Supra*, par. 2.

Privatsphäre trova quindi fondamento e tutela nel combinato disposto degli artt. 1, comma 1 e 2, comma 1 GG[149].

La teoria delle sfere viene abbandonata nella storica sentenza sul censimento del 1983[150]. Il contesto tecnologico è infatti mutato, la raccolta e il trattamento dei dati personali sono più rapidi e quindi più insidiosi. Nessun dato può essere considerato innocuo, perché è possibile intrecciarlo con altri dati e ottenere così profili della personalità. La *privacy* acquista una dimensione collettiva[151]. La Corte costituzionale tedesca si mostra consapevole degli effetti negativi che ciò può avere per lo sviluppo della personalità. Non avere il controllo sui propri dati personali[152] e sulla loro circolazione, può indurre gli individui a limitare la propria azione, può inibire determinati comportamenti. La tutela della dignità umana, secondo il *BVerfG* comprende anche il diritto di ogni persona di poter disporre liberamente e consapevolmente delle notizie e informazioni relative alla propria vita privata. Di qui la creazione dell'*informationelle Selbstbestimmungsrecht*, elaborato a partire dagli artt. 1, comma 1 e 2, comma 1 *GG*.

Tale diritto, tuttavia, non è protetto in maniera assoluta. Esso va infatti bilanciato con altre esigenze, anch'esse di rango costituzionale. Innanzitutto, eventuali limitazioni potranno essere disposte solo attraverso norme di legge, che rispettino i principi di chiarezza e determinatezza, e perseguano uno scopo legittimo. Inoltre, la legge che limiti l'*informationelle Selbstbestimmungsrecht* è a sua volta soggetta a limiti (c.d. *Schranken-Schranken*): deve rispettare il principio di proporzionalità e la tutela del nucleo essenziale della vita privata. Infatti, il *BVerfG*

[149] Questi principi sono stati applicati dal *BVerfG* nella sentenza sul microcensimento del 16 luglio 1969 (*BVerfGE*, 27, 1 ss.). In tale decisione, la Corte ammette che il riconoscimento di una sfera intima, separata dal mondo esterno, nella quale si possa godere del diritto alla solitudine, rappresenta il presupposto della tutela della dignità umana e dello sviluppo della personalità. Tuttavia, il *BVerfG* ritiene che la raccolta, e il trattamento in forma anonima, di dati che riguardano l'agire del singolo nel mondo esterno (si trattava di domande sulle abitudini vacanziere degli intervistati), non ledano tale sfera intima. Pertanto, la Corte salva la legge impugnata dalla declaratoria di incostituzionalità.

[150] *Volkszählungsurteil* del 15 dicembre 1983, *BVerfGE* 65, 1 ss. In generale sull'informationellen Selbstbestimmungsrecht si veda P. H., BULL, *Informationelle Selbstbestimmung – Vision oder Illusion?,* Tübingen*, 2. Auflage*, 2011; F. RIEPL, *Informationelle Selbstbestimmung im Strafverfahren*, Tübingen, 1998.

[151] *Supra*, par. 2.

[152] Non si distingue più tra dati intimi e dati sociali, ma si adotta la nozione onnicomprensiva di dati personali. Ciò che rileva non è tanto l'appartenenza di un'informazione ad una determinata sfera della personalità piuttosto che ad un'altra, quanto il contesto di utilizzazione. Cfr. M. P. ADDIS, *Diritto all'autodeterminazione informativa e processo penale in Germania*, in D. NEGRI (a cura di), *Protezione dei dati personali*, cit., p. 87 ss., in particolare p. 96.

nella sua giurisprudenza afferma costantemente l'esistenza di un nocciolo duro alla base di ogni diritto, assolutamente inviolabile, escluso da ogni bilanciamento. Per quanto riguarda invece il giudizio di proporzionalità, il relativo *test* si compone di tre fasi o giudizi: idoneità (*Geeignetheit*), necessità (*Erforderlichkeit*) e proporzionalità in senso stretto (*Angemessenheit* o *Verhältnismäßigkeit im engeren Sinne*)[153]. La misura limitativa del diritto fondamentale deve essere quindi idonea al raggiungimento dell'obiettivo, legittimo, preventivamente individuato e tale da comportare il minor sacrificio possibile per l'individuo. La proporzionalità in senso stretto, componente più caratteristica e penetrante del principio, va messa in relazione con quel nucleo essenziale di ogni diritto fondamentale (*Wesensgehalt*) che sfugge ad ogni opera di bilanciamento. Si tratta quindi di un giudizio di valore, di un «criterio essenzialmente politico»[154], che può inibire l'azione dei pubblici poteri, volta al perseguimento dell'interesse collettivo, qualora essa determini un sacrificio intollerabile della sfera giuridica dell'interessato[155].

Con specifico riferimento al processo penale, il principio di proporzionalità si traduce nell'esigenza di *proporzione* tra gravità del reato da accertare e grado di invasività della misura investigativa che si intende adottare e, quindi, in un bilanciamento tra interesse pubblico alla repressione dei reati e diritti fondamentali della persona. Tale accertamento deve essere fatto in un primo momento, a livello astratto, ad opera del legislatore, e successivamente, in concreto, dal giudice che applica la misura. Evidentemente, più una misura investigativa si intromette in forme elementari di manifestazione della libertà d'azione dell'uomo, più i presupposti della sua legittimità dovranno essere stringenti.

---

[153] Il principio di proporzionalità deriva dal principio dello Stato di diritto (*Rechtstaatsprinzip*), sancito dall'art. 20 *GG*.

[154] La valutazione di idoneità poggia invece su un criterio di idoneità pratica, e quella di necessità si presenta come un criterio misto di razionalità pratica e opportunità politica. Così, R. ORLANDI, *Garanzie individuali ed esigenze repressive (ragionando intorno al diritto di difesa nei procedimenti di criminalità organizzata)*, in AA. VV., *Studi in ricordo di Giandomenico Pisapia, Vol. II*, Milano, 2000, p. 545 ss., in particolare pag. 560.

[155] D. U. GALETTA, *Principio di proporzionalità e sindacato giurisdizionale nel diritto amministrativo*, Milano, 1998, p. 19. Il *BVerfG* segue un approccio c.d. a livelli del *test* di proporzionalità: più un'intromissione legislativa riguarda forme elementari di manifestazione della libertà d'azione dell'uomo, più occorre fare attenzione nel bilanciare la giustificazione di tale intromissione con il diritto di libertà dei cittadini. Cfr. *BVerfG*, 7 aprile 1964, *BVerfGE* 17, 306; L. DRALLÈ, *Das Grundrecht auf Gewährleistung*, cit., p. 23

In merito alle rilevazioni di informazioni, la Corte costituzionale tedesca chiarisce ulteriormente che un'eventuale legge dovrebbe individuare preventivamente lo scopo della rilevazione, a cui poi ogni ulteriore trattamento dei dati sarà vincolato, salva una ulteriore previsione normativa (*Zweckbindung*). Tale scopo dovrà essere reso noto all'interessato, in modo da garantirgli un potere di controllo effettivo. Sulla raccolta e sul trattamento delle informazioni dovrebbero vigilare autorità indipendenti; gli addetti al trattamento dovrebbero rispettare l'obbligo al segreto d'ufficio; all'interessato deve essere riconosciuto il diritto di chiedere chiarimenti sul trattamento e di ottenere la cancellazione dei dati.

Alla luce di queste premesse, il *BVerfG* dichiara illegittima l'allora vigente legge sul censimento.

L'ulteriore sviluppo tecnologico che ha caratterizzato il nuovo millennio ha fatto riemergere con forza quell'esigenza di riservatezza sui dati personali salvati in dispositivi informatici di nuova generazione o in rete. Prima ancora del bisogno di controllare l'utilizzo e la circolazione delle *information about oneself*, si avverte la necessità di impedire l'apprensione di quelle informazioni.

L'introduzione nella Legge sulla protezione della Costituzione del *Land Nord Rhein Westfalen* di uno strumento di indagine che consentiva l'infiltrazione segreta in un sistema informatico (c.d. perquisizione *online*), ha costituito l'occasione per la Corte costituzionale tedesca di pronunciarsi in merito alla tensione tra simile bisogno di riservatezza e le esigenze investigative[156].

Il *BVerfG* riconosce l'importanza che oggi hanno acquisito i dispositivi informatici come strumenti di sviluppo della personalità. Così come il domicilio è tutelato in quanto proiezione spaziale della persona, luogo in cui essa svolge la propria vita privata lontano da occhi indiscreti, analogamente i "luoghi" *informatici* o *virtuali* in cui sono salvati dati personali, meritano protezione costituzionale. A tal fine, tuttavia, i diritti fondamentali già esistenti si rivelano inadeguati.

Occorre infatti considerare che il sistema informatico è un sistema complesso, che contiene una moltitudine diversificata di dati personali e che non è ancora possibile un accesso selettivo al dispositivo tecnologico. Pertanto, l'intromissione in un sistema informatico consente di apprendere dati di ogni tipo e di venire a

[156] *BVerfG*, 27 febbraio 2008, *BVerfGE* 120, 274 ss., reperibile anche all'indirizzo *www.bundesverfassungsgericht.de*. *Infra*, capitolo III, par. 4.1.

conoscenza di aspetti della vita di un individuo e farsi un'idea della sua personalità[157].

Ciò rende la tutela offerta dall'*informationelle Selbstbestimmungsrecht* insufficiente. Il bene protetto è in verità lo stesso, ossia i dati personali, tuttavia, come mette in luce la Corte costituzionale, l'intromissione in un sistema informatico è qualitativamente differente rispetto ad una singola rilevazione di informazioni. Il diritto all'autodeterminazione informativa è sì una derivazione della tutela della sfera privata, ma nel contesto tecnologico odierno non è più possibile distinguere tra sfere[158], non ci sono più dati intimi e dati "sociali", anche il dato più innocuo, affiancato ad altri dati può rivelare informazioni sulla vita di una persona. La promiscuità dei dati e il tipo di intromissione da parte dell'autorità pubblica, fanno sì che il pericolo per il diritto della personalità in generale sia qualitativamente e quantitativamente diverso da quello di una *semplice* raccolta di dati, a cui fa da baluardo il diritto all'autodeterminazione informativa. Si rende quindi necessario tutelare il sistema informatico in quanto contenitore di informazioni che l'interessato intende mantenere riservate, a prescindere dalla natura più o meno intima che essere possano avere.

Anche la tutela che il *Grundgesetz* offre alle comunicazioni (art. 10 *GG*) è inadeguata. Tale norma sancisce l'inviolabilità della segretezza delle comunicazioni, e come tale si applica anche a quelle che avvengono tramite un sistema informatico, ma riguarda solo comunicazioni in corso e non i dati che rimangono salvati sul *computer* dopo che la comunicazione è terminata. Inoltre, non potendosi sapere a priori se si capteranno solo comunicazioni o anche dati di altra natura (cosa che di fatto avverrà sempre), il secondo comma dell'art. 10 *GG*, che individua i presupposti di un'eventuale limitazione di tale diritto, non costituisce una base giuridica adeguata per l'intromissione in un sistema informatico. Tuttavia, l'utilizzo del sistema

[157] Non essendo possibile sapere in anticipo a quali dati si sta accendendo, non potrebbe venire in aiuto la c.d. teoria delle sfere, peraltro già abbandonata dal *BVerfG*.

[158] Per l'idea che non si possa più parlare di sfera privata o individuale, ma di «spazi virtuali di manifestazione della personalità», si veda R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d*. Online Durchsuchung*. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona. Aspetti di diritto penale sostanziale*, in *Riv. trim. dir. pen. ec.*, 2009, p. 697 ss., e in particolare p. 705, su cui *infra*, par. 5.2.

informatico per comunicare, attraverso *e-mail*, *chat* private, *forum* su *Internet*, ricade pur sempre nell'ambito di tutela dell'art. 10, comma 1 *GG*[159].

Nemmeno l'art. 13, comma 1 *GG* è in grado di offrire protezione nei confronti di intromissioni in un sistema informatico. Infatti tale norma, nel garantire l'inviolabilità del domicilio come "ultimo rifugio dell'uomo", tutela indirettamente la dignità umana e il libero sviluppo della personalità, ma l'ambito di tutela è pur sempre legato ad uno spazio fisico, il bene tutelato è la "sfera privata fisica" [160]. L'art. 13 *GG* potrebbe in ipotesi trovare applicazione quando il sistema informatico si trovi all'interno di un luogo di domicilio. Tuttavia, poiché non è possibile stabilire a priori dove si trovi il sistema informatico oggetto di indagine, simile disposizione costituzionale si rivela inadeguata[161].

Il *BVerfG* ritiene pertanto necessario elaborare un nuovo diritto fondamentale, il *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. Codesto nuovo diritto è a sua volta espressione dell'*allgemeine Persönlichkeitsrecht* e affonda le sue radici nella tutela della dignità umana (art. 1, comma 1 *GG*) e del libero sviluppo della personalità (art. 2, comma 1 *GG*)[162].

Oggetto di tutela del c.d. *Computer Grundrecht* sono la riservatezza e l'integrità di un sistema informatico, ossia di un sistema composto di *hardware* e *software*, che serva al rilevamento, alla memorizzazione, al trattamento, alla visualizzazione di informazioni e dati personali[163]. Il sistema informatico non è tutelato in quanto tale,

---

[159] Infatti, il nuovo diritto fondamentale appresta una tutela sussidiaria rispetto a quella garantita dai diritti costituzionali già esistenti, tra cui l'art. 10, comma 1 *GG*.

[160] Ciò non significa che la norma costituzionale tuteli sono nei confronti di intromissioni fisiche nel domicilio. Devono rispettare i presupposti dell'art. 13, commi 2 ss. *GG* anche le intercettazioni ambientali nel domicilio o le videoriprese domiciliari, nonché l'utilizzo di misuratori delle radiazioni elettromagnetiche.

[161] Se il sistema informatico si trova effettivamente all'interno di un luogo definibile come "domicilio", troverà applicazione, in aggiunta alla tutela offerta dal nuovo diritto fondamentale, anche l'art. 13, comma 1 *GG*. In tal senso già, G. HORNUNG, *Die Festplatte als "Wohnung"?*, in *JZ*, 2007, p. 828 ss.

[162] Si tratta di un diritto costituzionale non scritto, frutto di un'interpretazione estensiva di diritti scritti, in questo caso gli artt. 1, comma 1 e 2, comma 1 *GG*. Cfr. L. DRALLÈ, *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, *Lorenz-von-Stein-Institut*, 2010, p. 10 ss. Si veda anche C. GUSY, *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, in *DuD,* 2009, p. 33 ss.;

[163] Anche strumenti di memorizzazione esterni, quali *hard-disk*, penne *USB*, quando collegati ad un sistema informatico, ne sono considerati parte integrante. Sono protetti tutti quei sistemi informatici che «*da soli o attraverso le loro interconnessioni, possono contenere dati della persona interessata che, per le loro caratteristiche e per la loro diversità, possono far sì che l'accesso ad essi si trasformi*

ma in quanto mezzo per lo sviluppo della personalità. Ciò che si vuole garantire è l'interesse dell'utilizzatore a che i dati creati, elaborati e salvati all'interno del sistema informatico, rimangano riservati[164]. Il bene giuridico protetto dal nuovo diritto fondamentale è quindi il libero sviluppo della personalità attraverso la garanzia della riservatezza e dell'integrità del sistema informatico usato dall'interessato.

Come è stato autorevolmente sostenuto, con tale sentenza «il diritto ristabilisce la priorità sull'umano, affermando l'esistenza di una nuova entità, […] costituita dalla persona e dall'apparato tecnico al quale affida i suoi dati. […] Tra l'uomo e la macchina non vi è soltanto interazione, ma compenetrazione, [tra essi] si stabilisce un *continuum* e il diritto, riconoscendolo, ci consegna una nuova antropologia, che reagisce sulle categorie giuridiche e ne modifica la qualità. La riservatezza, qualità dell'umano, si trasferisce alla macchina»[165].

Il diritto fondamentale alla garanzia della riservatezza e integrità dei sistemi informatici non è assoluto; anch'esso può essere limitato, al ricorrere di determinati presupposti, per finalità di indagine o di prevenzione. Presupposti che saranno più o meno rigidi, soprattutto per quanto riguarda il *test* di proporzionalità, a seconda che si tratti di intromissioni segrete (come nel caso delle perquisizioni *online*) o palesi, con fini preventivi o repressivi. Innanzitutto, eventuali intromissioni segrete nel diritto alla garanzia della riservatezza e integrità dei sistemi informatici[166] dovranno essere previste per legge, che a sua volta dovrà rispettare i presupposti di chiarezza e determinatezza, ed essere proporzionata al perseguimento di uno scopo legittimo (in questo caso la prevenzione o repressione dei reati). Inoltre, le misure investigative si giustificheranno se adottate al fine di tutelare beni giuridici particolarmente elevati – la vita, l'integrità fisica, la libertà della persona, nonché beni collettivi la cui minaccia mina i fondamenti o l'esistenza dello Stato o dell'uomo - e dovranno

in un'interferenza in aspetti essenziali del modo di vivere della persona o renda possibile un profilo significativo della personalità», *BVerfGE* 120, 203.

[164] Sono tutelati sia i dati salvati in maniera permanente, sia quelli salvati temporaneamente (nella *RAM*).

[165] Le citazioni sono di S. RODOTÀ*, Il diritto di avere diritti*, Roma-Bari, 2012, p. 317.

[166] Oggetto del ricorso costituzionale erano misure investigative segrete, le c.d. perquisizioni *online*, utilizzate per fini preventivi. A queste fa pertanto riferimento il *BVerfG* nel fissare i presupposti di ammissibilità.

essere adottate dal giudice, o da un soggetto in analoghe condizioni di indipendenza e neutralità.

Le norme impugnate vengono quindi dichiarate incostituzionali, perché non rispettose di simili presupposti[167].

5.2 Le nuove dimensioni della privacy *nell'ordinamento italiano: verso la creazione di nuovi diritti fondamentali?*

La riflessione intorno alle c.d. nuove dimensioni della *privacy* nell'ordinamento italiano ha visto impegnata la dottrina civilistica, costituzionalistica e penalistica. Infatti, l'esigenza di tutela dei propri dati e informazioni, resa ancora più urgente dalle potenzialità di *Internet*, pervade trasversalmente diversi settori del diritto.

Il processo penale si alimenta di dati e informazioni relativi a persone identificate o identificabili e può dunque senz'altro essere considerato un'ipotesi di trattamento di dati personali[168]. Esso tuttavia sfugge alle principali regole generali fissate dal codice *privacy* – soprattutto a quelle relative ai diritti dell'interessato - in quanto strumentale al perseguimento di esigenze di giustizia (art. 47 codice *privacy*). Se, tuttavia, come ritenuto dalla dottrina, il diritto all'autodeterminazione sui propri dati personali (sancito dall'art. 1 codice *privacy*) ha rango fondamentale, esso si impone come limite ad attività investigative.

Quanto al fondamento costituzionale di tale diritto, si è fatto ricorso alle stesse norme a cui già si riconduceva il diritto alla riservatezza: si è richiamato l'art. 2 Cost. come "clausola aperta", l'art. 3 Cost. quale clausola generale della dignità umana, l'art. 21 Cost. letto in negativo come libertà di non manifestare il proprio pensiero; si è seguita la strada di una lettura estensiva degli artt. 13, 14, 15 Cost.[169]

---

[167] La sentenza verrà esaminata più approfonditamente nel prosieguo della trattazione. *Infra*, capitolo III, par. 4 ss.

[168] S. CARNEVALE, *Autodeterminazione informativa*, cit., p. 5.

[169] Sicuramente suggestiva è la tesi che riconduce l'autodeterminazione all'art. 13 Cost. inteso come «libertà informatica» o *habeas data*. Sostiene infatti S. RODOTÀ, *Libertà personale. Vecchi e nuovi nemici*, in M. BOVERO (a cura di), *Quale libertà. Dizionario minimo contro i falsi liberali*, Roma-Bari. 2004, p. 52, che «la libertà personale non è difesa soltanto attraverso il diritto di essere lasciato solo, secondo la definizione che racchiude la più antica essenza della *privacy* e che si concreta nel potere di impedire la circolazione dei dati personali. Diviene un potere di controllo sull'esterno, sia per mantenere l'integrità di sé seguendo in ogni momento i dati diffusi nell'ambiente, sia per impedire la

Oggi, tuttavia, la soluzione migliore è quella di ricondurre il diritto all'autodeterminazione informativa all'art. 8 CEDU e all'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea, che espressamente riconosce il diritto alla tutela dei propri dati personali.

Come si è già avuto modo di sottolineare, tuttavia, le nuove dimensioni della *privacy* non attengono solo ad un'esigenza di controllo sulla circolazione dei propri dati personali, ma prima ancora si avverte la necessità di riaffermare l'esistenza di quella sfera di riservatezza, i cui classici confini, legati agli spazi fisici e al tipo di informazioni che si vuole sottrarre alla conoscenza altrui, sfumano e si dissolvono[170].

A tal proposito illuminanti sono le riflessioni dei penalisti intorno al bene giuridico tutelato da alcune delle nuove norme in materia di criminalità informatica (artt. 615 *ter*, 615 *quater*, 617 *quater*, 617 *quinquies*, 617 *sexies* c.p.)[171].

Con il termine dati informatici ci si riferisce ad una pluralità di informazioni, di diversa natura, in grado di circolare con grande facilità e rapidità, duplicabili su più supporti, privi di una dimensione fisica. In quest'ottica, ben si comprende come sia superata la distinzione tra dati intimi e dati sociali, tra informazioni segrete e

---

violazione della propria sfera privata attraverso informazioni non gradite. Il controllo sulle informazioni in entrata, strutturato in un più generale «diritto di non sapere», diventa un momento caratterizzante della nuova definizione della *privacy* e incarna quel momento di intangibilità del corpo e di divieto di sue invasioni che appartiene alla più antica tradizione dell'*habeas corpus*». Questa soluzione avrebbe, tuttavia, delle conseguenze ingovernabili se calata nel processo penale. L'art. 13 Cost. prevede infatti garanzie molto rigorose, in considerazione del bene protetto che, se applicate a tutte le ipotesi in cui si apprendono dati personali attraverso mezzi di ricerca della prova, condurrebbero alla paralisi del processo. «Per qualsiasi operazione di reperimento, raccolta, elaborazione di informazioni riguardanti persone determinate dovrebbe intervenire un provvedimento autorizzativo del magistrato o una sua successiva convalida, attestante la ricorrenza di una situazione di eccezionale necessità ed urgenza che non gli abbia consentito d'intervenire personalmente». Così, S. CARNEVALE, *Autodeterminazione informativa*, cit., p. 23.

[170] Sostiene S. RODOTÀ, *Il diritto*, cit., p. 319, che nella dimensione tecnologica l'identità personale sembra dilatarsi, *disperdersi*, sino a diventare *inconoscibile* da parte dello stesso interessato. Infatti, le informazioni riguardanti una persona sono contenute in diverse banche dati, ciascuna delle quali restituisce soltanto una parte o un frammento dell'identità complessiva. Talvolta addirittura lo stesso interessato non sa dove siano dislocati i propri dati personali. Si tratta quindi di apprestare idonee forme di tutela di questa «identità esterna, frutto di un'operazione nella quale sono gli altri a giocare un ruolo decisivo, con la presenza continua di elaborazione e controllo».

[171] L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 53, 54, distingue infatti tre diverse categorie di reati informatici a seconda dei beni giuridici tutelati (e delle modalità di aggressione). Vi sono innanzitutto fattispecie poste a tutela di beni giuridici tradizionali, offesi da nuove modalità o nuovi mezzi di aggressione, quale la frode informatica. In secondo luogo, «offese a beni giuridici analoghi a quelli tradizionali, in cui la diversità dei nuovi oggetti "passivi" su cui cadono le condotte tipiche, rispetto a quelli prima considerati dall'ordinamento, si riflettono anche sulla fisionomia dei corrispondenti beni protetti», come le falsità informatiche. «Infine, vi sono fattispecie in cui gli stessi beni giuridici offesi appaiono radicalmente nuovi perché sorti solo con lo sviluppo e la diffusione delle nuove tecnologie dell'informazione». È il caso degli artt. 615 *ter*, 615 *quater*, 617 *quater*, 617 *quinquies*, 617 *sexies* c.p.

informazioni riservate. Un dato apparentemente innocuo, collegato ad altri dati altrettanto apparentemente innocui può in realtà rivelare aspetti della vita di una persona, che si desiderano sottrarre alla conoscenza altrui. Si arriva così a teorizzare un nuovo bene giuridico meritevole di tutela, la *riservatezza informatica*, da intendersi quale «interesse al godimento e controllo esclusivo sia di determinati dati e informazioni, che dei relativi mezzi e procedimenti informatici e telematici di trattamento, che pur configurandosi sempre quale «diritto di escludere» i terzi non legittimati dal corrispondente accesso e utilizzo, prescinde in tutto o in parte dai tradizionali limiti e presupposti dei concetti civilistici di proprietà o possesso, ovvero dalle condizioni che fondano la rilevanza giuridica del segreto o della riservatezza personale in genere»[172]. La matrice del nuovo diritto è pur sempre quindi l'esigenza di riservatezza del titolare dello *ius excludendi alios*, ma essa va oltre la dimensione originaria della *privacy* e della tutela del domicilio, pur nella sua accezione di domicilio informatico[173].

L'intuizione, che si condivide, consiste nel riconoscere che l'interesse dell'utilizzatore di sistemi informatici e telematici è quello alla tutela dei propri dati, a prescindere dal "luogo" in cui si trovino, o dal mezzo di comunicazione prescelto. Tale affermazione è ben esemplificata attraverso il ricorso alla teoria c.d. assiomatica, anziché concentrica, delle sfere di tutela della vita privata[174]. Secondo tale ricostruzione, all'interno di un sistema informatico o telematico non ha più senso distinguere tra sfera individuale e sfera privata, ma occorre prendere atto dell'esistenza di «spazi virtuali di manifestazione della personalità, che coincidono

[172] L. PICOTTI, (voce) *Reati informatici*, in *Enc. giur. Treccani*, agg. VIII, Roma, 2000, p. 20 ss. Vedi anche R. FLOR, Phishing, identity theft *e* identity abuse. *Le prospettive applicative del diritto penale vigente*, *Riv. it. dir. proc. pen.*, 2007, p. 899 ss., secondo cui «il bene giuridico "riservatezza informatica", protetto dall'art. 615-*ter* c.p., si può configurare come interesse esclusivo, giuridicamente riconosciuto, di godere, disporre e controllare le informazioni, i procedimenti, i sistemi e "spazi" informatizzati e le relative utilità».

[173] R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht, p. 705. Si è già sottolineato come in origine, anche in base al tenore della relazione alla legge 574 del 1993 che considerava i sistemi informatici o telematici un' «espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli art. 614 e 615 c.p.», si era individuato il bene giuridico protetto dagli artt. 615 *ter* (accesso abusivo ad un sistema informatico o telematico) e 615 *quater* (detenzione e diffusione abusiva di codici d'accesso a sistemi informatici o telematici) nel c.d. domicilio informatico. *Supra*, par. 1.1.

[174] L'elaborazione di tale teoria si deve a R. FLOR, Phishing, identity theft, cit..; ID., *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht, cit.; ID., Flor R., *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di* Internet, in *www.penalecontemporaneo.it*.

con l'interesse sostanziale alla protezione di informazioni "riservate" e al loro controllo nello svolgimento di rapporti giuridici e personali *online* o in altri spazi "informatici"»[175]. In questo contesto è evidente che la tutela del domicilio, della segretezza delle comunicazioni, ma anche della riservatezza tradizionalmente intensa, non è sufficiente.

Nell'ottica del processualpenalista, si pone a questo punto il problema di individuare il fondamento costituzionale di tale diritto, al fine di stabilire i presupposti per una sua legittima limitazione da parte dell'autorità pubblica. Infatti, si tratta pur sempre di un diritto soggetto al bilanciamento con contrapposti interessi ed esigenze. I principi sono destinati a coesistere con altri principi in conflitto, e ciò vale anche per quelli concernenti diritti inviolabili: «ad essi è riservato uno spazio di assoluta inattaccabilità da parte dello Stato; ma al di fuori di quello spazio, la loro tutela può essere compressa in favore di altri principi che esigono di essere attuati»[176].

A tal fine, ci si deve richiamare alle riflessioni già svolte intorno all'art. 8 CEDU e al suo valore nell'ordinamento interno[177]. Codesta norma presenta infatti l'elasticità necessaria per ricomprendere anche la riservatezza informatica e al tempo stesso individua i presupposti per una limitazione di tale diritto fondamentale da parte dell'autorità pubblica[178].

Nel mondo del *Web* 2.0, delle comunicazioni globali e del *cloud computing*, non si può più distinguere tra sfera privata e sfera pubblica, e la stessa nozione di *privacy* muta e si arricchisce di contenuti nuovi. Da un lato, l'originario *right to be let alone* perde ogni riferimento alla realtà fisica; dall'altro, il *right to control the information about oneself*, acquista il significato di un diritto di controllo sui pacchetti di dati che viaggiano nel *web*.

Si è quindi forse ancora lontani dall'elaborazione di una «costituzione informativa o di un *Information Bill of Rights*, che comprend[a] il diritto di cercare, ricevere e diffondere informazioni, il diritto all'autodeterminazione informativa, il

[175] R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht, cit., p. 705.
[176] R. ORLANDI, *Garanzie individuali ed esigenze repressive*, cit., p. 559.
[177] *Supra*, par. 3 ss.
[178] Presupposti che per altro sono simili a quelli elaborati dalla giurisprudenza della Corte costituzionale tedesca a giustificazione di intromissioni nell'*informationellen Selbstbestimmungsrecht* e nel *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*.

diritto alla *privacy* informatica»[179], ma sicuramente, grazie al sistema di tutela multilivello dei diritti fondamentali, è possibile offrire una protezione adeguata all'individuo nei confronti dei pericoli derivanti dalla tecnologia. Non va infatti sottovalutata la circostanza che la Carta dei Diritti Fondamentali dell'Unione Europea riconosca rango di diritto fondamentale al diritto alla protezione dei propri dati personali (art. 8), distinguendolo dal più generale diritto alla vita privata (art. 7)[180].

La protezione multilivello dei c.d. diritti di *privacy* (art. 2 Cost., art. 8 CEDU e art. 117 Cost., artt. 7 e 8 CDFUE) assicura ad essi rango fondamentale nel sistema delle fonti ed impone il loro rispetto anche da parte dell'autorità giudiziaria nel condurre indagini penali. Ciò che impone un ripensamento di alcuni mezzi di ricerca della prova, o prassi investigative, poco rispettose dei nuovi diritti fondamentali.

[179] S. RODOTÀ, *Tecnologie*, cit., p. 107.
[180] «Siamo di fronte a una vera reinvenzione del concetto di protezione dei dati personali, non solo perché viene esplicitamente considerato come un autonomo diritto fondamentale, ma perché si presenta come strumento indispensabile per il libero sviluppo della personalità e per definire l'insieme delle relazioni sociali. Si rafforza così la costituzionalizzazione della persona grazie a un insieme di poteri che davvero caratterizzano la cittadinanza del nuovo millennio». S. RODOTÀ, *Il diritto*, cit., p. 321.

CAPITOLO II
MEZZI DI RICERCA DELLA PROVA TIPICI E NUOVE TECNOLOGIE INFORMATICHE

SOMMARIO: *1. Le indagini informatiche nella legge di ratifica della Convenzione* Cybercrime*: il recepimento delle tecniche di* computer forensics *2. Ispezioni e perquisizioni 2.1 La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico 2.2 Le attività urgenti di investigazione informatica e telematica 3. Sequestro 3.1 Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici 3.2 Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici: l'acquisizione di corrispondenza informatica 4. Questioni aperte in tema di perquisizione e sequestro di* computer *4.1 Natura giuridica dell'attività di clonazione e attuazione del contraddittorio con la difesa 4.2 Conseguenze derivanti dal mancato rispetto delle misure tecniche 4.3 Il riesame e il problema dell'interesse ad impugnare 4.3.1 Interesse alla legalità, interesse alla pronuncia e interesse alla prova 4.3.2 Solo l'interesse alla restituzione della* res *può giustificare il riesame: l'intervento delle Sezioni Unite 4.3.3 Le questioni non risolte dalle Sezioni Unite 4.4 Rischio di perquisizioni esplorative e tutela dei dati personali 4.4.1. La soluzione statunitense al rischio di perquisizioni esplorative 5. Perquisizione e sequestro di materiale informatico: una proposta 6. Captazione in tempo reale di dati digitali 6.1 Intercettazione di comunicazioni informatiche o telematiche 6.1.2 Intercettazione di comunicazioni* VoIP *6.2 Acquisizione di* e-mail *6.2.1 Acquisizione di* e-mail *nell'ordinamento processuale tedesco: la sentenza del* BVerfG *del 16 giugno 2009 7. Conservazione e acquisizione di dati di traffico 7.1 La conservazione dei dati relativi al traffico: il d. lgs. 109/2008 7.2 Acquisizione degli indirizzi* IP *7.3 L'acquisizione di dati di traffico ai sensi dell'art. 132 Codice* privacy *tra finalità repressive e preventive 7.4 Acquisizione (art. 132 codice* privacy*) e sequestro (art. 245* bis *c.p.p.) 7.5 La sentenza del* BVerfG *sul* data retention

1. Le indagini informatiche nella legge di ratifica della Convenzione Cybercrime*: il recepimento delle tecniche di* computer forensics

Con la legge 18 marzo 2008, n. 48 il legislatore italiano ha ratificato la Convenzione *Cybercrime* del Consiglio d'Europa, firmata a Budapest il 23 novembre 2001[181].

[181] Il Testo della Convenzione e l'elenco aggiornato degli Stati firmatari nonché delle ratifiche è disponibile all'indirizzo *www.conventions.coe.int*. La legge 48 del 18 marzo 2008 è pubblicata in G.U. 4 aprile 2008, n. 80, Suppl. ord. L'atto formale di ratifica è stato depositato il 5 giugno 2008.

Il provvedimento in questione modifica al capo II alcune disposizioni del Codice Penale e del Decreto legislativo 231/2001 e al capo III alcuni articoli del Codice di Procedura Penale e del Codice di cui al Decreto legislativo 196/2003 - codice *privacy* - .

Per quanto riguarda l'intervento sulla materia processuale, la legge n. 48/2008, oltre ad accentrare la legittimazione a svolgere le indagini per i principali reati informatici in capo alle procure distrettuali antimafia[182], è intervenuta in maniera mirata sul testo delle disposizioni riguardanti i mezzi di ricerca della prova e le indagini di polizia giudiziaria, disciplinando specifiche modalità nell'esecuzione di ispezioni, perquisizioni e sequestri, nonché prescrivendo regole di conservazione del materiale informatico per garantire l'intangibilità dei dati originari[183].

L'aspetto problematico del rapporto tra mezzi di ricerca della prova e materiale informatico risiede nella natura ontologicamente volatile e alterabile del dato digitale, su cui possono spesso incidere condotte involontarie atte ad ingenerare fenomeni di "inquinamento", ciò che richiede la puntuale previsione di tecniche volte ad assicurare la genuinità dell'accertamento.

Lo sforzo legislativo è stato nel senso di realizzare un ideale punto di equilibrio tra i diversi interessi in gioco. Da un lato l'esigenza, avvertita nell'ambito della *computer forensics*, di procedere subito e sfruttando l'effetto sorpresa, alla ricerca della *digital evidence,* al fine di non perdere informazioni che potrebbero risultare risolutive per il buon esito delle indagini; dall'altro la garanzia dell'esercizio del diritto di difesa della persona imputata o indagata[184]. Il compromesso è assicurato

[182] Il neo introdotto comma 3 *quinquies* dell'art. 51 c.p.p. attribuisce alle procure distrettuali la competenza ad indagare i delitti concernenti lo sfruttamento sessuale dei minori – i quali, ad eccezione del reato di pedopornografia virtuale, solo occasionalmente sono commessi avvalendosi di strumenti informatici – e i c.d. *computer crimes* in senso stretto, ovverosia quegli illeciti necessariamente commessi avvalendosi dell'ambiente digitale. Peraltro, inizialmente non vi era corrispondenza tra i delitti introdotti dalla legge 48/2008 e quelli per cui è legittimato il giudice per le indagini preliminari distrettuale. L'art. 328 c.p.p. continuava infatti a fare riferimento solo all'art. 51, commi 3 *bis* e 3 *ter*. La successiva legge 24 luglio 2008, n. 125, di conversione del d.l. 23 maggio 2008, n. 92 ha posto rimedio a questa discrasia, introducendo il comma 1 *quater* all'art. 328 c.p.p. Cfr., F. CASSIBBA, *L'ampliamento delle attribuzioni del pubblico ministero distrettuale*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, p. 113 ss. Si veda anche M. L. DI BITONTO, *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. Internet*, 2008, p. 503 ss.

[183] Cfr. L. LUPÀRIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc.* 2008, p. 717 ss.

[184] A. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico,* in *Dir. Internet,* 2008, p. 507 ss.

attraverso la qualificazione dell'attività di accesso a sistemi informatici in termini di ispezione e perquisizione – tipici atti a sorpresa – e contestualmente con la previsione, inserita nei novellati articoli 244, 247, 352, 354 c.p.p., dell'obbligatorietà dell'adozione di «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». Con ciò non si indica una singola modalità operativa, ma si segue la strada del rinvio a quelle che, nella parabola dell'evoluzione scientifica, saranno *ratione temporis* le migliori tecniche per tutelare l'integrità del dato digitale. Attraverso tale opzione il legislatore si mostra consapevole delle peculiarità dei dati informatici come strumento e oggetto di indagine e soprattutto della rapidità con cui la tecnologia evolve in questo settore[185]. Se sotto questo profilo la scelta è assolutamente apprezzabile, non si può tuttavia tacere il fatto che essa sia al tempo stesso foriera di incertezze per quanto riguarda la sanzione processuale applicabile nel caso in cui non siano state seguite le c.d. *best practices*. Senza voler anticipare riflessioni che saranno svolte nel prosieguo della trattazione, basti in questa sede accennare al fatto che, a fronte di coloro che affermano trattarsi di questione emergente solo in fase di valutazione della prova, vi è chi ritiene sussistente un'ipotesi di inutilizzabilità o di nullità[186].

L'esigenza di garantire l'integrità e la non alterazione dei dati è presente anche nel neo introdotto art. 254 *bis* c.p.p. che prevede una particolare ipotesi di sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazione, che deve avvenire mediante copia di essi su adeguato supporto[187].

Il *file rouge* che lega le modifiche al codice di rito apportate dalla legge 48/2008 è quindi certamente quello di preservare in sede investigativa la genuinità della prova digitale[188]. In particolare, il legislatore ha recepito alcuni dei principi

[185] G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, p. 189, definisce le nuove disposizioni introdotte dalla legge 48/2008 norme processuali "in bianco".
[186] L'argomento è oggetto di specifica trattazione, *infra*, par. 4.2.
[187] Il punto sarà approfondito *infra*, par. 3.1 e par. 7.4.
[188] E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in L. LUPARIA (a cura di), *Sistema penale*, cit., p. 135.

della *computer forensics*: corrette modalità di conservazione, procedure di duplicazione efficaci, garanzie di non alterabilità[189].

Allo stato attuale, la modalità tecnica utilizzata al fine di conservare i dati digitali senza alterarne il contenuto, è quella della c.d. *bit stream image* o *legal imaging*, grazie alla quale si realizza una sorta di "immagine" o di "clone" dell'*hard disk*. Si ottiene così una copia analitica identica al disco rigido originale (o a qualsiasi supporto di memoria), comprendente «sia le informazioni contenute nello spazio dei *cluster*, sia i frammenti d'informazione contenuti nello *slack space* o nell'*unallocated space* dei *cluster*»[190]. Tale procedura si differenzia da, e per questo è da preferire a, quella di semplice copiatura del contenuto dell'*hard disk*, atteso che essa non si limita a garantire la mera identità contenutistica dei dati presenti nei due supporti, ma assicura che ogni *file* dell'*hard disk* clonato abbia la medesima allocazione del corrispondente *file* del disco sorgente.[191] Preliminarmente, tuttavia, è

[189] In questi termini G. ZICCARDI, *L'ingresso della* computer forensics *nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. LUPARIA (a cura di), *Sistema penale*, cit., p.170, il quale fornisce una definizione di *computer forensics* basata sui concetti di valore e resistenza dei dati. In particolare, per *computer forensics* si intende «quella scienza che studia il valore che un dato correlato ad un sistema informatico o telematico può avere in un ambito sociale, giuridico o legale». C. MAIOLI, *Introduzione all'informatica forense*, in P. POZZI (a cura di), *La sicurezza preventiva dell'informazione e della comunicazione*, Torino, 2004, definisce la *computer forensics* come «la disciplina che studia l'insieme delle attività rivolte all'analisi e alla soluzione dei casi di criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un *computer*, diretti a un *computer*, o in cui il *computer* può rappresentare comunque un elemento di prova» e afferma che «gli scopi dell'informatica forense sono di conservare, identificare, acquisire, documentare e interpretare i dati presenti su un *computer*. A livello generale si tratta di individuare le modalità migliori per: acquisire le prove senza alterarle o modificare il sistema informatico su cui si trovano, garantire che le prove acquisite su altro supporto siano identiche a quelle originarie, analizzare i dati senza alterarli. In sintesi "dar voce alle prove"». Infine E. H. SPAFFORD, in B. D. CARRIER, E. H. SPAFFORD, *Categories of digital investigation analysis techniques based on the computer history model*, *Digital Investigation*, 3, 2006, p. 121, ha proposto una tripartizione della *forensics*, collegata al tipo di tecnologia (il che la rende rischiosa): egli individua una *computer forensics*, correlata al *computer*, una *network forensics*, legata alla presenza di una connessione di rete e una *intrusion forensics*, laddove vi siano atti di violazione di sistemi informatici. G. VACIAGO, Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, 2012, p. 6, riprendendo una distinzione fatta da K. ZATIKO, *Commentary: Defining Digital Forensics*, *Forensics Magazine*, 2007, ritiene più appropriato l'uso del termine *digital forensics*, poiché oggetto di indagine non è più soltanto il *computer*, ma altre tipologie di supporti (*smartphones*, lettori *mp3*, *console* di videogiochi, navigatori satellitari) e di risorse *hardware* o *software* distribuite in remoto (*cloud computing*), su cui sono archiviati dati utili per le indagini.

[190] Così A. VITALE, *La nuova disciplina*, cit., p. 508.

[191] Merita di essere segnalata la ricostruzione di A. CISTERNA, *Perquisizioni in caso di fondato motivo*, in *Guida dir.*, n. 16/2008, p. 66, secondo cui le misure tecniche di salvaguardia, nel caso dell'ispezione, consisterebbero nella «mera clonazione/duplicazione dei "dati originali"», mentre in quello della perquisizione atterrebbero alla «fase esecutiva della vera e propria ablazione degli oggetti rinvenuti nel sistema esplorato», ossia riguarderebbe la «custodia giudiziale dell'oggetto rinvenuto e appreso in esito alla perquisizione».

necessario garantire l'integrità dei dati attraverso la creazione di un'impronta di *hash*, che consente di dimostrare se i contenuti dei *files* o del supporto abbiano subito modifiche, e attraverso l'utilizzo di un *write blocker* che consente di bloccare ogni tipo di scrittura sul supporto ispezionato[192].

Le operazioni di investigazione informatica comprendono cinque fasi: l'individuazione, l'acquisizione, la conservazione, l'analisi e la presentazione della *digital evidence*[193]. Al fine di garantire il successo dello scopo ultimo della *computer forensics*, ossia quello di fornire prove utilizzabili in un procedimento penale[194], è necessario che sia stata rispettata la c.d. *chain of custody*, e che tale continuità probatoria sia dimostrabile[195]. Questa è una delle ragioni per cui gli esperti di *computer forensics* consigliano l'utilizzo di *software open source*, sempre verificabili; infatti i programmi commercializzati da grandi aziende (il più utilizzato è "*EnCase*" della *Guidance Software Inc.*) sono coperti da licenza, il che impedisce di poter accedere ai c.d. "codici sorgente", e quindi di verificare il corretto funzionamento del programma[196].

Prima di passare all'analisi delle specifiche disposizioni modificate dalla legge 48/2008 e ai relativi aspetti problematici, è opportuna un'ultima osservazione.

Il legislatore del 2008 ha scelto la strada dell'interpolazione delle norme relative ai tradizionali mezzi di ricerca della prova, che oggi possono avere ad oggetto anche sistemi e dati informatici[197]. Si dubita, tuttavia, della bontà di simile

---

[192] G. VACIAGO, *Digital evidence*, cit., p. 32. L'Autore definisce l'impronta di *hash* in questi termini «l'*hash* è una funzione univoca operante in un solo senso (ossia che non può essere invertita), attraverso la quale viene trasformato un documento di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata. Tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, ed è conosciuta come valore di *hash* o *Message Digest*. Se il documento fosse stato alterato anche in minima parte, cambierebbe di conseguenza anche l'impronta», ID., p. 62. Si veda anche D. BUSO, D. PISTOLESI, *Le perquisizioni e i sequestri informatici*, in F. RUGGIERI, L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, p. 183 ss.

[193] Questa partizione è ripresa da G. VACIAGO, *Digital evidence*, cit., p. 23.

[194] G. ZICCARDI, *L'ingresso della* computer forensics, cit., p. 171, ritiene particolarmente importante nell'ambito delle operazioni di *computer forensics*, l'aspetto della *resistenza informatica* alle contestazioni, ossia «la possibilità di provare con un buon grado di certezza in ogni momento che il dato digitale sia integro, non ripudiabile, correlabile direttamente ad un dato soggetto e che abbia valori di luogo e di tempo ben identificabili».

[195] In quest'ottica è di fondamentale importanza che tutte le operazioni di *digital forensics* vengano accuratamente documentate, se del caso anche fotograficamente e con riprese video.

[196] L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, p. 153 ss.

[197] Per espressa ammissione dello stesso legislatore, infatti, «le novelle in materia processuale consistono in un adeguamento prevalentemente lessicale delle disposizioni processuali già vigenti,

scelta; infatti, l'innovazione tecnologica mette in crisi le usuali categorie elaborate in tema ispezione, perquisizione e sequestro, sfumano i confini tra le diverse attività d'indagine, si inverte l'ordine con cui esse vengono eseguite – per perquisire un *computer* occorre prima sequestrarlo -[198].

Valga un esempio per tutti: il legislatore ha previsto che la perquisizione di un sistema informatico o telematico avvenga mediante «l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». Tali misure tecniche, tuttavia, lungi dall'essere una particolare modalità della perquisizione, integrano un'autonoma e prodromica attività che il legislatore ha omesso di qualificare. L'art. 247, comma 1 *bis* c.p.p. fa quindi in realtà riferimento a due attività, la seconda delle quali è una perquisizione. La qualificazione della prima, che attualmente viene realizzata mediante clonazione dell'*hard disk*, è al centro di un acceso dibattito, che sarà approfondito nel prosieguo della trattazione. Ciò che preme fin d'ora sottolineare è la necessità, in questo campo, di una sinergia tra informatica e diritto: la scarsa comprensione o la sottovalutazione delle potenzialità delle innovazioni tecnologiche può tradursi in minori garanzie per chi è sottoposto a procedimento penale.

2. Ispezioni e perquisizioni

2.1 La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico

La legge n. 48/2008 ha integrato il testo degli articoli 244 e 247 c.p.p., consentendo, esplicitamente, il compimento di ispezioni e perquisizioni su sistemi informatici o telematici. In particolare, l'autorità giudiziaria: «al fine di rilevare eventuali tracce digitali lasciate nella consumazione del reato ovvero se tali tracce non siano state lasciate o siano cancellate, disperse, alterate o rimosse, può disporre

finalizzato a renderne esplicite le potenzialità applicative in campo informatico». V. *Relazione di accompagnamento* al d.d.l. 2807, p. 7.

[198] Non è tuttavia necessario asportare fisicamente il *computer*, essendo possibile procedere *in loco* alla clonazione dell'*hard disk*. *Infra*, par. 5.

rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica anche in relazione a sistemi informatici o telematici» (art. 244, comma 2 c.p.p.);

«quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, può disporne la perquisizione» (art. 247, comma 1*bis* c.p.p.);

in entrambi i casi deve però «adottare misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

Già la formulazione delle due norme lascia intendere come l'ambito operativo dei nuovi strumenti riguardi non solo i delitti che abbiano ad oggetto, o la cui commissione avvenga per mezzo di, sistemi informatici o dati informatici (c.d. reati informatici in senso stretto e in senso ampio)[199], ma anche, più in generale, la raccolta delle prove informatiche relative a qualsiasi altro reato. A questo proposito vengono in rilievo reati in materia di traffici illeciti di vario tipo, di terrorismo internazionale, di criminalità organizzata interna e transnazionale, economica e finanziaria, per la cui commissione viene sempre più spesso utilizzata la rete o un sistema informatico o che comunque lasciano "tracce elettroniche" in singoli *computer* o supporti elettronici.

La modifica legislativa ha interessato anche l'art. 352 c.p.p. che disciplina il potere di perquisizione in capo agli ufficiali di polizia giudiziaria. È stato infatti introdotto il comma 1*bis*, specificamente dedicato alla perquisizione di sistemi informatici o telematici. Tale disposizione consente sostanzialmente di accedere ad un sistema informatico o telematico e di acquisire e conservare i dati in essi eventualmente contenuti, al sussistere dei requisiti indicati nei commi 1 e 2 della norma stessa, purché, si ribadisce ancora una volta, si adottino «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». Scopo di tale attività d'indagine è acquisire dati, informazioni, programmi o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.

[199] Per la distinzione dogmatica e sistematica tra reati informatici in senso stretto e in senso ampio, nonché fra reati cibernetici in senso proprio e improprio, si veda L. PICOTTI, Internet *e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. Internet*, 2005, p. 189 ss. Che le indagini informatiche debbano riguardare anche reati "comuni" e non solo i reati informatici è previsto dalla stessa Convenzione di Budapest (art. 14, par. 2, lett. c).

Si tratta, a questo punto, di capire cosa debba intendersi per "sistema informatico o telematico": al riguardo la Convenzione di Budapest si rivela poco utile, fornendo una definizione molto ampia. L'art. 1, lett. a) della Convenzione definisce, infatti, il sistema informatico come «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione sistematica dei dati». Ai fini che qui interessano, si può affermare che le disposizioni novellate fanno riferimento, come oggetto dell'accesso o perquisizione, al sistema informatico inteso come sistema operativo (o *software* di base), *software* applicativo e memorie del *computer* (comprensive, queste, della memoria centrale o interna al *computer* e delle memorie ausiliarie o esterne ad esso, quali *floppy disk*, *cd rom*, *dvd*, *pen drive*, ecc.), e al sistema telematico inteso come complesso degli strumenti (macchina, *modem*, collegamento alla linea telefonica, *software*) che consentono a un *computer* di collegarsi ad un altro attraverso linee telefoniche o linee dedicate, o anche come complesso dei *computers* collegati con tali modalità o con reti interne ad un determinato ufficio o unità operativa[200].

In relazione all'attività di perquisizione informatica, si è sostenuto che un sistema informatico o telematico, perfettamente inquadrabile nel concetto di corpo del reato o cosa pertinente al reato, quindi oggetto della perquisizione, mal si adatti, invece, ad essere considerato luogo della stessa, cioè spazio all'interno del quale la polizia giudiziaria è deputata ad operare per la ricerca, appunto, del corpo del reato.

Tale impostazione è frutto di una concezione della perquisizione ancorata ad un'idea ormai superata di luogo: si legge, infatti, nel passo in esame, «il *computer* e i programmi e i dati in esso contenuti non costituiscono e non possono costituire il luogo dove la perquisizione si svolge, ma soltanto, rispettivamente, l'oggetto e il risultato dell'attività di perquisizione, la quale può svolgersi evidentemente all'interno dei luoghi dove i sistemi informatici e telematici sono installati o custoditi»[201]. Nell'era di *Internet* e della tecnologia non è più possibile non considerare il *computer* come potenziale luogo della perquisizione, tanto più alla luce del fatto che gli sviluppi dell'informatica rendono oggi possibili perquisizioni *online*

[200] A. BARBIERI, *Le attività di indagine della polizia giudiziaria su sistemi informatici e telematici*, in *Dir. Internet*, 2008, p. 517.
[201] *Ibidem*, p. 518.

di supporti informatici e telematici che, essendo condotte attraverso l'installazione, in locale o in remoto, di un *software* in grado di "spiare" il contenuto di un *computer*, permettono, a buon titolo, di qualificare lo stesso come "luogo virtuale" della perquisizione, e il materiale informatico, la *digital evidence*, come oggetto della perquisizione[202]. Ciò detto, resta comunque la questione del se sia una scelta opportuna quella di qualificare in termini di perquisizione l'attività di indagine che insiste su un sistema informatico o telematico. Sul punto si avrà modo di tornare approfonditamente[203].

2.2 Le attività urgenti di investigazione informatica e telematica

L'art. 9 della legge 48/2008 ha integrato il secondo comma dell'art. 354 c.p.p. estendendo il potere della polizia giudiziaria di compiere accertamenti urgenti, finalizzati a conservare tracce e cose pertinenti al reato o ad evitare l'alterazione di luoghi e cose, ai dati, alle informazioni, ai programmi informatici e ai sistemi informatici o telematici. In relazione a codesta attività, il legislatore ha espressamente previsto che gli ufficiali di polizia giudiziaria adottino le misure tecniche o impartiscano le prescrizioni necessarie ad assicurare la conservazione dei dati e più in generale, dei sistemi oggetto di accertamento, e ad impedirne l'alterazione e l'accesso. A tal fine, ove possibile, è previsto che si proceda all'immediata duplicazione dei dati, delle informazioni e dei programmi su adeguati supporti, «mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità».

La *ratio* di tale modifica va ravvisata nella volontà di procedimentalizzare l'indagine informatica urgente e porre fine a prassi investigative irrispettose dei protocolli di *computer forensics*, e non semplicemente nell'intenzione di aggiungere un possibile *luogo* oggetto degli accertamenti urgenti[204].

Tale lettura della norma permette anche di risolvere una delle questioni interpretative che si sono poste, ossia quella del novero dei soggetti autorizzati a compiere tale attività urgente d'indagine. Questa problematica deriva ancora una

[202] Le c.d. perquisizioni *online* saranno esaminate *infra*, capitolo III, par. 4 ss.
[203] Vedi, *infra*, par. 4.1.
[204] Così, E. LORENZETTO, *Le attività urgenti*, cit., p. 138.

volta dall'infelice opzione legislativa per l'interpolazione. Infatti, l'art. 354 c.p.p. si riferisce espressamente solo alla polizia giudiziaria, ma è evidente che anche altri soggetti sono autorizzati ad accedere a «luoghi» o «cose» e potrebbero ritrovarsi nella necessità di compiere accertamenti indifferibili. Se l'intenzione del legislatore era quella di imporre, data la peculiare natura volatile dei dati digitali, l'adozione di specifiche misure tecniche volte a preservarne l'integrità e la non alterabilità, allora è evidente che la prescrizione deve valere anche per il pubblico ministero e per il difensore.

Per quanto riguarda il tipo di attività consentita, gli investigatori dovranno limitarsi al congelamento ed eventuale duplicazione delle informazioni o dei programmi inerenti a sistemi informatici o telematici, senza porre in essere alcuna trasformazione unilaterale dei dati, in vista di successive analisi critiche che i soggetti abilitati opereranno sull'elemento digitale reperito[205].

Pur così definito l'àmbito di applicazione dell'art. 354, comma 2, seconda parte c.p.p., la linea di confine con ispezione, perquisizione e sequestro è molto labile. Basti pensare che questo tipo di attività già porterà alla creazione della c.d. copia-clone, poiché per espressa previsione legislativa, ove possibile, occorrerà procedere all'immediata duplicazione dei dati, delle informazioni e dei programmi «su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità». Da qui derivano le difficoltà di inquadramento della clonazione stessa, astrattamente riconducibile a diverse attività d'indagine[206].

3. Sequestro

Il rapporto tra perquisizione e sequestro probatorio è chiaramente espresso dall'art. 252 c.p.p.: «le cose rinvenute a seguito della perquisizione sono sottoposte a sequestro».

Sebbene il legislatore tenda a favorire forme di consegna (art. 248 c.p.p.) o esibizione (art. 256, comma 1 c.p.p.) delle cose da sequestrare, per cui non sempre il sequestro è necessariamente preceduto da una perquisizione, è innegabile che tra i

[205] E. LORENZETTO, *Le attività urgenti*, cit., p. 146.
[206] Sul punto si tornerà approfonditamente *infra*, par. 4.1.

due mezzi di ricerca della prova esista un rapporto di logica consequenzialità che è ben esemplificato sul piano dell'elemento oggettivo: oggetto del sequestro, come della perquisizione, sono «il corpo del reato e le cose pertinenti al reato» (artt. 247, 253 c.p.p.)[207].

Analogamente a quanto accade in materia di perquisizioni, lo sviluppo di nuove tecnologie informatiche pone, in questo àmbito, rilevanti problemi di tutela della segretezza delle comunicazioni, della riservatezza, del dato informatico in quanto tale. La tecnologia permette oggi di evitare provvedimenti di sequestro di un intero *computer* e delle apparecchiature ad esso connesse, che tanto erano stati criticati dalla dottrina perché sproporzionati rispetto all'obiettivo da raggiungere, cioè assicurare al processo gli elementi di prova ivi contenuti[208].

La caratteristica fondamentale di un *file* è quella di consentire la piena separazione fra il contenuto rappresentativo dello stesso e il supporto che lo veicola. Prima dell'avvento delle tecnologie dell'informazione questa differenza non aveva un rilievo pratico rispetto all'esecuzione di sequestri probatori, atteso che il contenuto di un documento era di fatto inscindibile dal supporto materiale. Nel caso dei *files*, invece, si verifica una perfetta separazione fra i due elementi, per cui i dati possono essere trasferiti senza che il supporto segua la stessa sorte. La tecnica utilizzata per questo tipo di operazioni è – come già accennato - quella della *bit stream image* che permette, tra l'altro, di recuperare anche informazioni cancellate.

Tuttavia, la possibilità di fare una copia-clone dell'intero *hard disk*, lasciando il *computer* nella disponibilità dell'utente, pone innanzitutto il problema della qualificazione giuridica sia di tale attività, che di quella di successiva estrazione di copie. Emergono inoltre ulteriori questioni quali la persistenza dell'interesse a chiedere il riesame del provvedimento di sequestro, la tutela della riservatezza di dati personali salvati sulla memoria del disco rigido che non hanno alcuna pertinenza con il reato per cui si procede, la garanzia del rispetto del segreto professionale, nonché il

[207] G.CONSO, V. GREVI, M.BARGIS, *Compendio di procedura penale*, VI Ed., Padova, 2012, p. 361 ss.
[208] A. CHELO MANCHÌA, *Sequestro probatorio di* computers*: un provvedimento superato dalla tecnologia?*, in *Cass. pen.*, 2005, p. 1631 ss.; A. MONTI, *No ai sequestri indiscriminati di* computer, in *Dir. Internet*, 2007, p. 264 ss.

rischio, sempre attuale, di un sequestro "esplorativo", finalizzato alla ricerca della notizia di reato[209].

3.1 Le nuove disposizioni in tema di sequestro probatorio e di custodia e assicurazione dei dati informatici

La Convenzione di Budapest sui *cybercrimes*, dopo le disposizioni comuni e le regole sulla conservazione e la divulgazione di dati informatici immagazzinati in sistemi informatici e di quelli relativi al traffico, si occupa del sequestro, obbligando le parti contraenti a legiferare per rendere effettivo in capo all'autorità procedente il potere di sottoporre a vincolo reale i dati contenuti in sistemi informatici già oggetto di perquisizione o accesso. Le modalità attraverso cui raggiungere questo obiettivo consistono nel sequestro o acquisizione di sistemi informatici, di parte di questi o di supporti idonei alla conservazione di dati; nel trattenimento di copia delle informazioni raccolte; nella conservazione dell'integrità dei dati così memorizzati; nella segretazione nei confronti di terzi o, addirittura, rimozione dal sistema sequestrato di tutti i dati pertinenti al procedimento penale[210].

La legge di ratifica ha attuato in massima parte tali prescrizioni attraverso la modifica degli articoli 254, 256, 259 e 260 c.p.p., l'introduzione dell'art. 254 *bis* c.p.p., rubricato «sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazione» e con la modifica dell'art. 353 c.p.p. in tema di acquisizione di plichi e corrispondenza ad opera della polizia giudiziaria.

Il novellato testo dell'art. 254 c.p.p. recepisce all'interno del sistema processuale penale una più moderna e ampia nozione di corrispondenza quale *species* della comunicazione, estendendo la disciplina del sequestro probatorio, prima riferentesi ai soli oggetti presenti negli uffici postali o telegrafici, a tutte le comunicazioni inoltrate per via telematica, anche da fornitori diversi da quelli "tradizionali".

---

[209] Il tema assume ancora maggiore delicatezza nell'ambito delle perquisizioni *online*, laddove la linea di confine tra perquisizione e sequestro diviene impalpabile. *Infra*, cap. III, par. 4 ss.

[210] Art. 19 comma 3 Convenzione di Budapest. Cfr. A. MACRILLÒ, *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *La ratifica della Convenzione del Consiglio d'Europa sul* cybercrime*: profili processuali*, in *Dir. Internet*, 2008, p. 511 ss.

Ruolo centrale nella nuova disposizione ricoprono i fornitori di servizi che la Convenzione di Budapest identifica in «qualunque entità pubblica o privata abilitata a fornire ai propri utenti la possibilità di comunicare attraverso un sistema informatico» (art. 1, lett. c).

Nuovo è l'ampliamento dei destinatari del sequestro di corrispondenza: non più i soli uffici postali e telegrafici, ma, più in generale, i fornitori di servizi postali, telegrafici, telematici o di telecomunicazione; nuova è inoltre la specificazione della possibilità, riconosciuta all'autorità inquirente, di procedere a sequestro di corrispondenza inviata all'imputato per via telematica; nuova infine la previsione, accanto ai tradizionali divieti di aprire la corrispondenza e prenderne conoscenza, di un generale obbligo di garantire la genuina conservazione del materiale oggetto di apprensione, espresso dall'inciso «o alterarli», inserito nel secondo comma della norma in questione.

L'attuale versione dell'art. 254 c.p.p. è riferibile ai più recenti servizi forniti dagli uffici postali, in particolare a quello di spedizione delle raccomandate, della posta ordinaria e dei telegrammi *online*, che avviene mediante inoltro da parte del mittente (a mezzo *e-mail*) della corrispondenza al servizio postale, il quale provvede a stampare quanto ricevuto su supporto cartaceo e a curare la spedizione nelle forme tradizionali al destinatario, attestando ai fini legali l'invio e l'avvenuta ricezione[211].

Il novellato art. 254 c.p.p. si presta a ricomprendere le *e-mail*, considerato che gli uffici postali erogano, al pari di numerosi altri gestori iscritti in un apposito elenco, il servizio di posta elettronica certificata (PEC) che attribuisce valore legale alla consegna dei messaggi. I messaggi di posta elettronica sono, senza alcun dubbio, una forma di corrispondenza, suscettibile di inoltro, e come tale, sequestrabile presso fornitori di servizi; ma possono altresì essere considerati un «flusso di comunicazioni relativo a sistemi informatici o telematici», ai sensi dell'art. 266 *bis* c.p.p. Si pone a tal proposito un problema di più ampio respiro, relativo alla qualificazione giuridica delle operazioni di acquisizione probatoria delle *e-mail*[212].

Tra le novità della riforma, l'introduzione dell'articolo 254 *bis* c.p.p., che prevede una nuova ipotesi di sequestro, attuabile solo nei confronti dei fornitori di

[211] A. MACRILLÒ, *Le nuove disposizioni*, cit., p. 512 ss.
[212] La questione della captazione di *e-mail* è oggetto di un apposito paragrafo, a cui si rinvia. *Infra*, par. 6.2.

servizi telegrafici, telematici o di telecomunicazione. Con tale disposizione il legislatore ha voluto ribadire, *expressis verbis*, la generale sottoponibilità a sequestro di tutti i dati informatici in possesso dei gestori, compresi quelli di traffico o di ubicazione, la cui definizione è fornita dall'art. 1, lett. b e c del d.lgs. 109/2008, attuativo della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione[213].

I fornitori di servizi di cui all'art. 254 *bis* c.p.p., se non direttamente indagati nel procedimento penale, possono essere locatori dello spazio fisico (il *data center*) in cui l'indagato ha depositato il proprio *server*, possessori delle risorse fisiche su cui l'indagato ha memorizzato dati, informazioni e programmi (servizi di *hosting*), ovvero detentori di dati di varia natura (di traffico, amministrativi) relativi all'indagato o a terzi, significativi per l'indagine. Diverso nei tre casi il rapporto con il sequestro. Nel primo caso il *provider* è estraneo al sequestro e potrà al più consentire l'accesso dell'autorità giudiziaria al *data center*. Nella seconda ipotesi il *provider* potrà essere destinatario del provvedimento di sequestro quale soggetto presso cui si trovano le cose da sequestrare perché nell'*hosting* ha un ruolo attivo in quanto proprietario del *server* e detentore dei privilegi di accesso a livello di amministrazione del sistema. Nel terzo caso il sequestro è disposto direttamente a carico del *provider* in quanto unico possessore di quanto deve essere assoggettato al vincolo cautelare probatorio[214].

Il legislatore ammette la possibilità che tale attività di acquisizione dei dati avvenga mediante «copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità». Si mira così a contemperare le esigenze di ricerca della prova con le garanzie dei fornitori di servizi informatici e telematici, i quali, nella maggioranza dei casi rivestono lo *status* di terzo non indagato nel procedimento penale in cui è disposto il

[213] Ai sensi di tali disposizioni, si intende per *dati relativi al traffico* «qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione, ivi compresi i dati necessari per identificare l'abbonato» e per *dati relativi all'ubicazione* «ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico, ivi compresi quelli relativi alla cella da cui una chiamata di telefonia mobile ha origine o nella quale si conclude».

[214] In questi termini A. MONTI, *La nuova disciplina del sequestro informatico*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, cit., p. 210 ss.

sequestro e, soprattutto, con la necessità di assicurare una regolare fornitura dei servizi medesimi[215]. Infine, è imposto al fornitore di servizi di conservare e proteggere adeguatamente i dati originali[216].

L'art. 254 *bis* c.p.p. delinea una fattispecie di sequestro e, in quanto tale, può avere ad oggetto unicamente quei dati informatici che costituiscono corpo del reato o cosa pertinente ad esso, secondo la previsione generale dell'art. 253 c.p.p. A questo proposito occorre operare una distinzione tra reati informatici e "altri reati"; nel primo caso, infatti, i dati informatici costituiranno il mezzo mediante il quale il reato è stato commesso, cioè il corpo del reato. Per quanto riguarda, invece, altri reati, diversi da quelli informatici, ma per l'accertamento dei quali occorra procedere ad indagini su materiale informatico, la possibilità di sequestrare dati dipenderà principalmente dalla qualificazione degli stessi quali cosa pertinente al reato, costituendo gli stessi solo in rari casi corpo del reato.

Il concetto di "cose pertinenti al reato" è, e deve essere, secondo quanto insegna da tempo la Cassazione, generico, atto a comprendere tutte quelle *res* in rapporto indiretto con la fattispecie concreta e strumentali all'accertamento dei fatti[217]. Tuttavia, la stessa Corte sottolinea come l'identificazione, almeno nelle linee essenziali, delle cose da sequestrare e l'identificazione dello specifico valore probatorio rispetto ad una chiara fattispecie di reato devono, necessariamente, precedere l'attività di ricerca e apprensione del bene[218]. La precisazione si rivela di fondamentale importanza proprio con riferimento ai dati informatici: infatti, quando oggetto dell'attività di accertamento probatorio sono i dati informatici, tale nozione fluida di "cosa pertinente al reato" si presta a giustificare forme di sequestro "esplorativo", volte alla ricerca della *notitia criminis*, come tali inammissibili.

---

[215] Sono state espresse perplessità sulla scelta del legislatore italiano di prevedere la semplice possibilità dell'effettuazione della copia dei dati e non la sua obbligatorietà, come richiesto dalla Convenzione di Budapest. Si è pertanto auspicato che, in base ad una lettura costituzionalmente orientata e convenzionalmente conforme della norma, si proceda sempre alla acquisizione tramite copia dei dati informatici in questione. Cfr. S. VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, in L. LUPARIA (a cura di), Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, p. 140.

[216] Sul punto si veda, *infra*, par. 7 ss.

[217] Cfr. Cass., sez. III, 10 dicembre 2002, Camozza, in *C.E.D. Cass.,* n. 222974 e Cass., sez. III, 30 ottobre 2001, De Masi, *ivi*, n. 220114.

[218] Cfr. Cass., sez. I, 16 febbraio 2007, n. 25755, con nota di P. TROISI, *Sequestro probatorio del* computer *e segreto giornalistico*, in *Dir. pen. proc.*, 2008, p. 763 ss.

Profili di particolare interesse presenta, infine, il rapporto tra l'art. 254 *bis* c.p.p. e l'art. 132 codice *privacy*, i cui nuovi commi 4 *ter*, 4 *quater*, 4 *quinquies*[219] prevedono la possibilità per l'autorità procedente di ordinare ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive, ovvero per finalità di accertamento e repressione di specifici reati. Proprio in relazione a tale ultima previsione è configurabile una sovrapposizione tra i due strumenti in esame, che verrà approfondita nel prosieguo della trattazione[220].

L'art. 256, comma 1 c.p.p., come novellato nel 2008, attribuisce all'autorità giudiziaria il potere di ordinare ai soggetti indicati negli artt. 200 e 201 c.p.p. e a quelli titolari della facoltà di opporre il segreto di Stato, la consegna di dati, informazioni e programmi informatici dagli stessi detenuti per le ragioni afferenti all'esercizio dell'attività cui sono preposti. Incontra il favore di dottrina e giurisprudenza la previsione della possibilità di estrarre copia dei dati o dei programmi stessi su adeguato supporto, previa analisi *in loco* del contenuto degli elaboratori: in tal modo si riduce l'invasività dell'intervento ablativo e, soprattutto, non si pregiudica oltre misura la prosecuzione dell'attività da parte del soggetto interessato. Infatti, da tempo si criticavano le pratiche di sottoposizione a sequestro probatorio dell'intero *hardware* di proprietà di soggetti (come i giornalisti) tenuti al segreto professionale e sovente non indagati nel procedimento penale nel cui àmbito veniva disposto il provvedimento ablativo[221].

Per quanto riguarda la custodia delle cose sequestrate, quando oggetto di custodia siano dati, informazioni o programmi informatici, l'attuale formulazione del secondo comma dell'art. 259 c.p.p. prevede l'obbligo in capo al custode di impedirne l'alterazione o l'accesso da parte di terzi, salva in quest'ultimo caso diversa disposizione dell'autorità giudiziaria. Seppur già la prima parte del secondo comma dell'art. 259 c.p.p. imponga al custode obblighi di conservazione e presentazione

[219] Introdotti dalla stessa legge n. 48/2008.
[220] *Infra*, par. 7.4.
[221] Cfr. Cass., sez. I, 16 febbraio 2007, n. 25755, cit.; Cass., sez. VI, 31 maggio 2007, Sarzanini, con nota di A. MACRILLÒ, *Segreto* ex *art. 200 c.p.p. e sequestro del* computer *in uso al giornalista*, in *Dir. pen. proc*., 2008, p. 1416 ss.; A. CHELO MANCHÌA, *Sequestro probatorio di* computers, cit., p. 1634 ss.; A. MONTI, *No ai sequestri indiscriminati*, cit., p. 264 ss.

all'autorità giudiziaria delle cose sequestrate, la precisazione si rivela opportuna, tenuto conto della particolare natura dei dati informatici, soggetti, più di altri beni sequestrabili, a modificazione e cancellazione.

A completare il quadro delle modifiche apportate dalla legge 48/2008 alla disciplina del sequestro è l'art. 260 c.p.p., relativo all'apposizione dei sigilli alle cose sequestrate. In ossequio alle indicazioni contenute nell'art. 19, par. 3 della Convenzione di Budapest entra formalmente a far parte dell'ordinamento processuale il "sigillo elettronico"[222].

Quanto al secondo comma della norma, non resta che rinviare alle precisazioni fatte sopra, facendo la stessa riferimento alla necessità di effettuare una copia dei dati sequestrati su adeguati supporti in modo da garantirne la conformità all'originale e l'immodificabilità.

Il legislatore del 2008 ha attuato la Convenzione di Budapest insistendo sulla necessità che le operazioni di indagine e acquisizione probatoria di dati informatici siano condotte in modo da rispettare l'originalità del dato informatico. Proposizioni quali «adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione» (artt. 244, comma 2 e 247, comma 1*bis* c.p.p.), «acquisizione dei dati mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità» (art. 254 *bis* c.p.p.), «il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi» (art. 259, comma 2 c.p.p.), «quando si tratta di dati [...] la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità» (art. 260 c.p.p.), ricorrono nella maggior parte delle disposizioni novellate. Sicuramente si può convenire sull'opportunità di una simile disciplina che, ponendo fine alla criticata prassi consistente nell'asportazione dell'intero *computer* e relative periferiche, permette di evitare un'ingiustificata compressione della disponibilità del bene da parte del proprietario. Tuttavia, non si può tacere il fatto che, così operando, il legislatore ha dato cittadinanza nell'ordinamento processual-penalistico ad uno strumento dotato di considerevole potenzialità lesiva di diritti

[222] Precisazione peraltro superflua posto che la locuzione «con altro mezzo idoneo» già contenuta nel testo dell'art. 260, comma 1 si prestava a ricomprendere tale forma tecnologica di assicurazione delle cose sottoposte a sequestro.

fondamentali, senza predisporre una corrispondente adeguata tutela degli stessi. Non solo, ma rimanendo il destinatario di tale misura nella disponibilità del "bene originale", si vede altresì privato del diritto al riesame del provvedimento di sequestro, secondo quanto insegna la più recente giurisprudenza della Cassazione[223].

3.2 Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici: l'acquisizione di corrispondenza informatica

L'art. 9 comma 2 della legge 48/2008 ha novellato il secondo e terzo comma dell'art. 353 c.p.p. in materia di acquisizione di plichi o di corrispondenza ad opera della polizia giudiziaria. È stata innanzitutto riconosciuta alla polizia giudiziaria, su autorizzazione del pubblico ministero, la possibilità di prendere visione del contenuto di «plichi sigillati o altrimenti chiusi [che si abbia] motivo di ritenere contengano notizie utili alla ricerca e all'assicurazione di fonti di prova, che potrebbero andare disperse a causa del ritardo». Inoltre, si è estesa la tradizionale facoltà di sospendere l'inoltro di «lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza» alla corrispondenza in forma elettronica o inoltrata per via telematica. Infine, è stato ampliato il novero dei gestori di servizi destinatari dell'ordine della polizia giudiziaria: non più solo il servizio postale, ma anche quello telegrafico, telematico o di telecomunicazione. È così assicurata la corrispondenza, quanto ai destinatari, con i soggetti presso cui il pubblico ministero disporrà eventualmente il sequestro del materiale già acquisito dalla polizia giudiziaria (art. 254 c.p.p.)[224].

4. Questioni aperte in tema di perquisizione e sequestro di computer

Le scelte operate dal legislatore nel ratificare la Convenzione di Budapest sono criticabili sotto più profili e lasciano aperte alcune fondamentali questioni, tra loro interconnesse: la natura giuridica dell'attività di clonazione, cui è strettamente

[223] Cass., sez. un., 7 maggio 2008, n. 18253, con nota di S. CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. proc.*, 2009, p. 469 ss.; la Suprema Corte è ancora legata all'orientamento tradizionale che identifica l'interesse al riesame in quello alla restituzione della *res*. Sul punto si veda, *infra*, par. 4.3 ss.
[224] Cfr. A. BARBIERI, *Le attività d'indagine*, cit., p. 518.

collegato il problema dell'attuazione del contraddittorio con la difesa, le conseguenze derivanti dall'inosservanza delle *best practices* nel condurre le indagini informatiche, la persistenza dell'interesse al riesame del decreto di sequestro di *computer*, restituito dopo la clonazione dell'*hard disk*, il rischio di perquisizioni esplorative, che muovono alla ricerca della *notitia criminis*.

Tali aspetti problematici saranno oggetto di approfondimento nei successivi paragrafi.

4.1 Natura giuridica dell'attività di clonazione e attuazione del contraddittorio con la difesa

Come già anticipato, il *leitmotiv* della legge di ratifica della Convenzione *Cybercrime* è stato quello di imporre, nel condurre le indagini informatiche, il rispetto di metodi e tecniche in grado di garantire la conservazione dell'originale e di prevenire il rischio di alterazione di dati, informazioni, programmi contenuti nei sistemi informatici e telematici. Il legislatore non ha invece preso posizione in merito a quali modalità tecniche permettessero di raggiungere tale risultato, affidandosi piuttosto allo sviluppo tecnologico. Attualmente, le *best practices* suggeriscono di utilizzare la tecnica della *bit stream image*, che consente di ottenere una copia-clone del disco rigido, o di qualunque altro supporto di memoria.

I problemi derivano dal fatto che il legislatore ha "uniformato" la disciplina di ispezione, perquisizione, sequestro, accertamenti urgenti, prevedendo che tutti si svolgano con le stesse modalità tecniche. Ciò, da un lato rende ancora più sfumati i già labili confini tra le diverse attività di indagine informatica; dall'altro lato, fa sorgere l'interrogativo circa la corretta qualificazione dell'attività di clonazione, che di esse costituisce il presupposto[225].

Probabilmente sarebbe stato opportuno introdurre norme *ad hoc* per la disciplina delle attività investigative informatiche, anziché percorrere la strada dell'estensione dei tradizionali mezzi di ricerca della prova al mondo digitale.

[225] Se ispezioni e perquisizioni sono divenute attività ripetibili, lo stesso non si può dire con riferimento alla clonazione del supporto di memoria, su cui poi tali operazioni insisteranno. *Infra*, par. 5.

La principale questione che si è posta in riferimento alla qualificazione dell'attività di clonazione dell'*hard disk* è se si tratti di atto ripetibile o irripetibile[226].

Come noto, manca nel codice di rito una definizione di atto irripetibile; a ciò hanno sopperito dottrina e giurisprudenza. Tradizionalmente sono stati definiti non ripetibili gli atti «il cui oggetto sia suscettibile di modificazione, talché l'eventuale ripetizione successiva dell'accertamento che lo concerna risulti impossibile od inutile, non potendosene riproporre con caratteri identici le condizioni o il contesto»[227]. Due categorie di atti rientrano nel concetto di atto irripetibile: quelli non differibili e quelli non reiterabili. I primi sono quelli che vertono su persona, cosa o luogo soggetto a modificazione inevitabile, a prescindere dal compimento dell'atto stesso (art. 360 c.p.p.)[228]; i secondi sono quegli atti che diventano non ripetibili in conseguenza dell'accertamento stesso (art. 117 disp. att. c.p.p.)[229].

Per quanto riguarda in particolare l'effettuazione della copia-clone, a fronte di chi ritiene di poterla qualificare come attività irripetibile solo in quanto indifferibile, ossia perché il suo oggetto è destinato a modificazione inevitabile[230], vi è chi sostiene che, anche quando non riguardino dati in procinto di modificarsi, le indagini

[226] La *ratio* della novella del 2008, infatti, pare proprio essere quella di rendere ispezioni e perquisizioni - atti normalmente irripetibili - concernenti supporti informatici o telematici attività sempre ripetibili in futuro. In tale senso devono leggersi le prescrizioni riguardanti l'adozione di «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». Una volta ottenuta la copia-clone dell'*hard disk*, sarà possibile estrarne un numero infinito di copie su cui svolgere successive e ripetute analisi. Resta evidentemente il problema di stabilire se quest'ultima attività sia ripetibile o meno.

[227] La citazione è ripresa da C. CESARI, *L'irripetibilità sopravvenuta degli atti di indagine*, Milano, 1999, p. 48, che a sua volta riprende concetti espressi da D. POTETTI, *Svolta restrittiva della Cassazione in tema di atto irripetibile*, in *Cass. pen*., 1996, p. 1468, G. ICHINO, *Gli atti irripetibili e la loro utilizzazione dibattimentale*, in G. UBERTIS (a cura di), *La conoscenza del fatto nel processo penale*, Milano, 1992, p. 114, F. CORDERO, *Codice di procedura penale commentato*, Torino, II edizione, 1992, p. 516.

[228] R. E. KOSTORIS, *I consulenti tecnici nel processo penale*, Milano, 1993, p. 155, li definisce anche «atti non ripetibili per cause estrinseche». L'Autore peraltro, con specifico riferimento agli accertamenti tecnici, individua un concetto più ristretto di non rinviabilità dell'atto, riferibile non al dibattimento, ma all'incidente probatorio, i cui tempi di attivazione risultano incompatibili con la specifica situazione di urgenza. Il riferimento è all'art. 360, comma 4 c.p.p. e alla riserva di incidente probatorio proponibile dalla persona sottoposta alle indagini, che può essere disattesa dal pubblico ministero nel caso in cui gli accertamenti, se differiti, «non possano più essere utilmente compiuti».

[229] R. E. KOSTORIS, *I consulenti tecnici*, cit., p. 156 li definisce «atti non rinnovabili per cause intrinseche».

[230] È evidente infatti che i dati, le informazioni e i programmi contenuti in un sistema informatico o telematico sono soggetti a continua e rapida modifica. Per queste osservazioni si veda E. LORENZETTO, *Le attività urgenti*, cit. p. 148. L'Autrice giunge a tale conclusione sulla base della considerazione che in occasione del primo accesso alla fonte di prova digitale è consentito individuare il dato ma non apporvi variazioni unilaterali; tale affermazione è fatta in relazione alle attività di accertamento urgente *ex* art. 354, comma 2 c.p.p.

informatiche causino comunque mutazioni irreversibili, integrando la fattispecie dell'art. 117 disp. att. c.p.p.[231].

Strettamente connessa, e parzialmente sovrapponibile alla questione della ripetibilità o meno dell'attività di clonazione, è quella della qualificazione giuridica di essa quale accertamento o mero rilievo. Il codice del 1989 non fornisce una definizione di tali attività di indagine, ma la dottrina maggioritaria ritiene che il legislatore abbia sostanzialmente recepito le elaborazioni sviluppate nella vigenza del codice Rocco. Ne deriva che gli accertamenti tecnici possono essere qualificati come un'attività di tipo critico-valutativo, mentre i rilievi sono attività «aventi lo scopo di acquisire in via immediata e con elaborazione critica elementare dati della realtà, vale a dire materiale probatorio grezzo, destinato ad essere rielaborato in sede di indagini tecniche e peritali»[232].

Con specifico riferimento alle attività che insistono su dati, informazioni e programmi informatici si è affermato che le operazioni di rilevamento consistono in una «mera osservazione, individuazione ed acquisizione di dati», gli accertamenti invece comportano «un'opera di studio critico, di elaborazione valutativa ovvero di giudizio di quegli stessi dati»[233].

È di tutta evidenza che dalla qualificazione dell'attività di clonazione quale atto ripetibile o irripetibile, quale accertamento o rilievo, discenderanno conseguenze diverse in relazione all'attuazione del contradditorio tecnico con la difesa.

La giurisprudenza pressoché unanime qualifica l'attività di clonazione dell'*hard disk* del *computer* come attività ripetibile, e la inquadra nella categoria dei rilievi (art. 354 c.p.p.)[234]; qualche sporadica pronuncia fa riferimento agli accertamenti tecnici ripetibili (art. 359 c.p.p.)[235].

---

[231] In questi termini, M. DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, p. 440.

[232] R. E. KOSTORIS, *I consulenti tecnici*, cit., p. 141.

[233] Le citazioni sono di E. APRILE, *Le indagini tecnico-scientifiche: problematiche giuridiche sulla formazione della prova penale*, in *Cass. pen.*, 2003, p. 4035.

[234] Cass., sez. I, 9 marzo 2011, n. 17244, in *Cass. pen.*, 2012, p. 440, con nota di M. DANIELE, *Il diritto al preavviso*, cit.; Cass., sez. I, 30 aprile 2009, n. 23035, Corvino, in *C.E.D. Cass.*, n. 244454; Cass., sez. I, 1 aprile 2009, n. 16942, inedita; Cass., sez. I, 11 marzo 2009, n. 12472, Izzo, inedita; Cass., sez. I, 5 marzo 2009, n. 14511, Aversano Stabile, in *Cass. pen*., 2010, p. 1520, con nota di E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia,* e con nota di A. E. RICCI, Digital evidence *e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc.*, 2010, p. 337; Cass., sez. I, 26 febbraio 2009, n. 15153, inedita. Conforme anche Cass., sez. I, 25 febbraio 2009, 11503, Dell'Aversano, in *CED Cass*., n.

Ricorrente è l'affermazione per cui «*non rientra nel novero degli atti irripetibili l'attività di estrazione di copia di* file *da un* computer *oggetto di sequestro, dal momento che essa non comporta alcuna attività di carattere valutativo su base tecnico-scientifica, né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità d'informazioni identiche a quelle contenute nell'originale*»[236].

Seguendo questa impostazione, il contraddittorio tecnico con la difesa è spostato ad un momento successivo e addirittura è considerato onere dell'imputato dimostrare che non sono state seguite le *best practices* e che ciò ha portato ad un'alterazione dei dati[237].

Tale orientamento non può essere condiviso innanzitutto perché trascura di considerare che qualsiasi ingresso in un sistema informatico può alterare i dati in esso contenuti, generando mutazioni che, anche se minimali, rischiano di risultare decisive; inoltre in quanto mostra di sottovalutare le competenze tecniche necessarie per condurre operazioni di *computer forensics*[238].

Più variegato il panorama dottrinale. A fianco di chi la considera un'ispezione [239], non manca chi condivide l'impostazione giurisprudenziale menzionata e annovera l'attività di clonazione dei supporti di memoria informatici tra i rilievi, in quanto si tratterebbe di mera repertazione di dati pertinenti al reato, e

243495; in quest'ultima pronuncia, tuttavia, si fa riferimento ad una generica lettura dell'*hard disk* sequestrato, pare quindi che non fosse stata nemmeno effettuata la copia clone.

[235] Cass., sez. I, 26 febbraio 2009, n. 11863, Ammutinato, in *C.E.D. Cass.*, n. 243922, laddove si legge «*correttamente invero per l'estrazione dei dati contenuti nel supporto informatico - essendo l'accertamento all'evidenza ripetibile se eseguito, come non è dubbio sia avvenuto nel caso di specie, da personale esperto perfettamente in grado di evitare la perdita dei dati medesimi - è stato applicato l'art. 359 c.p.p. e non l'art. 360 c.p.p.*».

[236] Cfr. giurisprudenza citata *supra*, note 234, 235.

[237] Cass., sez. I, 25 febbraio 2009, n. 11503, cit., in cui si statuisce che 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. Conformi, Cass., sez. III, 2 luglio 2009, n. 38087, Cinti, in *C.E.D. Cass.*, n. 244928; Cass., sez. I, 30 aprile 2009, cit., Cass., sez. I, 1 aprile 2009, cit.

[238] Cfr. L. LUPARIA, *La disciplina processuale e le garanzie difensive*, in L. LUPARIA, G. ZICCARDI, *Investigazione penale*, cit., p. 151; P. P. PAULESU, *Notizia di reato e scenari investigativi complessi: contrasto alla criminalità organizzata, operazioni "sotto copertura", captazione di dati digitali*, *Riv. dir. proc.*, 2010, p. 801; P. TONINI, *Documento informatico e giusto processo*, *Dir. pen. proc.*, 2009, p. 404. In tal senso anche E. CASEY, *What does "forensically sound" really mean?*, *Digital investigation*, 2007, f. 4, p. 49.

[239] A. CISTERNA, *Perquisizioni in caso di fondato motivo*, in *Guida dir.*, 2008, 16, p. 66 ss.

non sarebbero richieste particolari competenze tecniche, ulteriori rispetto a quelle che l'uomo medio, e quindi anche gli inquirenti, devono possedere[240].

La conseguenza è che tali operazioni possono essere compiute dalla polizia giudiziaria senza darne preavviso alla persona sottoposta alle indagini e al suo difensore[241] e che, se irripetibili, i relativi verbali confluiranno nel fascicolo per il dibattimento e saranno acquisiti tramite lettura *ex* art. 511 c.p.p.[242].

L'orientamento dottrinale prevalente ritiene che la raccolta di prove digitali vada inquadrata nella categoria degli accertamenti tecnici, poiché richiede il possesso di specifiche competenze tecnico-informatiche ed implica già un'attività critico-valutativa.

All'interno di questo filone interpretativo è possibile distinguere tra chi ritiene che l'acquisizione (*rectius*: clonazione) integri sempre un'attività irripetibile e vada pertanto svolta nel rispetto della procedura prevista dall'art. 360 c.p.p., ossia 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[243], e chi invece non esclude a priori il ricorso all'accertamento tecnico ripetibile di cui all'art. 359 c.p.p., ma ritiene che la scelta vada fatta caso per caso. Circa l'individuazione del criterio discretivo, tuttavia, gli interpreti si differenziano ulteriormente. Alcuni fanno riferimento alle metodologie utilizzate, di talché solo se l'azione si uniformi a canoni condivisi, idonei ad assicurare la corretta preservazione del dato digitale ed *ex post* controllabili, sarà possibile annoverarla tra gli atti

---

[240] In tal senso, da ultimo, F. M. MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, p. 1259 ss. Si veda anche, S. FASOLIN, *La copia di dati informatici nel quadro delle categorie processuali*, in *Dir. pen. proc.*, 2012, p. 372 ss.; G. ZICCARDI, *Manuale breve di informatica giuridica*, Milano, 2006, p. 204 ss. Classifica l'attività in esame quale accertamento tecnico ripetibile, G. VACIAGO, Digital evidence, cit., p. 89, il quale afferma che «è evidente che nel momento stesso in cui venga rispettata la procedura di acquisizione *bit-stream* dell'immagine del disco e sia verificata, attraverso il calcolo dell'algoritmo di *hash*, la perfetta identità della copia, non vi sono ragioni per ritenere irripetibile tale accertamento tecnico». L'Autore peraltro esprime perplessità in merito al totale disinteresse della giurisprudenza verso il mancato rispetto delle procedure di *digital forensics* idonee a garantire la non alterazione del dato.

[241] Si applica l'art. 356 c.p.p. che richiama l'art. 354 c.p.p. relativo agli accertamenti urgenti della polizia giudiziaria.

[242] S. FASOLIN, *La copia di dati*, cit., pur classificando tale attività di indagine quale mero rilevo, riconosce che non sia possibile stabilire in maniera univoca se si tratti di attività ripetibile o irripetibile perché ciò dipende dal tipo di operazione concretamente posta in essere. Copiare un supporto non modificabile, come *cd* o *dvd* non riscrivibili, è diverso dal copiare un supporto modificabile, quale *hard disk*, memorie *USB*.

[243] In questo senso, P. TONINI, *Documento informatico*, cit., p. 405; A. E. RICCI, Digital evidence *e irripetibilità*, cit., p. 345; S. VENTURINI, *Sequestro probatorio*, cit., p. 130.

irripetibili, in caso contrario, ossia se non si sono seguite le *best practices* e non è quindi possibile verificare la *chain of custody*, se ne dovrà dedurre che «l'attività ha comportato un'irreversibile modifica dell'oggetto digitale, il quale ultimo potrà essere preso in considerazione solo ove assistito nella fase originaria di captazione dal contraddittorio preventivo ex art. 360 c.p.p.»[244].

Questa interpretazione non può essere condivisa, innanzitutto perché fa riferimento ad una valutazione che può essere fatta solo *ex post*, dando peraltro per scontato che se si seguono le *best practices* non si alterano i dati, mentre se non le si rispettano ciò porta inevitabilmente ad una modifica, e poi in quanto sembra implicitamente sostenere che la presenza del tecnico della difesa giustifichi l'adozione di tecniche meno rigorose nello svolgere l'accertamento informatico.

Altra parte della dottrina, partendo dal presupposto che in alcuni casi il preavviso alla difesa può nuocere alle indagini - alto è infatti il rischio che l'indagato cancelli gli elementi a suo carico o ne comprometta il valore conoscitivo - propone una «graduazione del contraddittorio tecnico»[245]. Secondo tale tesi, quando hanno ad oggetto dati nella potenziale disponibilità dell'indagato, le indagini informatiche andrebbero svolte nella forma degli atti a sorpresa, ai quali il difensore ha diritto di assistere senza preavviso[246]. La più garantita procedura degli accertamenti tecnici non ripetibili andrebbe osservata, al contrario, quando in rapporto al caso concreto il pericolo della distruzione delle prove non sussiste. In tal caso, l'inosservanza dell'obbligo di preavviso al difensore *ex* art. 360, comma 1 c.p.p., integrerebbe una

[244] In questi termini, E. LORENZETTO, *Le attività urgenti*, cit., p. 148. L. LUPARIA, *I profili processuali*, cit., p. 720, segnala la circostanza che si tratta di criterio seguito da alcune Procure della Repubblica, le quali procedono nelle forme semplificate di cui all'art. 359 c.p.p. ove la metodologia adottata garantisca verificabilità *ex post* ovvero attivando il contraddittorio preventivo di cui all'art. 360 c.p.p. quando l'elevata componente scientifica della rilevazione possa acuire il rischio di modificazione dei dati rilevati.

[245] M. DANIELE, *Caratteristiche della prova digitale*, in F. RUGGIERI, L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale*, cit., p. 203 ss.; ID., *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 283 ss.

[246] M. DANIELE, *Caratteristiche*, cit., p. 212, qualifica la raccolta delle prove digitali come accertamento tecnico e da ciò fa derivare la necessità di integrare le norme in tema di ispezioni, perquisizioni e sequestri con quelle che prescrivono l'intervento di appositi esperti in tutti gli stadi del procedimento. Quindi, dopo che il pubblico ministero ha assunto la direzione delle indagini, con il disposto dell'art. 359 c.p.p.

nullità a regime intermedio poiché si tratta di disposizione che riguarda l'assistenza dell'indagato (artt. 178, lett. c e 180 c.p.p.)[247].

Infine, va segnalata quella teoria per la quale il provvedimento di clonazione dell'*hard disk* del *computer* integrerebbe un'autonoma forma di sequestro[248]. Tale impostazione appare assolutamente condivisibile perché individua la specificità dell'attività volta ad ottenere una copia dei supporti di memoria digitale, rispetto ad un tradizionale provvedimento *ex* art. 258 c.p.p. Resta il fatto però che, pur integrando le disposizioni in materia di sequestro con quelle in tema di accertamento tecnico, il contraddittorio con la difesa resta meramente eventuale; infatti, il difensore avrà sì il diritto a presenziare alle operazioni, ma senza preavviso (art. 365 c.p.p.)[249].

4.2 Conseguenze derivanti dal mancato rispetto delle misure tecniche

Come si è già avuto modo di evidenziare, data la natura ontologicamente volatile e modificabile dei dati digitali, è necessario che le indagini informatiche siano condotte attraverso metodi e tecniche in grado di preservarne la genuinità, l'integrità e la non modificabilità. A tal fine è necessario che sia rispettata la c.d. catena di custodia, ossia che le varie operazioni di *computer forensics* siano condotte in modo tale da non alterare i dati e, soprattutto, che esse siano documentate[250]. L'autenticità e la verificabilità della prova digitale è presupposto per il suo successivo utilizzo da parte del giudice ai fini della decisione. In quest'ottica sarebbe ideale che il legislatore prestabilisse «una specifica tecnica di acquisizione delle

[247] M. DANIELE, *Il diritto al preavviso*, cit., p. 442. Ritengono, al contrario, sussistente un'ipotesi di inutilizzabilità L. LUPARIA, Computer crimes *e procedimento penale*, in G. GARUTI (a cura di), *Modelli differenziati di accertamento*, vol. VII, t. I, Torino, 2011, p. 388; F. GIUNCHEDI, *Gli accertamenti tecnici irripetibili*, Torino, 2009, p. 2009, p. 136; in giurisprudenza, in questo senso Cass., sez. III, 10 febbraio 2010, n. 16387, inedita. In entrambi i casi peraltro l'effetto è l'azzeramento del valore conoscitivo dell'atto; diverso è invece l'arco temporale della rilevabilità e il c.d. effetto di propagazione dell'invalidità, che non si produce nel caso di nullità riguardanti le prove (art. 185, comma 4 c.p.p.).

[248] S. CARNEVALE, *Copia e restituzione*, cit., p. 481 ss.

[249] Sul punto, si veda diffusamente *infra*, par. 4.3.2.

[250] Valga un esempio per tutti. Nel noto caso di Garlasco, l'iniziale impossibilità di stabilire la validità o meno della prova d'alibi è dipesa dal fatto che il *computer* fosse stato esaminato senza rispettare le basilari regole di *computer forensics*.

prove digitali, da osservare scrupolosamente a pena di inutilizzabilità ogni volta in cui un reato lasciasse tracce in un sistema informatico»[251].

Tuttavia, l'informatica è una scienza ancora relativamente giovane, la tecnologia evolve molto rapidamente in questo settore – alto è il rischio di obsolescenza - e non c'è per il momento un metodo consolidato e verificato che possa assurgere a «*regola d'ora* della formazione della prova digitale»[252]. Gli stessi esperti riconoscono che la scelta del metodo dipenderà in concreto dalla situazione che si presenta agli investigatori[253].

Da questo punto di vista è sicuramente apprezzabile la scelta del legislatore del 2008 di non individuare specifiche modalità di conduzione delle investigazioni informatiche, ma di rinviare a quelle che, nella parabola dell'evoluzione scientifica, saranno le migliori tecniche di *computer forensics.*

Ciò, tuttavia, fa sorgere il quesito di quali siano le sanzioni applicabili nel caso in cui le investigazioni informatiche non siano state condotte seguendo le *best practices*. Tre le possibili soluzioni.

Secondo un primo orientamento, l'adozione di «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione», integrerebbe uno speciale requisito – con finalità garantista – che andrebbe sempre rispettato quando si procede ad ispezione o perquisizione di sistemi informatici o telematici. Si tratterebbe di un elemento costitutivo delle fattispecie investigative, la cui violazione determinerebbe la nullità del mezzo di ricerca della prova ai sensi degli artt. 178 lett. c) e 180 c.p.p. per violazione delle garanzie difensive[254].

Altra parte della dottrina ritiene invece integrata un'ipotesi di inutilizzabilità *ex* art. 191 c.p.p.[255]. Il mancato rispetto delle migliori tecniche di *computer forensics* nella raccolta della *digital evidence* sarebbe infatti da ricondurre ad una situazione di inidoneità probatoria della risultanza in sé e di qualsiasi ulteriore mezzo di prova

[251] In questi termini, M. DANIELE, *Caratteristiche*, cit., p. 211.
[252] *Ibidem*, p. 211. L'espressione, riferita all'esame incrociato, è di P. FERRUA, *La regola d'oro del processo accusatorio: l'irrilevanza probatoria delle contestazioni*, in R. E. KOSTORIS (a cura di), *Il giusto processo, tra contraddittorio e diritto al silenzio*, Torino, 2002, p. 11 ss.
[253] A. GRILLO, U. E. MOSCATO, *Riflessioni sulla prova informatica*, in *Cass. pen.*, 2010, p. 375 ss.
[254] A. VITALE, *La nuova disciplina*, cit., p. 509.
[255] E. LORENZETTO, *Le attività urgenti*, cit. p. 162 ss. Prima della riforma del 2008, in tal senso anche L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit. p. 197.

finalizzato ad analizzarla, tale per cui il giudice dovrebbe escluderle già in fase di ammissione della prova[256].

Infine, alcuni Interpreti ritengono che la questione si risolva sotto il profilo della valutazione della prova (art. 192 c.p.p.)[257]. Non sarebbe, infatti, possibile ravvisare né un caso di nullità né un'ipotesi di inutilizzabilità in quanto ciò equivarrebbe a ricavare divieti probatori dalla sola lesione dell'interesse tutelato dalla legge, ma privi in realtà di un'espressa copertura normativa[258]. Spetterebbe quindi al giudice, avvalendosi dell'apporto dei periti e dei consulenti tecnici della difesa, valutare se le indagini siano state condotte in maniera corretta e se sia stata rispettata la *chain of custody*.

4.3 Il riesame e il problema dell'interesse ad impugnare

Ai sensi dell'art. 257 c.p.p., contro il decreto di sequestro, l'imputato, la persona alla quale le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione possono proporre richiesta di riesame, anche nel merito, a norma dell'art. 324 c.p.p.

---

[256] Ciò sul presupposto che il requisito di idoneità probatoria richiamato espressamente come requisito per l'ammissione della prova atipica dall'art. 189 c.p.p., debba valere come presupposto implicito anche della prova tipica. Sul punto, si veda C. BRUSCO, *La valutazione della prova scientifica*, in *Dir. pen. proc.*, 2008, suppl. al n. 6, p. 27. Con specifico riferimento alle indagini informatiche, L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit. p. 197, riconnette al difetto di genuinità della *digital evidence* l'inutilizzabilità del materiale raccolto per *unreliability*, ossia per inidoneità delle evidenze ad assicurare un accertamento attendibile dei fatti di reato. S. VENTURINI, *Sequestro probatorio*, cit., p. 125, ritiene che nel caso di inosservanza dei protocolli investigativi debba operare la categoria dell'inutilizzabilità, in quanto tali protocolli «sono ormai assurti al rango di imprescindibili linee guida destinate ad operare come affidabili chiavi ermeneutiche che colorano e completano il sistema normativo».

[257] M DANIELE, *Caratteristiche*, cit., p. 212 ss., aderendo all'impostazione di N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Padova, 1992, p. 139 ss.; G. BRAGHÒ, *L'ispezione e la perquisizione*, cit., p. 190 ss. In giurisprudenza v. già Trib. Bologna, 22 dicembre 2005, Vierika, in *Dir. Internet*, 2006, p. 153 ss., con nota di L. LUPÀRIA, *Il caso "Vierika": un'interessante pronuncia in materia di* virus *informatici e prova penale digitale - I profili processuali*. Critico nei confronti di questa impostazione L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit. p. 198, il quale intravvede in ciò «un rischioso intreccio tra "libertà di valutazione" e "libertà di acquisizione" che il riformatore del 1988 aveva voluto sciogliere definitivamente» e teme quindi che «la materia della *digital evidence* si trasformi in un'occasione per effettuare "salti all'indietro" nella nostra storia processuale».

[258] Per la necessità che le inutilizzabilità siano esplicitamente costituite dalla legge processuale nella forma dei divieti di acquisizione, si veda F. CORDERO, *Procedura penale*, IX ed., 2012, Milano, p. 619 ss. Ammette l'assenza di chiare previsioni di inutilizzabilità anche A. MONTI, *La nuova disciplina*, cit., p. 217.

Secondo l'impostazione tradizionale, finalità del riesame è la restituzione della *res* alla persona che ne era stata spossessata. *Nulla quaestio* quando oggetto del sequestro è un bene materiale, di cui esiste un solo esemplare; perplessità sorgono, invece, quando il pubblico ministero, avvalendosi del potere conferitogli dall'art. 258 c.p.p., abbia estratto copia della documentazione restituita. Al verificarsi di una simile evenienza, il destinatario del provvedimento di sequestro risulta privo di tutela. Infatti, essendo stata la *res* originale restituita, egli non potrà chiedere il riesame per carenza di interesse; inoltre, considerato che l'estrazione di copie *ex* art. 258 c.p.p. è un provvedimento autonomo e distinto rispetto al sequestro, e in ossequio al principio di tassatività delle impugnazioni, lo stesso è privo, altresì, di qualsiasi rimedio per ottenere la restituzione delle copie.

Il problema, già rilevante e al centro di acceso dibattito in dottrina e giurisprudenza, assume importanza fondamentale alla luce della nuova disciplina delle indagini informatiche: l'attuale tendenza degli investigatori, nel rispetto delle novellate disposizioni in materia di sequestro, è quella di non asportare il supporto contenente i dati informatici, ma "limitarsi" ad estrarne copia su adeguato supporto che garantisca la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. Già nell'ipotesi in cui vengano trattenute le copie di documenti cartacei, privando il destinatario di simile misura di qualsiasi mezzo per ottenerne la restituzione, si lamenta un vuoto di tutela, ma quando oggetto di sequestro e successiva estrazione di copia siano dati informatici conservati nell'*hard-disk* del *computer* o in altre memorie digitali (penne *USB*, lettori *mp3*, *smartphones*, *tablets*, *etc.*), la mancanza di uno strumento che permetta di riottenere le copie del materiale sequestrato, diviene intollerabile. Infatti, sull'*hard-disk* di un *computer* è salvata un'ingente quantità di dati, la maggior parte dei quali assolutamente irrilevante per le indagini.

L'orientamento tradizionale e ad oggi ancora maggioritario[259], nel caso in cui la *res* sequestrata sia restituita, individua un'ipotesi tipica di carenza di interesse al riesame – originaria o sopravvenuta a seconda del momento in cui viene proposta impugnazione rispetto al momento della restituzione dei beni – in quanto il risultato tipico cui tende l'impugnazione, ovvero il dissequestro, è già stato raggiunto. Non

[259] Da ultimo si veda la recente sentenza della Cassazione, sez. un., 7 maggio 2008, n. 18253, in *Dir. pen. proc.*, 2009, p. 496 ss., con nota di S. CARNEVALE, *Copia e restituzione*, cit.

mancano, tuttavia, pronunce e orientamenti dottrinali di segno contrario, di cui è opportuno offrire una breve panoramica.

4.3.1 Interesse alla legalità, interesse alla pronuncia e interesse alla prova

Secondo una prima ricostruzione, nonostante la restituzione dell'originale, sarebbe ammissibile l'istanza di riesame in quanto diretta a verificare che l'uso del mezzo di acquisizione probatoria sia avvenuto nei casi ed entro i limiti previsti dalla legge[260]. Obiettivo del controllo incidentale sarebbe quindi una verifica circa l'osservanza dei limiti posti dalla disciplina processuale all'uso dei poteri investigativi, una mera esigenza di riaffermazione della legalità. Ciò si scontra, tuttavia, con la giurisprudenza consolidata della Cassazione che con fermezza nega l'ammissibilità di impugnazioni miranti a conseguire fini astratti: occorre che la pronuncia abbia ripercussioni concrete[261]. L'indagine circa l'ammissibilità del riesame deve, quindi, prendere le mosse dai risultati concretamente conseguibili con l'impugnazione, considerando tutta la gamma dei vantaggi prospettabili per l'impugnante, compresi quelli indiretti e secondari e la meritevolezza di tutela degli stessi secondo l'ordinamento.

Nella consapevolezza di tale necessità, altra parte della dottrina, seppur minoritaria, e alcune pronunce giurisprudenziali, ammettono il riesame di un provvedimento di sequestro di cosa restituita in quanto volto ad ottenere una decisione che accerti la consistenza degli elementi a carico della persona sottoposta alle indagini, in vista di positive ripercussioni sul procedimento principale[262]. Il ricorrente sarebbe, in questo caso, mosso da un c.d. interesse alla pronuncia, cioè mirerebbe ad ottenere un titolo attestante un vizio processuale, da far valere negli stadi più avanzati del procedimento. Così facendo si dimenticano, tuttavia, i rapporti tra il procedimento incidentale e quello principale. Si possono a tal proposito

[260] Cass., sez. VI, 31 maggio 2007, Sarzanini, cit., p. 1416 ss.; Cass., sez. V, 13 settembre 1990, Menci, in *Arch. n. proc. pen.*, 1991, p. 293 ss.
[261] Cass., sez. un., 13 dicembre 1995, Timpani, in *Cass. pen.*, 1995, p. 788 ss.; Cass., sez. un., 24 marzo 1995, Boido, *ivi*, p. 3308 ss.; Cass., sez. un., 11 maggio 1993, Amato, *ivi*, 1993, p. 2808 ss.
[262] Tra questi, E. TURCO, *Legittimazione ed interesse ad impugnare in tema di sequestro preventivo: dualismo teorico?*, in *Cass. pen.*, 2003, p. 2382 ss. e Cass., sez. VI, 1 luglio 2003, Ronco, in *Cass. pen.*, 2005, p. 914 ss., con nota di R. CANTONE, *Sulla riesaminabilità del decreto di sequestro probatorio di cose già restituite*.

richiamare i risultati a cui già la dottrina era giunta in tema di provvedimenti restrittivi della libertà personale: le conclusioni in tema di *fumus commissi delicti* raggiunte in sede cautelare sono insuscettibili di travalicare i confini del procedimento incidentale[263].

Ne consegue, quindi, che anche quando la catena dei controlli sul provvedimento ablativo conduca ad una pronuncia della Cassazione, la quale abbia riscontrato una fragilità dell'impianto accusatorio, il procedimento principale resterebbe impermeabile a simile valutazione. Il che significa, ai fini che in questa sede rilevano, che un gravame volto a tale unico scopo sarebbe da qualificare astratto, risolvendosi in un controllo sulla mera correttezza del provvedimento impugnato, inidoneo ad assicurare all'impugnante alcuna pratica utilità.

A completare il quadro delle diverse ricostruzioni relative all'interesse al riesame, quella che ravvede in tale mezzo di impugnazione un rimedio volto ad ottenere l'espunzione dal materiale probatorio delle informazioni raccolte a seguito del sequestro. Il ricorrente sarebbe, quindi, mosso da un c.d. interesse alla prova, cioè dall'interesse ad impedire l'uso probatorio del patrimonio conoscitivo ottenuto dagli investigatori, che si assume abbiano agito deviando dai parametri di legge.[264] Questa

[263] L'unica disposizione che creava un collegamento tra procedimento cautelare e processo principale, era quella dell'art. 405, comma 1 *bis* c.p.p., che imponeva al pubblico ministero di chiedere l'archiviazione quando la Corte di Cassazione, adita ai sensi dell'art. 311 c.p.p., si fosse pronunciata circa l'insussistenza di quei gravi indizi di colpevolezza che avrebbero giustificato l'applicazione di una misura cautelare personale, e non fossero stati acquisiti successivamente ulteriori elementi a carico della persona sottoposta alle indagini. Tale comma, già non applicabile alle cautele reali, a causa dell'espresso richiamo dallo stesso compiuto all'art. 273 c.p.p., e a maggior ragione non riferibile al sequestro probatorio, è stato dichiarato costituzionalmente illegittimo dalla Corte Costituzionale. Cfr. C. cost., 24 aprile 2009, n. 121, p. 1367, in *Dir. pen. proc.*, 2009, con nota di C. CONTI, *Incostituzionale la richiesta coatta di archiviazione: la consulta tra principio di incidentalità e di preclusione*. Va dato atto, tuttavia, di un più recente intervento legislativo, suscettibile di alterare i rapporti tra processo principale e incidente cautelare. Il riferimento è al pacchetto sicurezza del 2008 che ha introdotto nel codice di rito il c.d. giudizio immediato custodiale. Tale rito si instaura sul presupposto dello *status* custodiale della persona sottoposta alle indagini, a condizione che la misura sia stata confermata in sede di riesame o siano decorsi i termini per proporre simile gravame. Non è chiaro cosa succeda se una volta instaurato il giudizio immediato, intervenga la pronuncia della Cassazione, adita *ex* art. 311 c.p.p. che dichiari l'insussistenza dei presupposti di applicazione della misura. Sul punto si rinvia a R. ORLANDI, *Note critiche, a prima lettura, in tema di giudizio immediato "custodiale" (art. 453 1° co. bis c.p.p.)*, in *Osservatorio del processo penale*, 2008, n. 3, p. 10; E. VALENTINI, *La poliedrica identità del nuovo giudizio immediato*, in AA.VV. *Misure urgenti in materia di sicurezza pubblica: (d.l. 23 maggio 2008, n. 92 conv. in legge 24 luglio 2008, n. 125)*, O. MAZZA, F. VIGANÒ (a cura di), Torino, 2008, p. 281 ss.

[264] S. CARNEVALE, *Copia e restituzione*, cit., p. 476. In tal senso anche alcune pronunce della Corte di Cassazione, tra cui Cass., sez. I, 1 dicembre 2005, Galletti, in *C.E.D. Cass.* n. 233402. In dottrina si vedano G. TRANCHINA, *Sequestro* (voce), in *Enc. giur. Treccani*, XXVIII, Roma, 1992, p. 6 ss. e S. MONTONE, *Sequestro penale* (voce), in *Dig. disc. pen.,* XIII, Torino 1997, p. 260 ss.

impostazione è respinta da coloro che, al contrario, negano che il riesame possa costituire la sede per ottenere una statuizione anticipata sulla non fruibilità in giudizio del materiale appreso: a tal fine possono essere sollevate eccezioni di nullità, inammissibilità o inutilizzabilità nel corso del procedimento principale.

4.3.2 Solo l'interesse alla restituzione della res *può giustificare il riesame: l'intervento delle Sezioni Unite*

L'andamento ondivago della giurisprudenza della Cassazione e il conseguente smarrimento degli interpreti è dovuto al silenzio della legge sugli effetti dell'accoglimento dell'istanza di riesame. Il codice di rito nulla dice circa le possibili ripercussioni che la pronuncia incidentale, in questo specifico caso, sia in grado di produrre sul processo principale, diversamente da quanto accade, ad esempio, in materia di intercettazioni, ove è prevista una verifica preliminare sulla legittimità delle operazioni (art. 268, commi 6 e 7 c.p.p.).

Nodo centrale dell'intera questione riguarda le copie estratte dei dati informatici in possesso dell'autorità inquirente e l'uso che delle stesse può essere fatto; infatti, come emerge da alcune pronunce "illuminate"[265], il fine ultimo cui tende colui che chiede il riesame di un provvedimento di sequestro di cose restituite, è proprio la restituzione o la distruzione delle copie. Allo stato attuale, tale obiettivo sembrerebbe impossibile da raggiungere.

La soluzione del problema passa inevitabilmente attraverso la qualificazione dell'attività di estrazione di copie di cui all'art. 258 c.p.p., anche alla luce delle modifiche introdotte dalla legge 48 del 2008[266], e sulla definizione dei rapporti tra tale attività e quella prodromica di sequestro.

Proprio sui rapporti tra sequestro e attività *ex* art. 258 c.p.p. e sulla possibile esistenza di un autonomo interesse alla restituzione delle copie si soffermano le Sezioni Unite della Cassazione in una recente sentenza[267], che delude le aspettative,

[265] Cass., sez. VI, 31 maggio 2007, Sarzanini, cit.; Trib. Brescia, ord. 4 ottobre 2006, in *Giur. Merito*, 2007, p. 1100 ss.; Cass., sez. II, ord. 22 febbraio 1995, Magliuolo, in *Riv. pen.*, 1996, p. 248 ss.

[266] Le novellate disposizioni in materia di perquisizione e sequestro, nello specifico ambito delle indagini informatiche, sono destinate a soppiantare quelle, ormai inadeguate dell'art. 258 c.p.p., che non è stato toccato dalla riforma.

[267] Cass., sez. un., 7 maggio 2008, cit., p. 469.

adagiandosi sulla soluzione tradizionale al problema anziché sviluppare importanti aspetti della questione che, peraltro, già erano emersi in precedenti pronunce della stessa Corte[268].

Preliminare è l'esatta individuazione del rapporto intercorrente tra sequestro ed estrazione di copie. Sul punto, la Suprema Corte non ha dubbi: l'attività *ex* art. 258 c.p.p. è autonoma e distinta rispetto al sequestro e l'ordine di estrazione di copie non è una manifestazione della sopravvivenza del sequestro.

Ciò emergerebbe innanzitutto da un'interpretazione letterale del comma 1 dell'art. 258 c.p.p., il quale nel disciplinare l'attività di estrazione di copie opera un *distinguo* a seconda che il sequestro degli originali sia mantenuto o meno, lasciando intendere che la restituzione dell'originale al privato esaurisce l'efficacia del provvedimento di sequestro probatorio facendo venir meno ogni interesse al riesame. Ad analoga conclusione si può giungere anche sulla base di altre argomentazioni; infatti, il presupposto dell'acquisizione di copie non è indefettibilmente collegato al sequestro probatorio, potendo avvenire all'esito di consegna spontanea o di adempimento al dovere di esibizione. Non solo, ma anche quando l'attività di estrazione di copia sia collegata al sequestro, non per questo ne costituisce un'automatica conseguenza. La decisione di estrarre copia è frutto di autonoma determinazione discrezionale (gli originali possono essere restituiti senza che ne sia stata estratta copia) e richiede, quindi, una autonoma giustificazione della rilevanza probatoria dell'acquisizione che non può esaurirsi nella semplice menzione dell'esistenza di un pregresso provvedimento di sequestro. Corollario di tali argomentazioni è che il provvedimento di acquisizione di copie, stante il principio di tassatività delle impugnazioni, non è soggetto a riesame o altre forme di gravame.

Queste conclusioni non sono, tuttavia, a detta della stessa Corte, risolutive; infatti, escludere la possibilità di fare istanza di riesame del provvedimento di estrazione di copie, non significa negare che, attraverso il riesame del sequestro di cui sia cessata l'efficacia per restituzione della cosa, si possa comunque evitare che le copie estratte ai sensi dell'art. 258 c.p.p. entrino a far parte del materiale probatorio.

[268] Il riferimento è a Cass., sez. VI, 31 ottobre 2007, 40380, cit., p. 1416 ss., in cui la Suprema Corte, relativamente ad un'ipotesi di sequestro di *computer* presso terzo non indagato, aveva riconosciuto che lo scopo dell'impugnazione, travalicato il limite della questione inerente alla mera disponibilità della *res*, finisce con l'investire tematiche più complesse, riconducibili alla tutela dei diritti della personalità.

E ciò perché, pur essendo avvenuta la restituzione, l'eventuale declaratoria di irritualità del sequestro, e conseguente annullamento, travolgerebbe anche il successivo ordine di estrazione di copie, al primo intimamente connesso, secondo la nota teoria dei "frutti dell'albero avvelenato"[269].

La Suprema Corte, tuttavia, non si sofferma sul tema dell'invalidità derivata del provvedimento di estrazione di copie considerandolo un argomento non decisivo, dal momento che, anche a voler ammettere la trasmissione del vizio dall'originale alle copie, non si potrebbe affermare la sussistenza, a fondamento dell'istanza di riesame, di un interesse alla restituzione delle copie.

Due sono gli argomenti portati dalla Corte di Cassazione a sostegno dell'inammissibilità di un riesame che miri esclusivamente alla restituzione delle copie in vista della sottrazione delle stesse dalla piattaforma probatoria. Innanzitutto, l'interesse a riappropriarsi di queste ultime non potrebbe considerarsi attuale, poiché il loro utilizzo ai fini di prova è, al momento dell'impugnazione, del tutto incerto ed eventuale. Infatti, il pubblico ministero potrebbe non chiederne mai l'acquisizione probatoria ovvero il giudice stesso potrebbe bloccarne l'ingresso nella piattaforma probatoria. Si sottolinea, inoltre, in proposito che altri sono gli strumenti che il legislatore mette a disposizione della parte che si voglia opporre all'acquisizione di prove che assume viziate: le eccezioni. Il rilievo è senza dubbio pertinente, ma vale solo per l'imputato e nelle ipotesi in cui allo stesso siano date possibilità d'intervento preventivo rispetto ad un provvedimento da emanare – il che non accade, ad esempio, quando le copie a disposizione del pubblico ministero vengano allegate ad una domanda cautelare - [270].

Centrale e risolutivo è, comunque, l'altro argomento addotto dalla Corte: la pronuncia incidentale, a qualunque risultato essa tenda, non fa stato nel processo principale. La decisione presa in sede di riesame non sarebbe comunque il grado di vincolare il giudice del processo principale circa l'ammissibilità o l'utilizzabilità delle informazioni contenute nelle copie.

[269] Ciò, ovviamente, solo nel caso in cui l'estrazione di copie sia effettivamente conseguenza di un precedente sequestro, cosa che non sempre avviene.
[270] S. CARNEVALE, *Copia e restituzione*, cit., p. 477. Nella prassi recente si assiste a frequenti casi di sequestro di *computer* presso terzi, non indagati nel processo di riferimento e che, quindi, non possono sollevare alcuna eccezione per lamentare l'irregolarità del provvedimento di acquisizione probatoria.

Logica conseguenza di tali affermazioni è che l'unico risultato perseguibile con il riesame è la restituzione della cosa o la riespansione dei diritti su di essa.

Un cenno merita, infine, un ultimo passaggio della sentenza in commento, non pienamente condivisibile. I sostenitori della tesi contraria a quella sposata dalle Sezioni Unite fanno leva, per suffragare l'esistenza di un interesse ulteriore rispetto a quello alla mera restituzione della *res*, sul dato testuale: gli artt. 257 e 322 c.p.p., nell'indicare i soggetti legittimati ad impugnare il provvedimento di sequestro, distinguono tra l'imputato e la persona a cui le cose sono state sequestrate o vanno restituite, lasciando così intendere che l'iniziativa dell'imputato potrebbe fondarsi su un titolo diverso da quello alla restituzione[271]. Le Sezioni Unite "superano" il rilevo affermando che la legge indica sì i soggetti legittimati al gravame, ma che l'impugnazione deve pur sempre essere sorretta da un interesse attuale e concreto, giusto il disposto del comma 4 dell'art. 568 c.p.p. Sicuramente è corretto sostenere che nel giudizio circa la legittimazione ad impugnare si debba verificare non solo l'astratta titolarità, ma anche la sussistenza di un interesse all'impugnazione; ciò tuttavia non significa che si possa partire dalle conclusioni già raggiunte in tema di interesse per svuotare di significato la previsione normativa. Il dato normativo rappresenta un punto fermo, mentre la verifica sui fini del gravame è affidata all'interpretazione; ne consegue che proprio il novero dei soggetti legittimati impone di ravvisare casi in cui l'interesse prescinda dall'esigenza di riappropriarsi del bene[272].

4.3.3 Le questioni non risolte dalle Sezioni Unite

Con la sentenza in parola le Sezioni Unite hanno perso l'occasione per pronunciarsi su un tema di sempre maggiore attualità e che provoca crescente preoccupazione. Limitandosi ad un'interpretazione rigorosamente legata al dettato

[271] Tale argomento si rivela comunque insoddisfacente ai fini della soluzione del problema dell'interesse ad impugnare nel caso in cui a chiedere il riesame, proprio per ottenere la restituzione delle copie, sia un terzo, non indagato nel processo penale. Il riferimento è al noto caso del sequestro, e successiva estrazione di copie, del *computer* di un giornalista di Repubblica ai fini della ricerca di una *e-mail* da questi inviata ad una collega e contenente varia documentazione informatica relativa al procedimento penale concernente il sequestro di Abu Omar. Cfr. Cass., sez. I, 16 febbraio 2007, Cavallo, in *Dir. pen. proc.*, 2008, p. 763 ss.

[272] Così S. CARNEVALE, *Copia e restituzione*, cit., p. 479.

normativo, hanno perso di vista quella che costituisce l'esigenza primaria in situazioni analoghe a quella sottoposta al loro esame: la tutela dei dati personali salvati sui supporti informatici da cui viene estratta copia. L'intera disamina circa la sussistenza di un possibile interesse alla restituzione delle copie resta comunque legata all'individuazione di un obiettivo ulteriore: l'affermazione di illegittimità del provvedimento in vista di riflessi nell'ambito del procedimento principale o la non acquisizione al materiale probatorio delle copie stesse. Il risultato a cui si giunge è coerente con le premesse: il riesame non sarebbe ammissibile, nel primo caso perché la pronuncia incidentale non produce alcun effetto vincolante nel processo principale, nel secondo, perché l'interesse non sarebbe attuale.

In nessun passo della sentenza emerge, al contrario, la prospettazione di un *mero* interesse alla restituzione delle copie in quanto contenenti dati personali, irrilevanti per le indagini e, soprattutto non pertinenti al reato e quindi che neppure avrebbero potuto essere sequestrati!

A tal proposito in dottrina, è stata prospettata l'esistenza di un interesse ulteriore al riesame: quello alla restituzione del dato. Si sottolinea infatti come «il prelievo di informazioni da un *personal computer*, […] attuato con tecniche di clonazione, riduce sensibilmente il sacrificio delle esigenze di fruizione del bene, ma è in grado di vulnerare interessi d'altra natura, [quali] impedire che i propri dati personali restino a disposizione degli inquirenti al di fuori dei casi consentiti, controllarne gli usi, verificarne la pertinenza rispetto agli scopi perseguiti, fino ad ottenerne la restituzione qualora difettino i presupposti per il loro trattenimento»[273]. Ne deriva la necessità di riconoscere l'interesse del destinatario del provvedimento alla "restituzione dell'informazione", qualora il sequestro sia eseguito in violazione dei requisiti previsti dalla legge.

In realtà, il problema importante, non affrontato dalla Cassazione, è quello della natura dell'attività di estrazione di dati informatici, che è cosa ben diversa dalla semplice estrazione di copie. Prova ne sia il fatto che, con specifico riferimento al sequestro di dati presso fornitori di servizi, ma applicabile più in generale al sequestro di materiale informatico, il novellato art. 254 *bis* c.p.p. qualifica l'attività di copiatura dei dati come una modalità del sequestro, mentre le Sezioni Unite si sono

[273] S. CARNEVALE, *Copia e restituzione*, cit., p. 479.

prodigate a sottolineare che sequestro e attività di estrazione di copie sono provvedimenti distinti e indipendenti. La Suprema Corte non ha, forse, colto la rilevante differenza che sussiste tra la copia di un documento cartaceo e quella della memoria di un *computer*: se anche nel primo caso è assolutamente opportuno garantire all'interessato la restituzione della copia, oltre che dell'originale, nel secondo, impedire che gli inquirenti rimangano a disposizione di dati personali, irrilevanti per le indagini, corrisponde ad un preciso diritto fondamentale dell'interessato: quello all'autodeterminazione informativa.

Il legislatore del 2008 ha predisposto specifiche modalità di ispezione, perquisizione e sequestro di materiale informatico, che già di per sé determinano la creazione di una copia dei dati esaminati. Inutile è, dunque, il richiamo all'art. 258 c.p.p. e alla sua autonomia rispetto al sequestro. L'attività volta all'apprensione di dati elettronici non va qualificata come sequestro del *computer* e successiva estrazione di copie, ma, più opportunamente, come sequestro dei dati informatici contenuti nel *computer* stesso [274]. Così precisata la questione, è inevitabile riconoscere il diritto dell'interessato alla restituzione, non tanto delle copie, quanto dei dati digitali, in tutti gli esemplari che di essi sussistono[275]. Vana l'individuazione di un interesse ulteriore al riesame, che si scontrerebbe inevitabilmente con le solide argomentazioni della Cassazione, ma anche inutile, posto che, anche aderendo all'orientamento tradizionale, è possibile tutelare l'interessato. Infatti, purché si ammetta che oggetto del sequestro sono i dati informatici, è ravvisabile un interesse alla restituzione fino a quando tutti i supporti su cui tali dati sono stati trascritti, non siano restituiti.

Resta, tuttavia, sempre attuale il problema della tutela dei dati personali, della segretezza e riservatezza delle comunicazioni, che non appare sufficientemente garantito dal riconoscimento del diritto a ottenere la restituzione o distruzione

[274] S. CARNEVALE, *Copia e restituzione*, cit., p. 481, sostiene che la clonazione dell'*hard disk* non sia una semplice attività di conservazione di tracce, bensì un vero e proprio sequestro di materiale conoscitivo. Il problema della qualificazione dell'attività di copiatura dei dati informatici è emerso anche in Germania nell'ambito del dibattito relativo alle perquisizioni *online*. Il *Bundesverfassungsgericht*, ancora una volta illuminante sul punto, ha già nel 2005 qualificato tale attività come sequestro dei dati informatici, con tutte le conseguenze che ne derivano. Cfr. *BVerfG*, *2BvR 1027/02* consultabile in *www.bundesverfassungsgericht.de* e M. KEMPER, *Anforderung und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten*, in *Zeitschrift für Rechtspolitik*, 2007, p. 105 ss. Per quanto riguarda l'ordinamento statunitense, si veda, *infra*, par. 4.4.1.

[275] Da intendersi come diritto alla disponibilità esclusiva dei propri dati.

(analogamente a quanto avviene per le intercettazioni in sede di udienza di stralcio) del materiale in possesso dell'autorità inquirente. La tutela, in questo caso, dovrebbe essere precedente al sequestro, impedendo l'apprensione stessa di informazioni personali, non pertinenti al reato e, quindi, irrilevanti per le indagini[276].

4.4 Rischio di perquisizioni esplorative e tutela dei dati personali

Restano da esaminare due ulteriori aspetti problematici, quello della tutela dei dati personali e quello strettamente correlato del rischio che le indagini informatiche, da mezzo di ricerca di prove di un reato già commesso si trasformino in strumento di ricerca della *notitia criminis*[277].

Infatti, sul *computer* – ma lo stesso vale per altri dispositivi digitali di memoria – è normalmente salvata un'ingente quantità di dati personali, molti dei quali irrilevanti per le indagini. Si pone il problema di come garantire la tutela di tali dati, soprattutto in considerazione del fatto che la tecnica oggi ancora non consente accessi selettivi al dispositivo, miranti ad apprendere solo i *files* che interessano e che quindi, per verificare se un *file* sia rilevante o meno è quasi sempre necessario aprirlo e visionarne il contenuto. A ciò va aggiunta la circostanza che non sempre il dispositivo sequestrato appartiene alla persona sottoposta a procedimento penale, il che rende ancora più insidiose tali modalità d'indagine e ancora più urgente la necessità di approntare specifici strumenti di tutela per l'interessato.

Inoltre, la prassi di sequestrare, tramite clonazione, l'intero *hard disk* del *computer* – o l'intero dispositivo di memoria - rischia di trasformare il sequestro probatorio, da vincolo da porre su cose che hanno caratteristiche tali da servire all'accertamento dei fatti, a inammissibile strumento a carattere "esplorativo"[278]. Significative a tal proposito sono le pronunce della Cassazione in tema di sequestro di *computer* di un giornalista in cui si è dichiarata l'illegittimità del provvedimento di

[276] Sul punto si rinvia a *infra*, par. 5.
[277] Come insegna Dürrenmatt nell'opera *Die Panne*: «un reato si finisce sempre per trovarlo».
[278] Cfr. R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, p. 129 ss., in particolare p. 136, il quale riconosce che il limite della *notitia criminis* è assai fragile di fronte alle perquisizioni e ai sequestri di materiale informatico. Tuttavia, la funzione della notizia di reato di prevenire possibili abusi di polizia e pubblico ministero va riaffermata con forza: «se così [non] fosse sarebbero aperte le porte all'arbitrio dell'inquirente, il quale avrebbe nella perquisizione e nel sequestro due formidabili strumenti per cercare quel che vuole, non quel che deve».

sequestro – *rectius*: di clonazione dell'*hard disk* – per eccessiva genericità, in quanto «il sequestro probatorio [deve] rispettare il principio di proporzionalità tra il contenuto del provvedimento e le esigenze di accertamento dei fatti, evitando quanto più è possibile indiscriminati interventi invasivi nella sfera professionale e/o privata»[279].

Entrambe le questioni verranno esaminate prendendo spunto dall'esperienza statunitense.

4.4.1. La soluzione statunitense al rischio di perquisizioni esplorative

La disciplina di perquisizione e sequestro è contenuta direttamente nella Costituzione americana, segnatamente nel IV Emendamento, che tutela i cittadini nei confronti di perquisizioni e sequestri irragionevoli, e richiede che tali attività d'indagine siano condotte sulla base di un mandato, supportato da un fondato motivo, che descriva in maniera dettagliata il luogo da perquisire e le cose da sequestrare[280].

In assenza di leggi processuali positive, il compito di stabilire quando un'attività d'indagine sia ragionevole e quando si debbano applicare le garanzie costituzionali è stato naturalmente assunto dalla Corte Suprema, il cui *case law* ha progressivamente delineato un sistema di regole volto a tracciare un equo bilanciamento tra esigenze investigative e tutela dei singoli, che passa attraverso la qualificazione di una determinata attività come perquisizione o sequestro.

La ricerca di informazioni all'interno di un *hard disk* è considerata una perquisizione. Controversa è invece la qualificazione come sequestro della procedura di clonazione del disco rigido; infatti, il concetto di sequestro è tradizionalmente legato all'idea di spossessamento, ciò che non si verifica – se non per un brevissimo

[279] Cass., sez. II, 9 dicembre 2011, in *Cass. pen.*, 2012, p. 2999 ss.; si veda anche Cass., sez. I, 16 febbraio 2007, Pomarici, n. 25755, in *Cass. pen.*, 2008, p. 2956 ss., con nota di A. LOGLI, *Sequestro di* un personal computer. *Misure* ad explorandum *e tutela della corrispondenza elettronica*; Cass., sez. III, 31 maggio 2007, Sarzanini, cit., p. 1416 ss.; E. APRILE, *Sequestro del* computer *di un giornalista, clonazione della relativa memoria e tutela del segreto professionale*, in *Dir. Internet* 2007, p. 585 ss.

[280] Letteralmente, il IV Emendamento recita: «*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*».

lasso di tempo - nel caso in cui si crei una "semplice" copia[281]. La Corte Suprema non si è ancora pronunciata in merito[282]; tuttavia, parte della dottrina propende per la classificazione dell'attività di clonazione quale sequestro, poiché, benché l'interessato rimanga nella disponibilità del proprio *computer*, egli perde il diritto ad essere l'utilizzatore esclusivo dei *files* in esso salvati[283].

Alla qualificazione di tali attività come perquisizione e sequestro segue l'applicabilità della c.d. *Fourth Amendment doctrine*, ossia della giurisprudenza elaborata in merito al IV Emendamento. La trasposizione di tale dottrina nel campo delle indagini informatiche, tuttavia, presenta alcune criticità, soprattutto con riguardo ai classici strumenti usati per circoscrivere l'ampiezza di una perquisizione ed evitare che essa muova alla ricerca della *notitia criminis*, ossia restrizioni *ex ante* e limiti di utilizzabilità *ex post*[284]. L'obiettivo di evitare che la perquisizione divenga esplorativa è tradizionalmente perseguito dalla c.d. *plain view doctrine*, con cui si cerca di ottenere un bilanciamento tra l'interesse dei cittadini alla tutela della *privacy* nei confronti di attività d'indagine particolarmente invasive e la necessità di perseguire quei reati, le cui prove siano trovate casualmente nel corso di una perquisizione per un diverso reato[285].

La *plain view doctrine* costituisce un'eccezione al IV Emendamento, poiché rende legittimi, sussistendo determinate condizioni, la scoperta prima e il sequestro poi, di prove o di un *corpus delicti* diverso rispetto a quello per il quale si sta

---

[281] *Arizona v. Hicks*, *480 U.S. 321 (1987)*; *Maryland v. Macom*, *472 U.S. 463 (1985)*; *United States v. Jacobsen*, *466 U.S. 109 (1984)*. In *Arizona v. Hicks*, la Corte Suprema ha stabilito che il copiare informazioni non costituisce un sequestro poiché non vi è interferenza con alcun interesse possessorio dell'interessato.

[282] La Corte Suprema potrebbe applicare il precedente di *Arizona v. Hicks* ai *computers*, e quindi negare che l'attività di clonazione sia un sequestro, oppure, in considerazione della diversità dell'oggetto, discostarsi da *Hicks* e qualificare tale attività come sequestro. Ritiene preferibile quest'ultima soluzione, O. S. Kerr, *Searches and Seizures in a Digital World*, in *119 Harv. L. Rev. 531 (2005)*, *558*.

[283] S. W. BRENNER, B. A. FREDERIKSEN, *Computer Searches and Seizures: Some Unresolved Issues*, in *8 Mich. Telecomm. Tech. L. Rev., 39 (2001/2002)*; O. S. KERR, *Searches and Seazures*, cit.

[284] La c.d. *exclusionary rule*, elaborata dalla Corte Suprema in *Weeks v. United States*, *232 U.S. 383 (1914)* quale corollario del divieto di perquisizioni e sequestri irragionevoli, prevede l'inutilizzabilità probatoria di quanto ottenuto in violazione del IV Emendamento. Cfr. O. S. KERR, *The Fourth Amendment and New technologies: Constitutional Myths and the Case for Caution*, in 102 *Mich. L. Rev.*, 801 (2004).

[285] Funzione analoga è svolta nell'ordinamento tedesco dal § 108 *StPO*, che disciplina il sequestro di cose casualmente rinvenute nel corso di una perquisizione, pertinenti ad un reato diverso da quello per cui si procede, il c.d. *Zufallsfund*, prevedendo che esse vengano temporaneamente sequestrate e che del sequestro venga immediatamente informato il pubblico ministero. Nell'ordinamento italiano manca invece una previsione simile.

conducendo una perquisizione, e che quindi non risultano autorizzati dal mandato, come richiesto dalla norma costituzionale.

Affinché il sequestro di cose non specificate nel mandato sia legittimo, occorre che esse appaiano in *plain view*: l'originaria perquisizione dev'essere condotta nel rispetto del IV Emendamento; dev'essere inoltre evidente la natura incriminatrice dell'oggetto rinvenuto; infine, chi sta svolgendo attività d'indagine, deve avere legittimo accesso al luogo nel quale l'oggetto si trova[286].

Nel campo delle perquisizioni di *computer*, tuttavia, non è possibile emettere mandati sufficientemente specifici e, quindi, autorizzare la perquisizione di un *hard disk* significa permettere l'apertura di ogni *file* per verificarne la rilevanza[287]. Ne consegue che tutto apparirà in *plain view* e sarà sequestrabile legittimamente pur in assenza di mandato, con l'effetto di vanificare la funzione della *plain view doctrine*,

[286] Infatti, posto che il mandato dovrà indicare in maniera specifica il luogo da perquisire e le cose da ricercare, nel caso in cui sia necessario aprire un contenitore, sarà possibile aprire solo quei contenitori al cui interno sia ragionevole ritenere vi siano cose del tipo di quelle ricercate. Classico esempio è quello della perquisizione di un'abitazione alla ricerca di armi, nel corso della quale si rivenga droga; se quest'ultima viene trovata all'interno di un contenitore che astrattamente potrebbe contenere armi, essa sarà legittimamente sequestrabile ai sensi della *plain view doctrine*; se, al contrario, la si rinviene in un contenitore troppo piccolo per poter ospitare armi, non si applicherà la *plain view doctrine* ed essa, in base alla *exclusionary rule*, sarà inutilizzabile come prova. La sanzione dell'inutilizzabilità funge quindi da deterrente nei confronti di perquisizioni esplorative.
In origine si pretendeva altresì che la scoperta fosse accidentale (c.d. *inadvertent discovery*, *Coolidge v. New Hampshire, 403 U.S. 443 (1971)*). Prendendo atto delle ontologiche difficoltà che si incontrano nell'indagare la sussistenza di requisiti di natura soggettiva, la Corte Suprema ha successivamente eliminato tale presupposto, sulla base della considerazione che lo scopo di evitare perquisizioni eccessivamente ampie, alla ricerca della *notitia criminis*, sarebbe già raggiunto attraverso la necessità che il mandato descriva in maniera dettagliata il luogo da perquisire e le cose da sequestrare. Ciò infatti, limitando lo scopo della perquisizione, renderebbe di per sé illegittimo il sequestro di cose trovate al di fuori dei luoghi che si potevano lecitamente perquisire, senza necessità di ricercare la volontà di colui che ha fatto la scoperta (*Horton v. California, 496 U.S. 130 (1990)*).

[287] Le *lower courts* sono spesso costrette ad ammettere che autorizzare la perquisizione di un *computer* alla ricerca di determinate prove, equivalga a permettere la perquisizione di tutto l'*hard disk*. Infatti, la considerevole quantità e varietà di dati salvati su *computer*, la circostanza che *files* rilevanti per l'accertamento siano mescolati a *files* certamente irrilevanti, e che esternamente essi appaiano tutti uguali, rendono particolarmente arduo il rispetto della previsione costituzionale. Vani i tentativi di parte della dottrina, di alcune *lower courts* e del *Department of Justice* di individuare dei correttivi affinché i mandati siano quanto più possibile dettagliati, ed in grado quindi di limitare l'ampiezza della perquisizione al fine di emettere mandati quanto più specifici possibile. Non è infatti possibile fare affidamento sull'estensione del *file*, che potrebbe essere artatamente modificata. Richiedere che il mandato specifichi il protocollo di ricerca da utilizzare contrasta innanzitutto con i precedenti della Corte Suprema in materia (*Dalia v. United States*, *441 U.S. 238 (1979)*, tale decisione riguarda le perquisizioni di documenti cartacei ma è stata applicata anche a quelle di dati digitali), e comunque è quantomeno arduo per i giudici, non esperti di *computer forensics*, stabilire a priori come una perquisizione digitale debba essere condotta. Infine, anche una ricerca per parole chiave, che allo stato sembra la soluzione migliore, trova un limite in *files* criptati o altrimenti protetti o modificati. Cfr. O. S. KERR, *Searches and Seizures,* cit., 876; A. V. MOSHIRNIA, *Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in Digital Domain,* 23 *Harv. J. Law & Tec.*, *609*, 625 (2010).

in palese violazione del IV Emendamento. Ciò da un lato dimostra l'inefficacia, quando la perquisizione abbia ad oggetto un *computer*, degli strumenti elaborati per restringerne *ex ante* l'ampiezza, dall'altro mette in luce l'esigenza di apprestare un idoneo sistema di limitazioni *ex post* all'uso probatorio del materiale rinvenuto, onde evitare che, ottenuto un mandato per un determinato reato, si sfrutti l'accesso al *computer* per ricercare prove di altri e distinti reati.

Tra le diverse reazioni di dottrina e giurisprudenza[288], merita di essere segnalato quel filone interpretativo, nato all'interno del *Ninth Circuit*, il quale

[288] Vanno menzionate anche soluzioni diverse, emerse nella prassi. Secondo un primo orientamento, che muove dall'equiparazione del *computer* ad un qualsiasi contenitore chiuso con numerosi documenti, non ci sarebbe bisogno di adottare regole nuove nel campo delle perquisizioni informatiche e la *plain view doctrine* andrebbe applicata così com'è, essendo sufficiente, a tutela della *privacy,* che la natura incriminatrice dell'oggetto sia immediatamente percepibile. Le radici di tale approccio affondano direttamente nei precedenti della Corte Suprema, la quale da un lato ammette, nel caso di perquisizione avente ad oggetto grandi quantità di documenti cartacei, che documenti irrilevanti vengano velocemente passati in rassegna, al preliminare scopo di stabilire se possano essere sequestrati in base al mandato che si è ottenuto (*Andersen v. Maryland, 472 U.S. 463 (1976)*); dall'altro afferma che il IV Emendamento, con tutto il corollario di principi e dottrine, sia applicabile indifferentemente a cose tangibili e intangibili (*Warden v. Hayden, 387 U.S. 294 (1967)*). Tale approccio è stato adottato da *United States v. Williams, 592 F. 3d 511 (4th Circuit 2010)*. In dottrina si veda, K. BRUEGGEMANN WARD, *The Plain (or not so Plain) View Doctrine: Applying the Plain View Doctrine to Digital Seizures,* in *79 U. Cin. L. Rev. 1163 (2011)*.
Una variante di questo orientamento cerca di adattare la *plain view doctrine* al mondo delle indagini digitali applicando un bilanciamento tra contrastanti esigenze: la tutela della *privacy* del destinatario della perquisizione e l'interesse della società alla repressione dei reati. Così, si ammette il sequestro di prove di reati diversi rispetto a quello per cui è stato ottenuto il mandato solo se la gravità dell'ulteriore reato è tale da far prevalere le esigenze collettive su quelle individuali e quindi, da giustificare una compressione del diritto alla riservatezza dell'interessato. Cfr. A. V. MOSHIRNIA, *Separating Hard Fact from Hard Drive,* cit., 627.
Prendendo atto che equiparare l'intero *computer* ad un qualsiasi contenitore chiuso è estremamente riduttivo, parte della dottrina e della giurisprudenza considera ogni singolo *file* un contenitore a sé, ed avverte la necessità di introdurre correttivi alla *plain view doctrine* nel caso in cui oggetto di indagine sia un *hard disk*, recuperando quel requisito della *inadvertent discovery* che la Corte Suprema aveva eliminato all'inizio degli anni '90. Secondo questo diverso orientamento, ogni *file* visionato, che non rientri nello scopo dell'originaria perquisizione, è sequestrabile solo se scoperto accidentalmente; altrimenti risulterebbe acquisito in assenza di mandato, e sarebbe pertanto inutilizzabile. I sostenitori di questo approccio giustificano la deviazione dai precedenti della Corte Suprema che hanno eliminato tale requisito (*Horton v. California,* cit.), sulla base delle differenze sussistenti tra perquisizioni "classiche" e perquisizioni informatiche; solo nel primo caso, infatti, le dimensioni dell'oggetto limitano lo scopo dell'attività di indagine e rendono superflua la ricerca dell'intenzione di colui che la sta conducendo. Ciò tuttavia contrasta con il già citato orientamento della Corte Suprema che non ravvisa differenze tra proprietà fisica e proprietà digitale nell'applicazione della *Fourth Amendment doctrine*. (*Warden v. Hayden,* cit.). Inoltre, rimarrebbe la difficoltà oggettiva di ricercare l'intenzione di colui che svolge la perquisizione. Hanno seguito quest'impostazione, *United States v. Mann, 592 F. 3d 779 (7th Circuit 2010)*; *United States v. Walser, 275 F. 3d 981 (10th Circuit 2001)*; *United States v. Cary, 172 F. 3d 1268 (10th Circuit 1999)*. In dottrina, D. C. BEHAR*, An Exception to an Exception: Officer Inadvertence as a Requirement to Plain View Seizures in the Computer Context,* in *66 U. Miami L. Rev. 471 (2012)*; N. HOOD*, No Requirement Left Behind: The Inadvertent Discovery Requirement. Protecting Citizens One File at a Time,* in *45 Val. U. L. Rev. 1529 (2011)*.

muovendo dal problema di come condurre perquisizioni aventi ad oggetto grandi quantità di documenti cartacei, arriva a teorizzare che le perquisizioni informatiche vengano condotte da tecnici indipendenti e terzi rispetto al procedimento penale, a garanzia della riservatezza dei dati personali salvati sul *computer*. L'origine di tale indirizzo giurisprudenziale va ricercata nella difficoltà di eseguire mandati di perquisizione, emessi per ricercare determinati documenti cartacei, quando questi siano mescolati a grandi quantità di documenti irrilevanti e l'operazione di selezione *in loco* si presenti quindi particolarmente impegnativa. La risposta giurisprudenziale è stata nel senso di esigere che gli investigatori chiedessero l'autorizzazione a sequestrare tutti i documenti e a provvedere alla selezione successivamente, in separata sede[289]. Nell'auspicare l'applicazione di tale regola anche nel campo delle indagini informatiche, parte della dottrina ne ha suggerito l'integrazione con ulteriori requisiti: l'indicazione da parte del giudice degli specifici protocolli di ricerca da utilizzare, una forma di controllo giurisprudenziale *ex post* sull'operato di coloro che hanno eseguito la perquisizione, al fine di verificare che abbiano aperto solo *files* che avevano ragionevole motivo di considerare rilevanti, e la partecipazione della difesa al momento in cui si esegue la perquisizione, con possibilità di indicare diversi

---

L'orientamento più radicale prevede la disapplicazione della *plain view doctrine* nel campo delle perquisizioni di *computer*; ciò avrebbe l'effetto di rendere illegittima, perché in violazione del IV Emendamento, la scoperta di materiale estraneo allo scopo del mandato, e inutilizzabili, in applicazione della *exclusionary rule*, le prove eventualmente sequestrate. Parte della dottrina considera questa la soluzione migliore allo stato attuale; infatti, la sanzione dell'inutilizzabilità probatoria di quanto rinvenuto al di fuori dello scopo del mandato costituirebbe un efficace deterrente nei confronti di perquisizioni esplorative. Al contempo, ciò non significherebbe necessariamente la dispersione di preziose informazioni, né costituirebbe un freno alla repressione dei reati, risultando comunque applicabili due eccezioni alla *exclusionary rule*, quali la *independent source rule* (elaborata dalla Corte Suprema in *Murray v. United States, 487 U.S. 533 (1988)*) e la *inevitable discovery rule* (elaborata dalla Corte Suprema in *Nix v. Williams, 467 U.S. 431 (1984)*), in base alle quali tali prove sarebbero comunque utilizzabili a condizione che gli inquirenti riescano a dimostrare di avere ottenuto quelle informazioni da una fonte indipendente oppure che la loro scoperta fosse inevitabile. Questa soluzione è stata adottata da *United States v. Comprehensive Drug Testing Inc., 579 F. 3d 989 (9th Circuit 2009)*.
Tali apprezzabili sforzi interpretativi muovono comunque dalla premessa che sia legittimo aprire i *files* per verificarne la rilevanza. E la sanzione dell'inutilizzabilità processuale appare ben poca cosa, come rimedio all'invasione della *privacy*, una volta che si sia avuto accesso a documenti di natura strettamente personale. In argomento, volendo si veda già F. IOVENE, *Perquisizione e sequestro di* computer*: un'analisi comparatistica*, in *Riv. dir. proc.*, 2012, p. 1607 ss.

[289] Tale regola, nota come *Tamura Rule*, è stata elabora in *United States v. Tamura, 694 F. 2d 591 (9th Circuit 1982)*, e successivamente seguita da *United States v. Shilling, 826 F. 2d 1365 (4th Circuit)*.

metodi di selezione del materiale e di individuare i *files* irrilevanti per le indagini[290]. Altra parte della dottrina, prendendo atto dell'impreparazione tecnica dei giudici rispetto all'individuazione delle tecniche di *computer forensics* da utilizzare, e della circostanza che i precedenti della Corte Suprema negano che il mandato debba indicare i metodi di ricerca da utilizzare[291], auspica che la perquisizione dell'*hard disk* venga fatta da personale specializzato e indipendente[292].

Questi suggerimenti sono stati raccolti da una recente sentenza della *Ninth Circuit Court of Appeal*[293], la quale ha stabilito che l'operazione di selezione dei *files* rilevanti per le indagini debba essere eseguita da personale specializzato o da soggetti indipendenti, e che nel caso in cui tale attività sia svolta da tecnici del pubblico ministero, essi saranno autorizzati a rivelare a quest'ultimo le sole informazioni desumibili dal contenuto del mandato. Inoltre, si è stabilito che gli inquirenti debbano distruggere ovvero, trattandosi di cose che il proprietario può detenere legalmente, restituire i dati non rilevanti, e informare di ciò il magistrato. Tuttavia, poiché tali indicazioni operative non erano necessarie ai fini della decisione, e quindi violavano il Terzo Articolo della Costituzione[294], tale sentenza è stata successivamente riformata, con la conseguenza che essa non costituisce un precedente vincolante, nemmeno all'interno del *Ninth Circuit*[295].

---

[290] Cfr. R. WINICK, *Searches and Seizures of Computers and Computer Data,* 8 *Harv. J. L. & Tec.* 75 (1994), 108.

[291] *Dalia v. United States,* cit.

[292] Così, O. S. KERR, *Searches and Seizures,* cit., 572. Questo è anche l'orientamento del *Department of Justice*. Un'impostazione simile si ritrova anche nella dottrina tedesca che si è occupata delle c.d. *Online Durchsuchungen*, (su cui *infra*, capitolo III, par. 3 ss.). Poiché la tecnica non permette di programmare un accesso selettivo al sistema informatico, è stato proposto di individuare un'Autorità Garante, indipendente e terza rispetto al processo, che esamini i dati appresi attraverso la perquisizione prima che questi vengano visionati dagli inquirenti, selezionando, e conseguentemente eliminando, quelli tra essi estremamente personali, e irrilevanti per le indagini. Il compito di tale Autorità sarebbe, per l'appunto, quello di garantire, dapprima la non apprensione (nel senso di non conoscenza da parte dell'autorità procedente) dei dati, e successivamente il rispetto degli obblighi di non utilizzo e immediata cancellazione. Cfr. P. SCHANTZ, *Verfassungsrechtliche Probleme von "Online-Durchsuchungen"*, in *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft*, 2007, p. 324 ss.

[293] *United States v. Comprehensive Drug Testing Inc.*, cit.

[294] Il Terzo Articolo della Costituzione americana, infatti, nell'investire le *lower courts* del potere giudiziario, ne definisce i confini, stabilendo che esse possono esercitarlo solo al fine di risolvere i casi e le controversie sottoposte alla loro attenzione.

[295] Tali prescrizioni, che andavano oltre la soluzione del caso concreto, sono comunque ribadite nella *concurring opinion* del Giudice Kozinski, estensore della prima sentenza, e costituiscono delle linee guida per gli inquirenti. Cfr. *United States v. Comprehensive Drug Testing Inc., 621 F. 3d 1162 (9th Circuit 2010)*.

5. Perquisizione e sequestro di materiale informatico: una proposta

Quando oggetto di indagine sono dati informatici, è difficile distinguere nettamente tra le diverse attività investigative che su di essi vengono intraprese. Di qui le summenzionate difficoltà nel qualificare le operazioni di clonazione dell'*hard disk* e in generale dei supporti di memoria digitali. Perquisire un sistema informatico o telematico adottando «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione», come prescritto dal legislatore, significa effettuare una previa *bit stream image* di quel sistema, ciò che equivale a sequestrare i dati ivi contenuti[296]. Da questa *copia originale* verranno poi estratte ulteriori copie, su cui accusa e difesa possono compiere – ripetutamente e autonomamente? - gli accertamenti che ritengono necessari. Ciò non solo non risolve, ma accentua i problemi legati alla tutela dei dati personali salvati sul *computer* e al rischio che la perquisizione muova alla ricerca della *notitia criminis*.

Il dibattito sviluppatosi in seno alla giurisprudenza e alla dottrina nordamericana costituisce un utile spunto per una possibile soluzione da adottare nel nostro ordinamento.

Per garantire quanto più possibile la riservatezza dei dati personali, preso atto dell'inesistenza di strumenti che permettano un accesso selettivo alla memoria del *computer*, sarebbe innanzitutto opportuno garantire la partecipazione dell'interessato, eventualmente tramite persona di fiducia, alla clonazione dell'*hard disk*, momento centrale dell'intera indagine, nonché al momento in cui si procede alla selezione del materiale rilevante per le indagini.

Si tratta evidentemente di atti a sorpresa, per cui non è previsto il preavviso al difensore. L'ideale quindi sarebbe asportare il supporto fisico, in modo da sottrarlo alla disponibilità dell'interessato, e successivamente instaurare il contraddittorio tecnico. Tuttavia, non sempre è possibile o opportuno asportare fisicamente il

[296] Come si è già evidenziato, l'art. 254 *bis* c.p.p. in materia di sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni prevede che tale sequestro avvenga mediante «copia di essi su adeguato supporto mediante una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità», espressamente qualificando l'attività di copia come sequestro. Non si vede, quindi, perché ciò non dovrebbe valere nel caso di acquisizione di copia di dati da sistemi informatici e telematici.

computer o altro dispositivo di memoria[297]. In particolare, occorre distinguere l'ipotesi in cui il *computer* sia spento, da quella in cui sia acceso. Mentre nel primo caso la rimozione del *computer* sarà senz'altro possibile, la seconda ipotesi è problematica poiché un *computer* acceso è in continuo aggiornamento. Gli esperti di *computer forensics* suggeriscono di spegnere il *computer* staccando la spina, ossia privando il sistema di alimentazione elettrica; l'ordinaria procedura di chiusura del sistema operativo, infatti può apportare delle modifiche (si pensi ai procedimenti di sincronizzazione dei dati o all'eventuale installazione di aggiornamenti)[298]. Tuttavia, potrebbe essere necessario compiere delle operazioni urgenti per preservare la genuinità e la non alterazione dei dati da sottoporre a successiva analisi, come ad esempio acquisire il contenuto della memoria volatile (*RAM*), o verificare la sussistenza di eventuali connessioni attive[299]. Si tratta di attività urgenti e irripetibili che di fatto verranno svolte unilateralmente dalla polizia giudiziaria ai sensi dell'art. 354 c.p.p.

Ci sono poi situazioni nelle quali spegnere il *computer* non è proprio possibile, e occorrerà necessariamente procedere alle operazioni di *Live Forensics Analysis in loco*. Il riferimento è a sistemi informatici da cui dipendono infrastrutture critiche, il cui spegnimento comporterebbe anche ingenti danni economici. Il problema aggiuntivo in questo caso è che non si potrà procedere ad effettuare la copia clone perché ciò è possibile solo se il sistema è spento[300].

---

[297] Il manuale *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* del *Department of Justice* americano, cit., individua alcuni criteri guida in base ai quali stabilire se sia opportuno rimuovere il *computer* o no.

[298] Cfr., A. GHIRARDINI, G. FACCIOLI, *Computer forensics*, Milano, 2010, p.65 ss.; G. ZICCARDI, *Manuale breve*, cit. p. 205 ss.; G. NICOSIA, D. E. CACCAVELLA, *Indagini della difesa e alibi informatico: utilizzo di nuove metodiche investigative, problemi applicativi ed introduzione nel giudizio*, in *Dir. Internet*, 2007, p. 525 ss.

[299] Si tratta della c.d. *Live Forensics Analysis*, che comprende le attività di analisi e cristallizzazione della prova su dispositivi accesi o in *stand-by*.

[300] L'*International Information Systems Forensics Association* ha condotto un sondaggio, che si è svolto nel periodo novembre/dicembre 2011, sull'impatto della legge 48/2008 sulle procure distrettuali; hanno risposto al questionario nel suo complesso in tutto 22 procure distrettuali. Per quanto riguarda la natura ripetibile o irripetibile dell'attività di analisi di un *computer*, 9 delle 20 procure distrettuali che hanno risposto la ritengono ripetibile se deve essere esperita su un *computer* portatile spento al fine di estrapolare i dati ivi contenuti, anche se cancellati, 11 la ritengono irripetibile. Le proporzioni cambiano quando oggetto d'analisi è un *computer* aziendale che non può essere spento: in questo caso 14 su 21 procure che hanno risposto ritengono l'attività irripetibile, 7 la ritengono ripetibile. Per quanto riguarda le scelta se sequestrare l'*hard disk* o effettuare *in loco* la copia clone, 15 delle 22 procure che hanno risposto optano per il sequestro dell'*hard disk* originale, le restanti 7 per la creazione della *bit stream image* senza necessità di asportare il *computer*. Queste le ragioni che spingono al sequestro: evitare riserve e contestazioni in merito alla possibile alterazione

Eccezion fatta per le operazioni urgenti, il contraddittorio con tecnici nominati dalla difesa e dal destinatario del provvedimento di sequestro, che può essere persona diversa dall'indagato[301], va sempre instaurato sia per l'effettuazione della copia clone, che per la successiva estrazione di copie su cui verranno concretamente svolte le indagini[302]. Ciò è necessario per garantire il rispetto delle *best practices* e la verificabilità *ex post* della catena di custodia.

Va quindi certamente censurato quell'orientamento giurisprudenziale in forza del 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[303]. Come giustamente osservato, tale impostazione va respinta perché contrasta con la scelta del legislatore del 2008 di includere le investigazioni informatiche nei contenitori normativi delle ispezioni, perquisizioni e sequestri, ossia mezzi di ricerca della prova rispetto ai quali il difensore, pur non avendo diritto ad essere preavvisato, ha in ogni caso diritto di assistere, stabilito a pena di nullità intermedia[304].

Scopo principale di tale fase preliminare sarebbe di eliminare dal materiale probatorio i dati personali, irrilevanti per le indagini: una volta individuati, tali *files* andrebbero, infatti, distrutti, ai sensi dell'art. 7, comma 3, lett. b), codice *privacy*[305].

---

dei dati, assicurare più garanzie in relazione alle possibili eccezioni difensive, esigenze pratiche o temporali, maggior facilità di esecuzione, mancanza di personale specializzato in grado di effettuare la copia-clone, possibilità di effettuare ulteriori accertamenti. La copia-clone viene invece eseguita per evitare di conservare "reperti inutili" e perché consente accertamenti più rapidi. I risultati sono pubblicati nel volume a cura di G. COSTABILE e A. ATTANASIO, *IISFA Membergroup 2012*. Digital Forensics*. Condivisione della conoscenza tra i membri dell'*IISFA ITALIAN CHAPTER, *Experta Edizioni*, 2012.

[301] La situazione è ancora più delicata, nel caso, frequentemente verificatosi nella prassi, di sequestro di *computer* di un giornalista. Qui, oltre alle preoccupazioni generali riguardanti la *privacy* e la tutela dei dati personali, si pongono più specifiche questioni attinenti alla tutela del segreto professionale. Ciò fa sì, non solo che il decreto di sequestro debba essere quanto più dettagliato possibile in merito all'individuazione dell'oggetto dell'*adprehensio*, ma anche che si debba seguire la specifica procedura dettata dall'art. 256, commi 1 e 2 c.p.p., che prevede che l'apposizione del vincolo sul bene sia preceduta dall'emissione di un decreto di esibizione. Così, Cass., sez. I, 16 febbraio 2007, n. 25755, Pomarici, cit.; v. anche Cass., sez III, 31 maggio 2007, Sarzanini, cit.

[302] Il fatto che, una volta ottenuta la copia clone, le successive attività di indagine possano essere fatte più volte non significa che esse necessariamente vadano fatte ripetutamente. Vi sono, anzi, buone ragioni per ritenere che sia comunque opportuno renderle attività irripetibili.

[303] Cass., sez. I., 25 febbraio 2009, n. 11503, cit.; Cass., sez. III, 2 luglio 2009, n. 38087, cit.; Cass., sez. I, 30 aprile 2009, n. 23035, cit.; Cass., sez. I, 1 aprile 2009, n. 16942, cit.

[304] In questi termini, M. DANIELE, *Caratteristiche*, cit., p. 214.

[305] Tali *files* vanno eliminati sia dalla copia-clone "originale", sia da tutte le ulteriori copie estratte.

La copia del disco rigido, così depurata, andrebbe depositata presso la segreteria del pubblico ministero, con facoltà per la difesa di prenderne visione ed estrarne copia. Questo al fine di tutelare la *privacy*, un fascio di diritti dei quali non è più possibile disconoscere il rango costituzionale (art. 2 Cost. e artt. 117 Cost. e 8 CEDU) e che, pertanto, al pari dei tradizionali diritti fondamentali (libertà personale, libertà domiciliare, libertà e segretezza delle comunicazioni), merita di essere tutelata con riserva di legge, riserva di giurisdizione, alla luce del principio di proporzionalità[306].

Per evitare, invece, che il pubblico ministero muova alla ricerca della *notitia criminis*, sarebbe auspicabile innanzitutto prevedere che la "copia-clone" venga fin dall'inizio depositata presso la cancelleria del giudice per le indagini preliminari, inoltre che l'ulteriore attività di individuazione del materiale rilevante per le indagini venga fatta nel corso di un'udienza-stralcio (sul tipo di quella prevista per le intercettazioni di comunicazioni)[307], convocata dal GIP nelle forme dell'incidente probatorio[308] e infine, introdurre un'ipotesi di inutilizzabilità, a qualsiasi scopo e fino a che non si sarà svolto l'incidente probatorio, di quanto rinvenuto sull'*hard disk*. Se durante l'incidente probatorio si dovessero rinvenire prove o il corpo di un reato diverso, il pubblico ministero dovrebbe procedere all'iscrizione della relativa notizia di reato. Una volta terminato l'incidente probatorio, il materiale selezionato confluirebbe naturalmente nel fascicolo per il dibattimento mentre i *files* irrilevanti, in tutte le copie che se ne posseggono, andrebbero distrutti o restituiti al proprietario.

---

[306] *Supra*, capitolo I, par. 2 ss.

[307] In tal senso anche F. RUGGIERI, *Profili processuali nelle investigazioni informatiche*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica*, Cedam, Padova, 2004, p. 157; S. CARNEVALE, *Copia*, cit., p. 481; S. VENTURINI, *Sequestro probatorio*, cit., p. 119.

[308] A tal proposito si segnala un'interessante sentenza della Cassazione in cui è stato ritenuto legittimo il sequestro di un *server* informatico (completamente sigillato) presso lo studio di un avvocato, indagato, in quanto «*funzionale alla* [successiva] *selezione dei dati informatici pertinenti attraverso l'incombente processuale della perizia da espletarsi con incidente probatorio*». Il Tribunale aveva annullato il sequestro autorizzato dal GIP in quanto esso, avendo ad oggetto l'intero *server* informatico, era privo del requisito pertinenziale richiesto dall'art. 253 c.p.p. Più correttamente il pubblico ministero avrebbe dovuto procedere a perquisizione avvalendosi dell'apporto di un consulente tecnico da lui nominato *ex* art. 359 c.p.p. al fine di selezionare il materiale pertinente e quindi sequestrabile. La Suprema Corte ritiene al contrario legittima la procedura seguita dal pubblico ministero proprio in quanto essa permetteva di selezionare il materiale sequestrato con le garanzie del contraddittorio anticipato, evitando indebite conseguenze sulle garanzie del difensore in violazione dell'art. 103 c.p.p. Cass., sez. V, 19 marzo 2002, n. 2816, in *Cass. pen.*, 2004, p. 1339 ss.

Ciò permetterebbe altresì di risolvere la questione della mancanza dell'interesse ad impugnare il provvedimento di sequestro nel caso in cui il bene sia stato restituito[309].

Si tratta nell'insieme di una procedura complessa, ma necessaria per tutelare la *privacy* dell'interessato. Inoltre, non sembra che i tempi processuali subiscano un eccessivo allungamento; infatti, secondo la prassi giurisprudenziale attuale si eseguono prima accertamenti tecnici o rilievi ripetibili e poi viene disposta una perizia in dibattimento, deputata a verificare che le operazioni siano state effettuate correttamente. In tale sede, quindi a molti mesi di distanza, si potrebbe appurare ad esempio che le tecniche usate non sono quelle corrette e che quindi la *chain of custody* non è verificabile in ogni suo anello. Inoltre, i supporti su cui sono conservati i dati, anche la copia clone, sono soggetti a deterioramento se non correttamente conservati. La precostituzione della prova digitale non nuoce alla difesa[310], la quale nutre un interesse analogo a quello del pubblico ministero a che la prova digitale sia utilizzabile e valutabile dal giudice[311].

6. Captazione in tempo reale di dati digitali

6.1 Intercettazione di comunicazioni informatiche o telematiche

Dell'intercettazione di comunicazioni informatiche e telematiche si occupa l'art. 266 *bis* c.p.p., norma facente parte del pacchetto di misure introdotte dalla legge n. 547 del 1993 per contrastare la criminalità informatica e volta a consentire «nei procedimenti relativi ai reati indicati nell'art. 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche» la captazione «del

[309] Vedi *supra*, par. 4.3 ss.

[310] In senso contrario, F. M. MOLINARI, *Attività investigative*, cit., la quale individua una *chance* difensiva importantissima nel poter «richiedere la ripetizione in udienza della perquisizione informatica (o di sue parti) sia al fine di verificare la correttezza delle operazioni di ricerca eseguite, eventualmente sollecitando una perizia (*analysis*); sia al fine di fare emergere nuovi elementi rimasti in ombra nel corso delle attività compiute dagli inquirenti in sede d'indagini».

[311] Un sistema informatico potrebbe contenere una prova d'alibi, e il fatto che le indagini si siano svolte senza seguire i protocolli di *computer forensics* potrebbe vanificarla. Emblematico a tal proposito è il caso Garlasco: in un primo momento a causa degli errori fatti nell'esaminare il *computer* di Alberto Stasi, il Giudice non aveva potuto ritenere confermato l'alibi da questi fornito. A tal fine è stata quindi disposta perizia dibattimentale, attraverso la quale è stato possibile dimostrare la fondatezza dell'alibi, esaminando i metadati presenti nel *computer* e che non erano stati inficiati dalle indagini effettuate. In merito, si rinvia E. COLOMBO, *La sentenza del caso di Garlasco e la* computer forensics, in *Cyberspazio e diritto*, 2010, p. 454 ss.

flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi».

Sulla scorta della nozione di intercettazione elaborata dalla giurisprudenza con riferimento all'art. 266 c.p.p.[312], si può definire l'intercettazione telematica come l'«apprensione in tempo reale, attuata mediante l'ausilio di strumenti tecnici, di una trasmissione di dati segreta e riservata»[313].

Per quanto riguarda la definizione di sistema informatico o telematico, tradizionalmente si afferma che la differenza tra i due risiede nel metodo utilizzato per la trasmissione dei dati a distanza. Nell'ambito di un sistema informatico i dati sono trasmessi tramite un cavo, nel sistema telematico si sfruttano invece onde guidate, cavi telefonici, ponti radio o altri canali di comunicazione[314]. Tale distinzione ha oggi perso attualità poiché, come già accennato, la Convenzione di Budapest non distingue tra sistema informatico e sistema telematico, fornendo una definizione unitaria che ricomprende genericamente qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnessi o collegati, che eseguono l'elaborazione automatica di dati, in base ad un programma[315].

Poiché l'art. 266 *bis* c.p.p. è innestato nell'ambito delle intercettazioni di comunicazioni, valgono i principi (art. 15 Cost., art. 8 CEDU) e i presupposti dettati per questo mezzo di ricerca della prova quanto a competenza e presupposti applicativi (richiesta del pubblico ministero al giudice, a cui è riservato il potere di autorizzazione; possibilità per il pubblico ministero di disporre le intercettazioni in caso di urgenza, salvo poi ottenere, pena l'inutilizzabilità delle comunicazioni nel frattempo intercettate, l'autorizzazione del giudice; necessità di gravi indizi di reato; assoluta indispensabilità delle intercettazioni per la prosecuzione delle indagini;

---

[312] Cfr. Cass., sez. un., 24 settembre 2003, n. 36747, Torcasio, in *Cass. pen.*, 2004, p. 21: «*Le intercettazioni regolate dagli artt. 266 e seguenti c.p.p. consistono nella 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, attuata da soggetto estraneo alla stessa mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del suo carattere riservato*».

[313] Tale definizione si deve a L. LUPARIA, *La disciplina processuale*, cit. p. 162.

[314] Cfr. G. BUONOMO, *Metodologia e disciplina delle indagini informatiche*, in R. BORRUSO, R. BUONOMO, G. CORASANTI, G. D'AIETTI, *Profili penali dell'informatica*, Milano, 1994, p. 148. L'Autore precisa che il riferimento al "flusso di comunicazioni intercorrenti tra più sistemi" è utile per indicare quelle forme di collegamento tra più elaboratori che, essendo del tutto occasionali non costituiscono nel complesso un "sistema telematico"; infatti tale concetto postula un collegamento di carattere permanente tra i vari sistemi informatici.

[315] Art. 1 Convenzione di Budapest. Cfr. *supra*, par. 2.1.

limiti di durata delle operazioni) e modalità di esecuzione (registrazione su supporti, redazione del verbale, avviso di deposito, udienza stralcio, *etc.*).

La portata innovativa di tale disposizione normativa è controversa in dottrina. Mentre secondo taluno essa era necessaria perché le intercettazioni telematiche non erano previste dalla previgente normativa[316], per altri si tratterebbe di «una norma in parte vuota» perché l'espressione "altre forme di telecomunicazione" di cui all'art. 266 c.p.p. si prestava a ricomprendere «qualunque sistema per la trasmissione a distanza di informazioni di diversa natura»[317]. Pertanto, l'unica novità sarebbe consistita nell'ampliare il novero dei reati per cui è possibile disporre simile misura, comprendendovi anche quelli commessi mediante l'impiego di tecnologie informatiche. In posizione intermedia si pongono coloro che affermano che un'interpretazione estensiva dell'art. 266 c.p.p. avrebbe consentito di comprendere nelle "altre forme di telecomunicazione" le intercettazioni telematiche, ma non quelle informatiche, aventi per oggetto più *computers* in grado di interagire tra loro senza avvalersi dello strumento telefonico[318].

In merito all'individuazione dei «reati commessi mediante l'impiego di tecnologie informatiche o telematiche» si registrano orientamenti diversi. A fronte di chi sostiene che tale locuzione faccia riferimento solo ai *computer crimes* in senso stretto[319], ossia quelli in cui lo strumento informatico è elemento costitutivo della fattispecie, vi è chi ritiene la locuzione comprensiva anche dei reati comuni commessi con il mezzo informatico[320]. Ad ogni modo, il catalogo dei reati per cui si può disporre un'intercettazione telematica è più ampio di quello che costituisce il

[316] C. SARZANA DI S. IPPOLITO, *Informatica e diritto penale*, Milano, 1994, p. 266 ss.
[317] Le citazioni sono di A. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, p. 12, il quale ritiene che l'art. 266 *bis* c.p.p. sia una norma inutile e dannosa, perché potrebbe indurre a ritenere che la generica possibilità di intercettare "altre forme di telecomunicazione" di cui all'art. 266 c.p.p. necessiti di una concretizzazione esplicita.
[318] Cfr. F. TESTA, Cybercrime*, intercettazioni telematiche e cooperazione giudiziaria in materia di attacchi ai sistemi informatici*, 2005, p. 22, reperibile su sito *Persona e danno*, diretto da P. CENDON, *http://www.personaedanno.it/;* C. PARODI, *Le intercettazioni: profili operativi e giurisprudenziali*, Torino, 2002, p. 290. Secondo tale interpretazione, nel caso in cui i *computer* siano connessi tramite *modem* si potrebbe applicare l'art. 266 c.p.p. perché la comunicazione avviene tramite il sistema telefonico, mentre se gli elaboratori fanno parte di una rete locale (*LAN*, *Located Area Network*), come tipicamente accade all'interno di uffici o pubbliche amministrazioni, l'art. 266 *bis* c.p.p. conserva una sua utilità.
[319] L. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, p. 82. Secondo tale interpretazione la lettura restrittiva del catalogo dei reati presupposto deriverebbe dalla necessità di rispettare l'art. 15 Cost.
[320] A. CAMON, *Le intercettazioni*, cit., p. 67; L. LUPARIA, *La disciplina processuale*, cit., p. 163; C. PARODI, *Le intercettazioni*, cit., p. 889.

presupposto di un'intercettazione *ex* art. 266 c.p.p. Ne deriva che, mentre nel caso in cui sussistono i presupposti per disporre un'intercettazione telefonica, si potrà anche procedere ad intercettazione telematica, non è vero il contrario. Si tratta di un aspetto che non va sottovalutato, infatti gli strumenti utilizzati per la captazione di flussi informatici possono al tempo stesso intercettare il traffico telefonico, il che fa sorgere delicate questioni di utilizzabilità probatoria dei risultati acquisiti per violazione dell'art. 15 Cost.[321].

Per quanto riguarda invece l'oggetto dell'intercettazione *ex* art. 266 bis c.p.p., la collocazione sistematica, la genesi storica e la gamma dei reati presupposto, inducono a ritenere che tale istituto non sia preposto alla captazione di qualsiasi comunicazione intercorrente tra sistemi informatici, ma solo a captare lo scambio di dati digitali determinato da un'attività umana, ossia un'attività di comunicazione o di altro genere riconducibile ad una persona[322]. Ne deriva che lo strumento in esame può essere utilizzato per l'apprensione di messaggi scritti come le *e-mail*, di conversazioni via *chat*, ovvero per la captazione di collegamenti con siti *web*[323].

L'art. 266 *bis* c.p.p. non dovrebbe, al contrario, applicarsi ad attività, come il pedinamento satellitare, che sfruttano il sistema *GPS*, il quale invia dati in maniera

[321] Per questi rilievi si veda L. LUPARIA, *La disciplina processuale*, cit., p. 163 il quale porta l'esempio del *telemonitor*, un «apparecchio che, per le sue caratteristiche tecniche e per il fatto di essere posizionato direttamente "alla fonte" e non presso il *service provider* (come accade invece per le unità *sniffer*), traccia in tempo reale dati voce, *fax* e *Internet*, anche quando l'autorizzazione giudiziale sia circoscritta ai soli flussi telematici». Si tratta peraltro di uno strumento simile a quello che in Germania viene denominato "*Quellen-Telekommunikationsüberwachung*" e che rappresenta una particolare forma di intromissione nel *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. Secondo la Corte costituzionale tedesca tale misura va considerata un'intromissione nel *Computer Grundrecht* quando, in collegamento con l'intromissione nel sistema, si può giungere ad acquisire dati rilevanti per la personalità senza riferimento alla comunicazione in corso. In questo caso, infatti, l'art. 10, comma 1 *GG* non fornisce sufficiente tutela per gli specifici pericoli per la personalità. Cfr. L. DRALLÉ, *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, *Lorenz-von-Stein-Institut*, 2010, p. 94 ss. Il rapporto tra il nuovo diritto fondamentale e l'art. 10 *GG* è esaminato *supra*, capitolo I, par. 5.1.

[322] In questi termini, G. DI PAOLO, (voce) *Prova informatica (diritto processuale penale)*, in *Enc. dir.,* Annali VI*,* Milano, 2013, p. 744.

[323] Cfr. N. GALANTINI, sub *art. 12, Le intercettazioni*, in A. CADOPPI (a cura di), *Commentario delle norme contro la violenza sessuale e della legge contro la pedofilia*, Padova, 2002, p. 774, la quale nega che costituisca intercettazione la semplice scoperta di un sito *web*, in cui qualsiasi utente della rete può accedere, anche occasionalmente, mediante *password*; G. DI PAOLO, (voce) *Prova informatica*, cit., p. 745, la quale sostiene che la disciplina delle intercettazioni *ex* art. 266 *bis* c.p.p. dovrebbe applicarsi anche qualora si voglia effettuare «la captazione di collegamenti *in fieri* al sito di interesse per risalire, attraverso l'indirizzo *IP*, all'identità degli utenti che vi accedono e caricano/scaricano *files* di contenuto illecito». La questione dell'apprensione delle *e-mail* verrà approfondita *infra*, par. 6.2.

del tutto automatica, senza che sia necessario un *input* umano[324]. Né rientrano nell'ambito di applicazione di tale norma le attività di accertamento della polizia giudiziaria che accede, mediante strumento informatico, alle comunicazioni aperte a tutti i navigatori della rete, venendo a mancare in questo caso il carattere di segretezza della comunicazione.

6.1.2 Intercettazione di comunicazioni VoIP

Particolare attenzione merita il tema dell'intercettazione di comunicazioni *VoIP* (*Voice over Internet Protocol*). Si tratta di una tecnologia che rende possibile effettuare conversazioni telefoniche sfruttando una connessione *Internet* o un'altra rete dedicata che utilizza il protocollo *IP*, anziché passare attraverso la rete telefonica tradizionale[325]. In concreto il sistema *VoIP* provvede ad instradare sulla rete pacchetti di dati contenti le informazioni vocali, codificati in forma digitale, solo nel momento in cui è necessario, cioè quando uno degli utenti collegati sta parlando. La disponibilità di connessioni *web* a banda larga e la particolare semplicità di utilizzo del più noto e diffuso modello di fruizione della telefonia via *Internet – Skype –* hanno decretato la diffusione capillare e l'utilizzo quotidiano di tale sistema di comunicazione, ciò che impone di considerarlo quale possibile oggetto di indagini penali[326].

---

[324] Così, G. DI PAOLO, (voce) *Prova informatica*, cit., p. 744, la quale esclude inoltre che costituisca intercettazione di telecomunicazione l'attività della polizia giudiziaria consistente nell'accesso a *files* condivisi in rete, mediante un programma di *file sharing*, liberamente e gratuitamente reperibile in *Internet*, senza che tale accesso sia accompagnato da modalità tipiche di contrasto quali l'acquisto simulato e l'intermediazione dei prodotti esistenti né cartelle condivise. In giurisprudenza si veda Cass., sez. III, 5 febbraio 2009, Luzi, in *C.E.D. Cass.*, n. 243389; Cass., sez. III, 20 ottobre 2010, R., in *C.E.D. Cass.*, n. 245262; Cass., sez. V, 7 maggio 2004, Lagazzo, in *C.E.D. Cass.*, n. 228089. Il pedinamento satellitare verrà esaminato *infra*, capitolo III, par. 2 ss.

[325] Le conversazioni *VoIP*, infatti, non devono necessariamente viaggiare su *Internet*, ma possono anche usare come mezzo trasmissivo una qualsiasi rete privata basata sul protocollo *IP*, per esempio una *LAN* all'interno di un edificio. Non è inoltre necessario che entrambi gli utenti siano connessi a *Internet*, infatti, i sistemi *VoIP* permettono di effettuare chiamate anche su reti fisse o cellulari. In questo caso la comunicazione corre via *Internet* fino alla nazione del destinatario, dove viene poi instradata sulla normale rete telefonica del Paese. Cfr. C. PARODI, VoIP, Skype *e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?*, in *Dir. pen. proc.*, 2008, p. 1309 ss.

[326] La progressiva diffusione di tale sistema dipende anche dai limitati "mezzi" dei quali l'utente deve disporre per procedere all'utilizzo: un sistema operativo (quale *Macintosh* o *Windows*), un collegamento *Internet*, una scheda audio e un microfono.

La prima difficoltà che si incontra riguarda l'individuazione della normativa di riferimento. Secondo un primo orientamento, il semplice dato tecnologico, costituito dal transito della comunicazione in forma digitalizzata attraverso *computers* tra loro collegati, o in rete o via *modem* o con qualsiasi altra forma, deporrebbe a favore dell'applicazione dell'art. 266 *bis* c.p.p.[327]. A sostegno di questa lettura potrebbero deporre due peculiarità delle chiamate *VoIP*, che le differenzierebbero dalle telefonate tradizionali: la circostanza che l'utente scelga consapevolmente un *computer* come mezzo di comunicazione e il fatto che nelle comunicazioni *VoIP* gli utenti siano identificati, non da un numero di telefono, ma tramite un *account* e un *IP*[328].

Secondo una diversa interpretazione, l'evoluzione tecnologica non può tradursi in un allentamento dell'apparato di garanzie che l'art. 266 c.p.p., in ossequio all'art. 15 Cost., prevede per l'apprensione occulta del contenuto di una comunicazione[329]. Ragione per cui «ogni comunicazione vocale, anche se trasmessa via *Internet*, rientra sotto l'ombrello della più rigida disciplina di cui all'art. 266 c.p.p.»[330].

Si ritiene di aderire a questo secondo orientamento. Infatti, si assiste oggi ad un fenomeno di digitalizzazione dei servizi di telefonia e di convergenza tecnologica,

---

[327] Così F. TESTA, Cybercrime, cit., p. 22; in tal senso anche G. VACIAGO, Digital evidence, cit., p. 70, il quale fa rientrare nell'oggetto delle intercettazioni telematiche «l'intero flusso di dati (*e-mail* inviate e ricevute, siti *web* visitati, comunicazioni *VoIP* non criptate, d*ownload* e *upload* di *files*, conversazioni in *chat room*) del sistema informatico d'interesse».

[328] Per tali affermazioni si veda G. DI PAOLO, (voce) *Prova informatica*, cit., p. 745, la quale però esprime perplessità sul fatto che tali circostanze abbiano valore dirimente, soprattutto perché sempre più spesso i sistemi *VoIP* vengono impiegati per effettuare chiamate verso telefoni cellulari o utenze fisse (è il caso ad esempio del servizio a pagamento *SkypeOut*). Secondo l'Autrice, proprio l'intreccio tra due diversi metodi di comunicazione rende urgente una equiparazione tra le intercettazioni *ex* art. 266 c.p.p. e le intercettazioni telematiche *ex* art. 266 *bis* c.p.p. In termini analoghi, già L. LUPARIA, *Le investigazioni informatiche*, cit., p. 165, secondo il quale non è ragionevole che la stessa identica telefonata venga assoggettata a regimi differenziati in punto di reati presupposti e impianti utilizzabili, a seconda del *target* dell'attività di intercettazione o del punto in cui venga installato il dispositivo.

[329] Ciò è coerente con la scelta del legislatore del 1988 che, a differenza del codice Rocco, ha volutamente adottato una formula ampia e aperta per definire l'oggetto dell'intercettazione. Cfr., A. CAMON, *Le intercettazioni*, cit., p. 11, secondo cui «da tale formula il concetto normativo di intercettazione riceve una notevole forza espansiva, capace di ricomprendere a priori nel dettato codicistico le eventuali acquisizioni della scienza elettronica».

[330] Così, L. LUPARIA, *Le investigazioni informatiche*, cit., p. 166, il quale peraltro segnala che il disegno di legge in materia di intercettazioni telefoniche ed ambientali, approvato alla Camera il 17 aprile 2007 prevedeva di aggiungere all'art. 266 *bis* c.p.p. un comma in cui esplicitare che «alle intercettazioni di cui al comma 1 si applicano le disposizioni di conversazioni o comunicazioni telefoniche». Aderisce a tale impostazione L. MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4509 ss.

tale per cui anche la normale telefonata è trasmessa attraverso la piattaforma elettronica[331]. Se ne potrebbe quindi dedurre che anch'essa sia un flusso informatico, intercettabile ai sensi dell'art. 266 *bis* c.p.p. Non si dubita tuttavia dell'applicabilità dell'art. 266 c.p.p., posto che si tratta di conversazione che nasce come vocale[332]. Ciò significa, seguendo un ragionamento *a contrariis*, che il semplice dato tecnologico non può essere il discrimine tra art. 266 e art. 266 *bis* c.p.p. L'intercettazione di una comunicazione vocale deve avvenire agli stessi presupposti e secondo la stessa disciplina, a prescindere dal mezzo scelto dagli interlocutori.

Conferma di ciò si trae dall'esperienza comparata. Come si è visto nella prima parte del presente lavoro, il *Bundesverfassungsgericht*, ha creato un nuovo diritto fondamentale, il *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, per tutelare i singoli di fronte alle nuove forme di intromissione rese possibili dall'evoluzione tecnologica. In particolare, la Corte si è trovata a vagliare la legittimità costituzionale di forme di intromissione segreta in un sistema informatico e nel fare ciò ha precisato che qualora tale intromissione permetta di captare il contenuto di una comunicazione che avvenga attraverso il sistema informatico stesso, troverà applicazione l'art. 10 *GG* che tutela la segretezza delle telecomunicazioni, e non il neo coniato diritto fondamentale alla tutela della garanzia della riservatezza e integrità del sistema informatico[333]. Ne deriva che la legittimità di tale captazione dipenderà dal rispetto dei rigidi presupposti dettati dai §§ 100a ss. *StPO* per l'intercettazione di comunicazioni. Anche per la Corte tedesca, quindi, la disciplina delle intercettazioni si applica a qualunque comunicazione vocale, a prescindere dal mezzo usato.

[331] L. LUPARIA, Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, diretto da G. SPANGHER, Vol. VII, *Modelli differenziati di accertamento*, Tomo I, a cura di G. GARUTI, Torino, 2011, p. 378, nota 51.
[332] F. TESTA, Cybercrime, cit., p. 22 ritiene, al contrario, che nulla impedisca di applicare alle intercettazioni telefoniche la più ampia formula dell'art. 266 *bis* c.p.p. Tale affermazione trae sostegno da una pronuncia della Cassazione – sez. VI, 4 ottobre 1999, n. 3067, in *Cass. pen.*, 2000, p. 2990 ss. – in cui si è riconosciuta la natura di sistema informatico alla rete telefonica fissa proprio in considerazione delle modalità di trasmissione dei flussi di conversazioni. In tal senso anche C. PARODI, VoIP, Skype, cit., p. 1309 ss.
[333] *Supra*, cap. I, par. 5.1.

Risolta la questione del regime normativo di riferimento, ancora non si è detto nulla circa l'effettiva possibilità di intercettare tali comunicazioni; infatti una cosa è la normativa astrattamente applicabile, altra la sua operatività in concreto[334].

Il tema della intercettabilità delle comunicazioni *VoIP* va affrontato sulla base della fondamentale distinzione tra sistemi *VoIP* che sfruttano protocolli *standard* tipo *SIP* o *H.323*, e quelli che, al contrario, si basano su protocolli proprietari, cioè non formalizzati in alcuno *standard* internazionale, come *Skype*[335].

I sistemi del primo tipo sono facilmente intercettabili dal momento che, normalmente, per garantire migliori prestazioni, non usano protezioni crittografiche. In ogni caso, anche se le usassero, si tratterebbe di codici *standard*, quindi, facilmente decrittabili.

Diversa la situazione di *Skype*, il sistema di comunicazione *VoIP* attualmente più diffuso, che utilizza un protocollo proprietario, corredato di protezioni crittografiche[336]. Le chiavi di decrittazione non sono divulgate pubblicamente, ciò che rende le chiamate effettuate attraverso questo sistema pressoché impossibili da intercettare con i metodi classici, o meglio, intercettabili con una tempistica e dei costi incompatibili con le esigenze di giustizia.

Skype può funzionare in due modalità: c.d. "disconnesso" o *peer to peer*. Nel primo caso, il *software* consente di effettuare telefonate ad utenze telefoniche (fisse o mobili) di utenti non collegati tramite *computer*. In questa modalità, a pagamento, la comunicazione giunge in rete fino alla nazione del destinatario, dove viene, quindi, instradata sulla normale rete telefonica locale. Nel secondo caso, il *software* permette di effettuare comunicazioni completamente gratuite, ma a condizione che mittente e destinatario siano collegati a *Internet* e connessi tramite il *client Skype*.

Le possibilità di intercettare comunicazioni *Skype* devono essere valutate in funzione delle due differenti modalità di funzionamento del programma. Nel caso di utilizzo c.d. "disconnesso", proprio il tratto locale della comunicazione consentirebbe

[334] E infatti sul versante applicativo, non risultano esserci precedenti giurisprudenziali.
[335] S. MARIOTTI, S. TACCONI, *Riflessioni sulle problematiche investigative e di sicurezza connesse alle comunicazioni* VoIP, in *Dir. Internet*, 2008, p. 558 ss.
[336] Per proteggere la segretezza delle comunicazioni *Skype* utilizza l'algoritmo *AES*, lo *standard* più avanzato e sicuro disponibile pubblicamente in fatto di cifratura.

di disporre l'intercettazione con forme non troppo dissimili da quelle ordinarie, ma rimarrebbero fermi i problemi di decriptazione dei dati[337].

L'intercettazione è, invece, pressoché impossibile nel caso di funzionamento *peer to peer*: in tale schema operativo, infatti, non esistono *servers* centrali, ma il *software* assegna ad alcuni suoi utenti, in modo dinamico, il ruolo di "supernodi", generando *password* monouso, temporanee, ogni volta che si avvia una comunicazione. Gli stessi dati personali degli utenti (usati per la registrazione) non sono archiviati su *servers* centrali, ma distribuiti nella rete *peer to peer* tra i nodi, in forma criptata. Della conversazione non rimane traccia nemmeno sui tabulati[338].

A tali aspetti tecnici va aggiunto il fatto che la società *Skype* rifiuta di fornire la chiave di decifratura[339].

Allo stato attuale, dunque, l'unica possibilità di fruizione dei contenuti delle comunicazioni *Skype* consiste nel captare il dato fonico a monte o a valle della protezione crittografica, ciò che presuppone la disponibilità o il controllo del *personal computer* usato dall'utente monitorato. Tale risultato può essere raggiunto solo attraverso l'installazione, in locale o in remoto, di uno specifico *software* di *computer forensics* sul *computer* oggetto di "osservazione", che consente di creare una copia del flusso voce tra la scheda audio e il programma *VoIP*, ossia prima che *Skype* cominci a cifrare la comunicazione[340].

6.2 Acquisizione di e-mail

Altro tema su cui conviene riflettere è quello dell'acquisizione del contenuto dei messaggi di posta elettronica. Si assiste ad una potenziale concorrenza tra la

[337] C. PARODI, VoIP, Skype, cit., p. 1312.
[338] Il particolare funzionamento tecnico di *Skype* incide, inoltre, su altri strumenti d'indagine; infatti, la mancanza di un *server* centrale che immagazzina i dati rende difficilmente imponibili alla società stessa gli obblighi di conservazione dei dati. Da ciò deriva l'impossibilità di acquisire tali dati per le finalità di cui all'art. 132 codice *privacy* e di procedere a sequestro *ex* art. 254 *bis* c.p.p. Inoltre, va tenuto presente che la società *Skype* ha sede in Lussemburgo e quindi è soggetta alla normativa in tema di *data retention* di quel Paese, che ha attuato la direttiva 2006/24/CE. Si pongono quindi anche delicati problemi di cooperazione giudiziaria.
[339] Con l'acquisto di *Skype* da parte di *Microsoft*, nel 2011, non è da escludere un cambiamento della politica aziendale.
[340] Si tratta del *software* utilizzato in Germania per condurre c.d. perquisizioni *online* (*Online Durchsuchungen*) che sono state oggetto della sentenza del *BVerfG* esaminata nella prima parte del presente lavoro (*Supra*, capitolo I, par. 5.1). Si tornerà diffusamente sul tema nel prosieguo della trattazione, *infra*, capitolo III, par. 4 ss.

disciplina del sequestro e quella delle intercettazioni telematiche. Infatti, l'*e-mail* è al tempo stesso una forma di corrispondenza[341] e di comunicazione informatica. Inoltre, la comunicazione via *e-mail* è asincrona: il momento in cui il mittente spedisce il messaggio non coincide con quello della ricezione dello stesso da parte del destinatario[342]. Di qui le difficoltà nell'individuare la disciplina applicabile all'apprensione di *e-mail* immesse nel sistema di trasmissione, ma non ancora pervenute nella disponibilità del destinatario[343]. Infatti, se non si nutrono dubbi sull'assoggettabilità a sequestro dei messaggi di posta elettronica ricevuti e letti dal destinatario, il problema riguarda l'esatta individuazione dei confini dell'attività di intercettazione. Il quesito che si pone è se si debba considerare intercettazione solo quella che permette di captare il messaggio nel momento in cui il mittente lo invia, oppure se rientri in tale concetto anche l'acquisizione di copia del messaggio, dopo l'invio, ma prima che il destinatario lo abbia scaricato e letto, ossia quando la *e-mail* è in giacenza presso il *provider* del mittente o del destinatario.

Al fine di evitare l'applicazione di regimi diversi a seconda del momento in cui il messaggio è captato, si è proposto di applicare la disciplina delle intercettazioni ogni volta che l'apprensione riguardi messaggi non ancora letti o di cui non risulti certa la lettura, indipendentemente da dove si trovino. Infatti, l'intercettazione presuppone un procedimento di comunicazione in corso, procedimento che, nel caso dei messaggi di posta elettronica, si conclude solo con l'operazione di *check-mail* eseguita dal destinatario[344].

È evidente tuttavia, che quando la mail "giace" presso il *provider* del mittente o del destinatario, il flusso informatico è in stato di "quiete"[345] e ben potrebbe trovare

[341] Secondo la dottrina costituisce "corrispondenza informatica" quella destinata ad essere inoltrata o ricevuta per mezzo di un sistema informatico.
[342] R. ORLANDI, *Questioni attuali*, cit., p. 135.
[343] In maniera assolutamente sintetica ed esemplificando al massimo, si può descrivere il procedimento di comunicazione via *mail* come un percorso a tappe: innanzitutto il messaggio viene inviato dal mittente al suo *server* di posta elettronica, poi il *server* del mittente invia i dati al *server* del destinatario, infine, quando il destinatario si collega al proprio *server* per effettuare l'operazione di *check mail*, i dati vengono scaricati sul suo elaboratore. Cfr. G. DI PAOLO, (voce) *Prova informatica*, cit., p. 758.
[344] R. ORLANDI, *Questioni attuali*, cit., p. 135.
[345] Così, G. DI PAOLO, (voce) *Prova informatica*, cit., p. 26, la quale, in considerazione del funzionamento in concreto della comunicazione via *e-mail*, ritiene che la comunicazione elettronica non dia luogo ad un unico, ininterrotto flusso di dati, ma che «al contrario, sembra che essa sia la risultante del susseguirsi di distinti flussi, intervallati da momenti di "quiete"».

applicazione la disciplina del sequestro informatico di cui all'art. 254 *bis*[346] e all'art. 254 c.p.p., che consente di sequestrare presso i fornitori di servizi telematici o di telecomunicazioni, corrispondenza inoltrata per via telematica e che si deve supporre non ancora conosciuta dal destinatario, al pari di tutti gli oggetti di corrispondenza menzionati nel comma 1[347].

L'eventualità che una *e-mail* registrata nel *server* di posta elettronica del mittente, in attesa di essere comunicata al *provider* del destinatario, diverso da quello del mittente, possa essere sottoposta a sequestro con le modalità di cui all'art. 254 c.p.p. sarà del tutto remota, in considerazione dei tempi rapidissimi, e quindi della breve latenza, con cui il messaggio immagazzinato dal *server* viene smistato. Ciò non toglie che il problema della sovrapposizione tra disciplina del sequestro e delle intercettazioni sussista.

Il richiamo all'art. 254 *bis* c.p.p., invece, non convince. Tale norma introduce per la prima volta nell'ordinamento l'ipotesi del sequestro di dati informatici, compresi quelli di traffico e di ubicazione, presso i fornitori di servizi. Tuttavia, il codice di rito non definisce i dati in questione, né specifica per quanto tempo devono essere conservati. Occorre, dunque, fare riferimento al disposto del d. lgs. 109/2008, attuativo della direttiva comunitaria 2006/24/CE, che sancisce un generale obbligo di conservazione dei dati telematici per dodici mesi, escluso in ogni caso il contenuto della comunicazione[348]. È vero che l'art. 3 d. lgs. 109/2008 individua i dati da conservare facendo specifico riferimento alle «finalità di cui all'art. 132 codice *privacy*», ma sembra altresì ragionevole ritenere che gli obblighi di conservazione ivi sanciti assolvano alla più generale esigenza di accertamento e repressione dei reati a cui lo stesso sequestro *ex* art. 254 *bis* c.p.p. è preordinato. Ne consegue, con specifico riferimento alle *e-mail*, che tale norma consentirà di sequestrare i dati di traffico identificativi della comunicazione, ma non di apprenderne il contenuto.

Per quanto riguarda infine l'assoggettabilità a sequestro di un messaggio di posta elettronica già letto – e pertanto equiparato a corrispondenza aperta – va fatta una precisazione. I programmi di posta elettronica si dividono in due principali

[346] L. MARAFIOTI, Digital evidence, cit., p. 4515; S.VENTURINI, *Sequestro probatorio*, cit., p. 11.
[347] R. E. KOSTORIS, *Ricerca e formazione delle prova elettronica: qualche considerazione introduttiva*, in F. RUGGIERI, L. PICOTTI, *Nuove tendenze*, cit., p. 180. Questa peraltro la soluzione adottata dal *BVerfG*, sul punto v. *infra*, par. 6.2.1.
[348] Diffusamente sul punto, *infra*, par. 7 ss.

tipologie, quelli basati sul *Post Office Protocol* (*POP*) e quelli basati su altri protocolli di lettura, quali l'*Internet Message Access Protocol* (*IMAP*). Entrambi i protocolli permettono ad un *client* di accedere, leggere e cancellare le *e-mail* da un *server*, ma con alcune differenze. Il protocollo *POP* scarica la posta direttamente sul *computer*, cancellandola dal *server*; con il protocollo *IMAP*, invece, è possibile conservare copia delle proprie *e-mail* sul *server*, e scaricarle in un secondo momento su altri *computer*. I programmi che usano quest'ultimo protocollo permettono quindi di leggere la posta elettronica da qualsiasi postazione, senza che rimanga traccia del messaggio sul *computer* di volta in volta usato a tal fine. Anche limitando il discorso ai messaggi già letti, e quindi possibile oggetto di sequestro, e supponendo di poter distinguere senza apprezzabili margini di errore, la posta "aperta" da quella "chiusa", siffatta differenza tecnica ha dei riflessi significativi sull'utilizzabilità dei diversi strumenti d'indagine penale. Infatti, se l'utente utilizza programmi di lettura della posta elettronica che si basano sul *Post Office Protocol*, quali *Outlook Express* o *Eudora*, i messaggi saranno automaticamente scaricati sul *computer* e salvati sul relativo *hard-disk*. Per cui se, a seguito di perquisizione *ex* art. 247 comma 1 *bis* c.p.p.[349], dovessero rinvenirsi *e-mail* che si suppone costituiscano «corpo del reato o cose pertinenti al reato necessarie per l'accertamento dei fatti», queste saranno sequestrate ai sensi dell'art. 253 c.p.p., con le specifiche modalità indicate dall'art. 260 c.p.p.[350].

Diversamente si procederà nel caso in cui l'utente utilizzi servizi di *Webmail*, che sfruttano il protocollo *IMAP*. In questo caso, infatti, la posta elettronica può essere letta da qualsiasi *computer* con accesso ad *Internet*, senza che di essa rimanga traccia sull'*hard-disk*. Per "accedere" a tali messaggi sarà necessaria la collaborazione della persona colpita dall'operazione investigativa, che può essere anche soggetto diverso dall'indagato e terzo rispetto al processo penale. In caso di rifiuto di fornire *username* e *password*[351], l'accesso alla casella di posta elettronica

[349] Ad analoga attività di indagine può procedere la polizia giudiziaria ai sensi dell'art. 352 comma 1 *bis* c.p.p., nei casi ivi espressamente indicati.

[350] A seguito delle modifiche introdotte con legge 48/2008, l'art. 260 c.p.p. con riferimento a dati, informazioni o programmi informatici, ora dispone che la copia di essi, ai fini della conservazione, sia eseguita mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.

[351] Si ritiene che questa ipotesi rientri nel campo di applicazione del diritto al silenzio. La *password* è, infatti, un'informazione riservata che la persona sottoposta alle indagini ha diritto a mantenere tale. Lo

potrà avvenire solo attraverso l'installazione di uno specifico programma sul *computer* del destinatario della misura, che consenta agli inquirenti di prendere visione delle *e-mail* dell'utente ogni qualvolta questi acceda alla propria casella di posta elettronica[352]. In alternativa, si potrà procedere al sequestro delle *e-mail* presso il *service provider*[353].

Il discorso si complica ulteriormente se si considera che, in realtà, non sempre è agevole stabilire con certezza se il destinatario del messaggio lo abbia effettivamente letto. Questo vale per entrambi i protocolli di lettura della posta elettronica: normalmente i messaggi non ancora letti sono evidenziati, in modo da distinguerli da quelli già aperti, ma è opportuno considerare anche l'ipotesi in cui il messaggio sia stato inavvertitamente aperto dall'utente, che poi non lo abbia letto, o addirittura da un terzo, che legittimamente ha accesso a quella casella di posta. Si tratterà senz'altro di ipotesi remote, ma sufficienti ad insinuare il dubbio circa l'effettiva conoscenza del messaggio da parte del destinatario.

In definitiva, non resta che auspicare un intervento del legislatore, ai fini di un chiarimento circa la normativa applicabile e i confini tra i diversi mezzi di ricerca della prova.

6.2.1 Acquisizione di e-mail *nell'ordinamento processuale tedesco: la sentenza del* BVerfG *del 16 giugno 2009*

Spunti interessanti vengono dall'esperienza tedesca e da una recente sentenza del *BVerfG*[354]. Oggetto del ricorso era un provvedimento di sequestro delle *e-mail* dell'interessato, terzo rispetto al procedimento penale in corso, presso il *service provider* di posta elettronica, a seguito del rifiuto dell'interessato di fornire la *password* di accesso alla casella *e-mail*. Nell'affermare la legittimità di simile

---

stesso vale per chi, non sottoposto a procedimento penale, rischia con la sua collaborazione di far emergere una sua responsabilità penale. Cfr. S. VENTURINI, *Sequestro probatorio*, cit., p. 134.

[352] Il riferimento è sempre al *software* di *computer forensics* introdotto in Germania e che ha dato origine alla sentenza del *BVerfG* sulle *Online Durchsuchungen*. *Infra*, capitolo II, par. 4 ss.

[353] V. *infra*, par. 6.2.1.

[354] *BVerfG*, 16 giugno 2009, *2BvR 902/06*, reperibile anche su *www.bundesverfassungsgericht.de*. Cfr. D. BRODOWSKI, *Strafprozessualer Zugriff auf E-Mail Kommunikation – zugleich Besprechung zu BVerfG, Beschl. V. 16.6.2009 – 2 BvR 902/06 sowie zu BGH, Besch. Vom 31.3.2009 – 1 StR 76/09* -, in *JR*, 2009, p. 402 ss.; O. KLEIN, *Offen und (deshalb) einfach – Zur Sicherstellung und Beschlagnahme von* E-Mails *beim* Provider, in *NJW*, 2009, p. 2996 ss.

provvedimento, la Corte fa una lucida e dettagliata ricostruzione degli interessi in gioco e dei diritti costituzionali coinvolti, fissando taluni punti fermi in relazione al rapporto tra sequestro e segretezza delle comunicazioni in generale, e in particolare con riferimento all'inquadramento dell'attività di captazione di *e-mail*.

Questo il ragionamento della Corte: il procedimento comunicativo termina nel momento in cui il destinatario riceve la *mail*, ciò che dovrebbe far venir meno l'ambito di tutela dell'art. 10, comma 1 *GG* che garantisce la segretezza delle telecomunicazioni. Tuttavia, tale tutela è legata al mezzo di comunicazione prescelto, e nel caso delle *e-mail*, anche dopo che il destinatario le ha ricevute, esse non sono in realtà nel suo esclusivo dominio, bensì "appartengono" al *service provider* e l'interessato può semplicemente renderle leggibili su uno schermo nel momento in cui si collega al suo *mail server*. Egli può senz'altro tutelarsi attraverso una *password* contro l'accesso da parte di terzi, ma non ha mezzi tecnici per impedire la trasmissione delle *e-mail* da parte del *provider* agli investigatori. Da ciò deriva la necessità di applicare anche alle *e-mail* salvate sul *server* la tutela dell'art. 10, comma 1 *GG*, a prescindere dal fatto che esse vi siano salvate in via temporanea o definitiva e a prescindere dal fatto che il destinatario le abbia o meno lette. Né osta all'applicazione dell'art. 10, comma 1 *GG* il fatto che nel periodo in cui la *mail* è in giacenza presso il *mail server* del *provider* non si è in presenza di una comunicazione nel senso dinamico del termine. È vero, infatti, che il § 3 nr. 22 del *Telekommunikationsgesetz* – di seguito *TKG* - definisce le telecomunicazioni come «il procedimento tecnico di invio, trasmissione e ricevimento di segnali attraverso mezzi di telecomunicazione» e non si riferisce ad oggetti statici, ma è altresì vero che la tutela della segretezza delle telecomunicazioni di cui all'art. 10, comma 1 *GG* non è legata alla definizione del *TKG*, ma si ricollega all'esigenza del titolare del diritto di mantenere segrete le proprie comunicazioni.

Inoltre, se l'intromissione nella segretezza delle comunicazioni comporta altresì l'apprensione di dati personali, viene in rilievo la tutela offerta dal diritto all'autodeterminazione informativa (*informationelles Selbstbestimmungsrecht*, artt. 2, comma 1 e 1, comma 1 *GG*). Ancora una volta, quindi, la Corte mostra di aver compreso i pericoli per i diritti fondamentali insiti nelle nuove tecniche di indagine e la necessità di apprestare una tutela specifica e separata ai dati personali.

Non trova invece applicazione il neo coniato diritto alla garanzia dell'integrità e riservatezza dei sistemi informatici, in quanto fattispecie residuale che viene in rilievo solo quando la tutela offerta da altri diritti fondamentali - segretezza delle comunicazioni, inviolabilità del domicilio e autodeterminazione informativa - non è sufficiente.

Quindi, il *BVerfG* qualifica espressamente come sequestro il provvedimento di acquisizione di *e-mail* presso il *service provider*, e ritiene i §§ 94 ss. *StPO* adeguati allo scopo. In particolare, tali prescrizioni rispettano i requisiti di chiarezza e certezza che le norme devono avere per rispettare la riserva di legge di cui all'art. 10, comma 1 *GG*[355].

Interessante è infine il ragionamento che la Corte fa in materia di proporzionalità del mezzo di ricerca della prova, interessante non solo con riferimento al sequestro di *e-mail*, ma più in generale all'ipotesi del sequestro di grandi quantità di dati elettronici.

Presupposto è il bilanciamento di interessi contrapposti: da un lato la segretezza e riservatezza delle *e-mail*, che contengono dati di natura personale, spesso riguardanti terze persone, dall'altro l'importanza che la loro acquisizione può avere per le indagini penali – anche in considerazione dell'utilizzo a fini criminali che viene fatto delle nuove tecnologie. Proprio alla luce di quest'ultimo aspetto, la Corte ritiene adeguata la disciplina del sequestro che, a differenza di quella delle intercettazioni, non prevede un catalogo di reati-presupposto. È evidente, infatti, che l'intensità dell'intromissione nella segretezza delle comunicazioni è più intensa se avviene all'insaputa dell'interessato, come nel caso delle intercettazioni, e richiede presupposti diversi. Il sequestro di *e-mail* che, come nel caso di specie, avvenga a seguito di perquisizione locale, può essere disposto anche per reati di minore gravità, poiché l'interessato ne è al corrente[356]. Ciò non toglie che il mezzo di indagine sia particolarmente insidioso poiché si tratta di acquisire grandi quantità di dati[357]. A tal proposito è evidente che il sequestro sarà tanto più proporzionato, quante meno *e-*

[355] Ai sensi del § 98 *StPO* il sequestro viene disposto con provvedimento del giudice e in caso di pericolo nel ritardo può essere compiuto direttamente dal pubblico ministero o dalla polizia giudiziaria, salvo successiva convalida da parte del giudice

[356] La Corte ammette che si possa rinunciare alla preventiva informazione all'interessato quando essa possa nuocere alle indagini; in ogni caso è prevista un'informazione successiva, preordinata a permettere all'interessato di far valere il proprio diritto alla cancellazione o restituzione delle *e-mail*.

[357] Nel caso di specie erano state sequestrate tutte le *e-mail* dei precedenti due anni.

mail o in generale dati digitali irrilevanti per il procedimento in corso esso avrà ad oggetto. La Corte detta alcuni criteri di massima da seguire per perseguire tale obiettivo: innanzitutto si potranno effettuare delle ricerche mirate per parole chiave che dovrebbero filtrare le *e-mail* potenzialmente rilevanti. Se già questa prima scrematura dà esito negativo, l'attività di indagine dovrà terminare. Se invece si individuano messaggi di posta elettronica significativi per le indagini, occorre verificare se sia possibile acquisire solo quelli, tramite copia. Se non è possibile effettuare questa selezione *in loco*, occorrerà procedere ad un sequestro temporaneo, funzionale ad un successivo esame – *Durchsicht* – delle *e-mail* volto ad individuare quelle rilevanti, che saranno poi oggetto di sequestro vero e proprio (§ 110 *StPO*)[358]. Se si dovessero apprendere dati personali, legati al contenuto di una comunicazione, essi vanno immediatamente cancellati e non possono essere utilizzati.

Le *e-mail* che non hanno valore probatorio devono anch'esse essere cancellate o restituite.

Vanno poi adottate specifiche garanzie, che valgono in ogni caso in cui si ottengano informazioni la cui riservatezza è protetta dalla Costituzione: obblighi di informazione e cancellazione, diritti di partecipazione dell'interessato, divieti di utilizzazione[359].

7. Conservazione e acquisizione di dati di traffico

Tra gli strumenti investigativi che consentono di ottenere dati digitali precostituiti, ossia già esistenti in un sistema informatico, particolare importanza riveste la possibilità di acquisire i dati di traffico telematico presso i fornitori di servizi[360]. A tal fine sono previsti specifici obblighi di conservazione di tali dati (c.d. *data retention*), che potranno poi essere utilizzati non solo per finalità di repressione e accertamento dei reati ma anche di prevenzione.

---

[358] L'esame di cui al § 110 *StPO* serve ad impedire una sottrazione dei dati durevole ed eccessiva e quindi a ridurre l'intensità dell'intromissione nel diritto alla segretezza delle comunicazioni.

[359] Non è prevista la partecipazione dell'interessato alla "perquisizione" delle *e-mail* - il comma 3 del § 110 *StPO* è stato abrogato. Occorrerà pertanto valutare caso per caso se sia opportuno garantire la partecipazione dell'interessato o meno.

[360] Gli obblighi di conservazione e la possibilità di successiva acquisizione riguardano anche i dati di traffico telefonico – c.d. tabulati telefonici -. Essi, tuttavia, per le precisazioni sopra fatte, non sono oggetto di analisi nel presente lavoro. Cfr. *supra*, Introduzione, par. 2.

La materia è disciplinata dall'art. 132 d. lgs. 196 del 2003 – di seguito codice *privacy* – così come modificato in rapida successione dalla legge 48 del 2008 di ratifica della Convenzione di Budapest e dal d. lgs. 109 del 2008 di attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione[361]. Scopo di tale direttiva è di armonizzare gli obblighi di conservazione dei dati al fine «di garantir[n]e la disponibilità per finalità di indagine, accertamento e perseguimento di reati gravi» (art. 1). Tale obiettivo, tuttavia, è ben lungi dall'essere realizzato, innanzitutto in quanto la direttiva lascia eccessiva discrezionalità agli Stati membri circa l'individuazione dei tempi di conservazione, che possono variare da sei a ventiquattro mesi (art. 6), e circa la definizione delle «procedure da seguire e [del]le condizioni da rispettare per avere accesso ai dati conservati» (art. 4). Inoltre, la normativa nazionale di attuazione della suddetta direttiva è stata dichiarata incostituzionale in ben quattro Paesi membri (Bulgaria, Romania, Germania, Repubblica Ceca), i quali attualmente sono privi di una disciplina in materia[362].

Da ultimo la direttiva *data retention* è stata impugnata davanti alla Corte di Giustizia per violazione degli artt. 5, par. 4 TUE (principio di proporzionalità), 7 (diritto alla vita privata), 8 (tutela dei dati personali), 52, par. 1 (che fissa i presupposti della limitazione dei diritti previsti dalla Carta) della Carta dei Diritti

[361] Direttiva 2006/24/CE del 15 marzo 2006, in *GUCE* del 13 aprile 2006, L 105/54. Pur essendo successive nel tempo, le modifiche introdotte dal d. lgs. 109/2008 verranno esaminate per prime poiché hanno inciso sugli obblighi di conservazione, mentre le modifiche della legge 48/2008 hanno ad oggetto l'acquisizione dei dati di traffico, attività che logicamente e cronologicamente segue quella di conservazione e pertanto verranno analizzate in un secondo momento.

[362] Evidenti sono i riflessi negativi in tema di cooperazione giudiziaria tra Stati membri. Ciò peraltro dipende da un *vizio genetico* della direttiva che, in quanto atto di Primo Pilastro, non può prendere in considerazione questioni attinenti alla cooperazione giudiziaria o di polizia e non si preoccupa di armonizzare «*né la questione dell'accesso ai dati da parte delle autorità nazionali competenti in materia di repressione, né quella relativa al ricorso ai medesimi e al loro scambio fra le autorità in parola*». In questi termini si è pronunciata la Corte di Giustizia sul ricorso in annullamento presentato dall'Irlanda la quale contestava proprio la scelta della base giuridica. Infatti, trattandosi essenzialmente di atto preordinato ad agevolare l'indagine, l'accertamento e la repressione dei reati, esso avrebbe dovuto essere fondato sul Titolo VI del Trattato UE, e quindi si sarebbe dovuta adottare una decisione quadro. La Corte di Lussemburgo, rigettando il ricorso, ha precisato che la divergenza tra le normative nazionali in questo settore aveva un'incidenza negativa diretta sul funzionamento del mercato interno e ciò giustificava l'adozione di una direttiva. Corte di Giustizia dell'Unione Europea, sentenza 10 febbraio 2009, causa C-301/06, Irlanda c. Parlamento e Consiglio, in *www.curia.eu*.

Fondamentali dell'Unione Europea[363]. Come si è già visto, nelle sue conclusioni del 12 dicembre 2013, l'Avvocato Generale ha sostenuto che la direttiva costituisce un'interferenza nel diritto alla vita privata (art. 7 CDFUE) e che la conservazione di dati di traffico fino ad un massimo di due anni viola l'art. 52, comma 1 della Carta sotto il profilo della proporzionalità della limitazione di tale diritto fondamentale[364].

7.1 La conservazione dei dati relativi al traffico: il d. lgs. 109/2008

In più occasioni si è avuto modo di sottolineare come lo sviluppo della tecnologia, se da un lato ha reso possibili indagini su materiale informatico, di cui oggi difficilmente potrebbe farsi a meno per l'accertamento della maggior parte dei reati, dall'altro ha esposto la riservatezza, bene giuridico di rango costituzionale, a nuove forme di "invasione".

La disciplina della conservazione dei dati relativi al traffico telefonico e telematico - *species* del *genus* "dati personali" - è emblematica del conflitto tra esigenze di repressione penale e tutela della riservatezza. Innegabile è l'importanza di tali dati per le indagini, ma altrettanto evidente ne è il riflesso sulla sfera privata. Infatti, se si può certamente convenire sull'opportunità e utilità di tale legislazione che permette la costituzione di una banca dati a cui sia l'autorità giudiziaria che gli avvocati difensori potranno attingere, è al tempo stesso innegabile il fatto che si tratta di dati personali riguardanti la generalità degli utenti, che vengono conservati a prescindere dalla commissione di un reato.

Sembra opportuno ripercorrere brevemente la storia legislativa dell'art. 132 codice *privacy* che, introdotto nel 2003, ha subito molteplici interventi di riforma.

Nella stesura originaria la norma constava di un unico comma che imponeva al fornitore di servizi la conservazione dei dati relativi al traffico telefonico (comunemente conosciuti come tabulati telefonici) per un periodo di trenta mesi a

[363] Causa C-293/12, *Digital Rights Ireland Ltd contro The Minister for Communications, Marine and Natural Resources e altri* e causa C-594/12, *Kärntner Landesregierung Michael Seitlinger* e *Christof Tschohl*.

[364] Cfr. *Supra*, capitolo I, par. 4. Le conclusioni dell'avvocato generale, come noto, non sono vincolanti per la Corte di Giustizia; cionondimeno esse costituiscono una significativa presa di posizione, anche in considerazione del fatto che raramente la Corte si discosta dalle stesse. La sentenza è attesa per metà 2014.

fini di accertamento e repressione dei reati; tale prescrizione non riguardava i fornitori di servizi di comunicazione elettronica.

La disposizione si conformava ai principi generali sanciti dalla direttiva 2002/58/CE – c.d. direttiva *e-privacy*[365] - secondo cui i dati inerenti al traffico, se non necessari, non dovevano neppure essere formati e, in ogni caso, dovevano essere proporzionati alla funzionalità della rete o della prestazione del servizio e dovevano essere cancellati o resi anonimi quando non più necessari ai fini della trasmissione della comunicazione (art. 6 direttiva 2002/58/CE, artt. 3 e 11 d. lgs. 196/2003). L'art. 132 codice *privacy* costituiva, quindi, già all'epoca della sua introduzione, un'eccezione rispetto al generale divieto di conservare i dati relativi al traffico, prevedendone una conservazione temporanea, per esclusive finalità di accertamento e repressione dei reati.

A pochi mesi di distanza dall'entrata in vigore, il testo originario dell'art. 132, comma 1 è stato sostituito dall'art. 3 d. l. 354/2003 (convertito, con modifiche, in legge n. 45/2004) che prescriveva la conservazione dei dati di traffico telefonico per due periodi di ventiquattro mesi ciascuno, limitando l'obbligo di conservazione, dopo il decorso del primo periodo, esclusivamente per scopi di accertamento e repressione dei delitti di cui all'art. 407 comma 2 lett. a) c.p.p. Nonostante le critiche della dottrina, il legislatore non colse l'occasione per estendere l'obbligo di conservazione anche ai dati relativi al traffico telematico, con grave danno per le indagini informatiche, in cui i c.d. *files* di *log*[366] consentono l'identificazione dell'autore o del destinatario della comunicazione.

Il successivo d. l. 144/2005 (c.d. decreto Pisanu), convertito con modifiche dall'art. 1 legge 155/2005, ha introdotto nel testo dell'art. 132, comma 1 l'obbligo di conservare i dati relativi al traffico, con esclusione dei contenuti, e le chiamate senza risposta, prevedendo due distinti regimi temporali di conservazione a seconda che si tratti di traffico telefonico (due periodi di ventiquattro mesi) o di traffico telematico (due periodi di sei mesi). Inoltre, l'art. 6 del medesimo decreto legge ha modificato l'art. 132, comma 3, prevedendo che la richiesta dell'autorità giudiziaria, volta ad

[365] Direttiva del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, in *GUCE* del 31 luglio 2002, L 201/37.
[366] Il *file* di *log* è un *file* dove vengono registrate le operazioni compiute da un'applicazione o da un *server*. Più precisamente, si tratta di un *file* che il *server* forma automaticamente ogni volta che un utente accede ad una pagina *web* e serve, pertanto, a tenere traccia del traffico di dati telematici.

acquisire i dati relativi al traffico, venisse effettuata, non con ordinanza del giudice per le indagini preliminari, ma 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. L'art. 7 d. l. 144/2005, infine, ha imposto ai gestori di servizi pubblici e circoli privati che mettono a disposizione della clientela terminali utilizzabili per le conversazioni telematiche, l'obbligo di identificare e monitorare i clienti e ha approntato un regime transitorio in virtù del quale è stata sospesa temporaneamente l'applicazione di qualunque disposizione che prescriva o consenta la cancellazione dei dati del traffico (art. 6 comma 1)[367].

In questo complesso e mutevole quadro legislativo si inseriscono le modifiche introdotte, in rapida successione, dalla legge 48/2008, di ratifica della Convenzione di Budapest sui *cybercrimes*, e dal decreto legislativo 109/2008, di attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica[368].

Il d. lgs. 109/2008 ha modificato ulteriormente il neo-novellato art. 132 codice *privacy*, riducendo tra l'altro la durata degli obblighi di conservazione dei dati di traffico (art. 2), ha individuato le categorie di dati da conservare (art. 3), e ne ha fornito la definizione (art. 1).

L'art. 1 d. lgs. 109/2008 non modifica né aggiorna le definizioni già presenti nel codice per la protezione dei dati personali in materia di *data retention*[369]*,* ma ne aggiunge di nuove inerenti la telefonia e i dati relativi al traffico. Tale scelta appare criticabile poiché le presenza di due disposizioni, aventi lo stesso oggetto, ma non perfettamente sovrapponibili, non fa che aumentare la confusione e il dubbio degli interpreti in una materia già di difficile comprensione a causa della sua tecnicità[370]. Per quanto riguarda i dati relativi al traffico, la definizione contenuta nel d. lgs. 109/2008 si differenzia da quella contenuta nel codice *privacy*, in quanto

[367] Termine originariamente fissato al 31 dicembre 2007, ma successivamente prorogato al 31 dicembre 2008 dall'art. 34 del d. l. 248/2007 convertito in legge n. 31/2008.
[368] Tale direttiva ha modificato la direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.
[369] Art. 4 d. lgs. 196/2003.
[370] S. ATERNO, A. CISTERNA, *Il legislatore interviene ancora sul* data retention*, ma non è finita*, in *Dir. pen. proc.*, 2009, p. 282 ss.

ricomprende anche i «dati necessari per identificare l'abbonato o l'utente», laddove per «dati necessari ad identificare l'utente» devono intendersi gli indirizzi *IP*[371].

Il decreto, inoltre, per la prima volta, fornisce una definizione di traffico telefonico, assente nel d. lgs. 196/2003. Tale definizione ha una portata innovativa non secondaria se si considera che include tra le "chiamate" anche "quelle basate sulla trasmissione di dati", cioè quelle effettuate con sistemi *VoIP* o con piattaforma *Skype*[372]. Ciò significa, contrariamente a quanto si potrebbe pensare, che i c.d. "dati di pacchetto", cioè dati informatici e telematici usati per le comunicazioni vocali via *Internet*, sono considerati dati di traffico telefonico e, come tali vanno conservati per ventiquattro mesi e non dodici, come prescritto per i dati informatici. Analogo discorso vale per la conservazione degli *SMS*, che vengono considerati traffico telefonico e che sono conservati, escluso il contenuto della comunicazione, per ventiquattro mesi.

Definizione altrettanto fondamentale e nuova è quella di «indirizzo di protocollo *Internet* (*IP*) univocamente assegnato»: si tratta di un indirizzo *IP*[373] che consente l'identificazione diretta dell'abbonato o utente che effettua comunicazioni sulla rete pubblica. I fornitori dei servizi pubblici di comunicazione elettronica hanno l'obbligo, sanzionato a norma dell'art. 162 *bis* comma 2 del codice *privacy*[374], di identificare i propri utenti attribuendo univocamente a ciascuno un indirizzo *IP* di rete pubblica. La scelta si giustifica alla luce della tendenza dei fornitori di servizi telematici di utilizzare sistemi *NAT/PAT* (*Network & Port Address Translation*) che prevedono l'assegnazione di un solo *IP* di rete pubblica ad una serie indeterminata di

[371] Al tema della conservazione degli indirizzi *IP* è dedicato un apposito paragrafo, v. *infra*, par. 8.1.
[372] Sulla possibilità concreta di imporre tali obblighi di conservazione alle società che forniscono servizi *VoIP*, e in particolare a *Skype*, si veda *supra*, par. 6.1.2.
[373] Un indirizzo *IP* è un numero che identifica univocamente, nell'ambito di una singola rete, i dispositivi collegati con una rete informatica che utilizza lo *standard IP* (*Internet Protocol*). Ciascun dispositivo (*router*, *computer*, *server* di rete, stampanti, *smartphone*, *etc.*) ha un suo indirizzo *IP*. Gli indirizzi sono composti da 4 *byte*, una parte dei quali identifica la rete e la restante parte il nodo all'interno della rete. Ogni *byte* è separato dagli altri con un punto e per questo gli indirizzi *IP* hanno una struttura del tipo 192.168.1.1. L'assegnazione dei numeri *IP* viene effettuata dall'*ICANN*, un ente americano che li distribuisce, singolarmente o in blocco, ai richiedenti.
[374] L'art. 162 *bis* è stato introdotto dall'art. 5 d. lgs. 109/2008 e prevede, nel caso di assegnazione di un indirizzo *IP* che non consente l'identificazione univoca dell'utente o dell'abbonato, l'applicazione della sanzione pecuniaria da euro 5.000 a 50.000, aumentabile fino al triplo in ragione delle condizioni economiche dei responsabili della violazione.

utenti assegnatari di indirizzi *IP* di rete privata, con conseguente maggiore difficoltà per gli investigatori nel risalire all'utente[375].

L'art. 6 d. lgs. 109/2008 recante «disposizioni transitorie e finali» fissa un termine di novanta giorni dall'entrata in vigore del decreto stesso, entro cui i fornitori di servizi devono adempiere all'obbligo. In particolare, entro questi novanta giorni (ossia entro il 1° ottobre 2008), i gestori avrebbero dovuto procedere ad un duplice adempimento: cancellare i dati telematici diversi da quelli enumerati dall'art. 3 d. lgs. 109/2008, oltre che quelli conservati anteriormente al 1° ottobre 2007 (in quanto conservati da un anno), e predisporre l'assegnazione di un indirizzo *IP* univoco per "tracciare"[376] gli indirizzi *Internet* cui l'utente ha accesso durante la navigazione[377].

L'art. 2 d. lgs. 109/2008 modifica nuovamente, a pochi mesi dall'entrata in vigore della legge 48/2008, che già vi aveva aggiunto i commi da 4 *ter* a 4 *quinquies*, l'art. 132 codice *privacy*, inserendo il comma 1 *bis* dedicato alle cosiddette chiamate senza risposta[378]. La direttiva comunitaria distingue tra "tentativo di chiamata non riuscito", soggetto all'obbligo di conservazione, e "chiamata non collegata", sottratto a qualsiasi obbligo di conservazione[379]. A questo scopo definisce il tentativo di chiamata non riuscito come «una chiamata telefonica che è stata collegata con successo ma non ha ottenuto risposta, oppure in cui vi è stato un intervento del gestore della rete» (art. 2, comma 2 lett. f). Di tale distinzione non vi è traccia nel d. lgs. 109/2008 che all'art. 1 definisce la chiamata senza risposta come «la connessione istituita da un servizio telefonico accessibile al pubblico, non seguita da un'effettiva comunicazione, in quanto il destinatario non ha risposto ovvero vi è stato un

[375] Poiché milioni di persone si collegano a *Internet* ogni secondo, è di fondamentale importanza nel momento in cui l'autorità giudiziaria chiede di acquisire tali dati che fornisca in maniera precisa data e ora. Un errore anche di un solo secondo potrebbe portare all'identificazione di una persona sbagliata. Cfr. G. VACIAGO, *La disciplina normativa sulla* data retention *e il ruolo degli* Internet Service Provider, in L. LUPARIA (a cura di), Internet provider *e giustizia penale*, cit., p. 156.

[376] Il c.d. *tracing*, o attività di tracciamento, è il primo accertamento tipico, e tecnico, delle indagini sul *cybercrime*, ed è cosa ben diversa dall'attività di intercettazione. Più opportunamente, è equiparabile all'acquisizione dei tabulati telefonici.

[377] Tuttavia, preso atto delle difficoltà incontrate da alcuni fornitori, i quali non disponevano, nell'immediato, di un numero sufficiente di indirizzi *IP* di rete pubblica da assegnare univocamente, il legislatore è intervenuto nuovamente, prorogando la scadenza al 31 dicembre 2008 (d. l. 151/2008, convertito in legge 186/2008).

[378] Anche in questo àmbito è intervenuto il d. l. 151/2008, convertito in legge 186/2008, stabilendo che le disposizioni concernenti la conservazione delle chiamate senza risposta di cui al nuovo art. 132, comma 1 *bis* codice *privacy* entreranno in vigore il 1° gennaio 2009 in ragione di analoga difficoltà incontrata dagli operatori telefonici nell'aggiornare gli apparati delle reti fisse. Sin a tale data è rimasta, quindi, in vigore la disciplina prevista dal decreto 144/2005.

[379] Art. 3, comma 2 direttiva 2006/24/CE.

intervento del gestore della rete». Il legislatore italiano ha, invece, previsto un periodo di conservazione diverso per le chiamate senza risposta, senza che ciò fosse prescritto dalla direttiva comunitaria. Il comma 1 *bis* dell'art. 132 prevede, infatti, che i dati relativi alle chiamate senza risposta siano conservati per trenta giorni. Ne deriva una disciplina degli obblighi di conservazioni dei dati di traffico che distingue tra dati telefonici (obbligo di conservazione per ventiquattro mesi), dati telematici (obbligo di conservazione per dodici mesi) e chiamate senza risposta (obbligo di conservazione per trenta giorni), e che non era prevista dalla direttiva comunitaria[380].

L'intervento del d. lgs. 109/2008 sull'art. 132 codice *privacy* non si limita alla sola disciplina delle chiamate senza risposta, ma comprende anche l'abrogazione di alcuni commi e la modifica delle modalità di conservazione dei dati.

Per quanto riguarda il primo aspetto, con l'abrogazione del comma 2 dell'art. 132, il d. lgs. 109/2008 ha escluso qualsivoglia rilevanza della tipologia dei delitti per cui si procede, instaurando un regime di conservazione indifferenziato, entro i limiti di tempo individuati dai commi precedenti[381]. Il comma 2 dell'art. 132, infatti, subordinava l'acquisizione dei dati di traffico, entro i più ampi limiti temporali in esso descritti, alla condizione che fossero sussistenti «esclusive finalità di accertamento e repressione dei delitti di cui all'art. 407, comma 2, lett a) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici». Conseguentemente, sono stati abrogati anche i commi 4 e 4 *bis* dell'art. 132 che

[380] L'art. 6 della direttiva 2006/24/CE stabilisce che «gli Stati membri provvedono affinché le categorie di dati di cui all'art. 5 siano conservate per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione». Il *considerandum* n. 12 della direttiva, tuttavia, esclude esplicitamente dall'ambito di applicazione della stessa le chiamate senza risposta, che continuano ad essere disciplinate dall'art. 15 della precedente direttiva, la direttiva 2002/58/CE. La legittimazione dei governi nazionali ad adottare misure di conservazione dei dati più stringenti e derogatorie rispetto alle previsioni comunitarie deve rinvenirsi proprio nel suddetto art. 15 che abilita i legislatori nazionali all'approvazione di una sorta di stato d'eccezione tutte le volte in cui la deroga alle procedure di conservazione dei dati telefonici e telematici risulti giustificata da particolari esigenze di sicurezza.

[381] Peraltro in aperta contraddizione con l'art. 1 della direttiva 2006/24/CE che prevede che i dati conservati siano utilizzati «a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale». G. VACIAGO, *La disciplina normativa*, cit., p. 155, ritiene che proprio la genericità dell'espressione reato grave abbia permesso ad alcuni Stati membri, tra cui l'Italia, di non recepire tale concetto e quindi di non limitare l'applicazione della direttiva. Come si è visto, nelle sue recenti conclusioni presentate il 12 dicembre 2013, nelle cause riunite C-293/12, *Digital Rights Ireland Ltd contro The Minister for Communications, Marine and Natural Resources e altri* e C-594/12, *Kärntner Landesregierung Michael Seitlinger* e *Christof Tschohl*, l'avvocato generale Pedro Cruz Villalòn ha criticato il fatto che la direttiva si limiti genericamente a fare riferimento a «reati gravi». Ciò, infatti, ha inevitabili conseguenze in sede di implementazione da parte degli Stati membri e quindi, in definitiva, ai fini dell'auspicata armonizzazione in materia di *data retention*. *Supra*, capitolo I, par. 4.

prevedevano, nel caso di cui al secondo comma, un controllo del giudice per le indagini preliminari circa la sussistenza del titolo di reato e di sufficienti indizi dei reati indicati nel comma 2. Allo stato attuale, dunque, i dati conservati a norma dei commi 1 e 1 *bis* dell'art. 132 codice *privacy* possono essere 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 (art. 132, comma 3 d. lgs. 196/2003)[382].

Infine, l'art. 2 d. lgs. 109/2008 modifica l'art. 132, comma 5 codice *privacy* che si occupa delle modalità di conservazione dei dati. In particolare, si intende assicurare che i dati vengano conservati con accorgimenti tecnologici che assicurino «i medesimi requisiti di qualità, sicurezza e protezione dei dati in rete»[383]. Si vuole, cioè, evitare che la conservazione dei dati di traffico avvenga con modalità difformi da quelle usualmente adoperate dal titolare nella gestione delle reti; in questo senso va dunque letta la soppressione delle lettere b) e c) dello stesso comma 5 che, invece, consentivano trattamenti e obblighi di conservazione differenziati tra dati in rete e dati immagazzinati.

L'art. 3 d. lgs. 109/2008 distingue sei macro-categorie di dati da conservare[384], all'interno delle quali distingue ulteriormente tra dati telefonici, suddivisi in telefonia fissa e mobile, e dati telematici. Si deve trattare, in ogni caso,

---

[382] Si tratta di un ordine di esibizione ai sensi degli artt. 256 c.p.p. e 132 d. lgs. 196/2003.

[383] Il Garante per la protezione dei dati personali ha individuato tali misure nell'obbligo per gli *Internet service providers* di dotarsi di idonei strumenti di autenticazione e autorizzazione, di conservare separatamente i dati di traffico utilizzati per finalità di accertamento e repressione dei reati rispetto a quelli utilizzati per altre finalità, di cancellare i dati decorsi i termini massimi di conservazione, di approntare strumenti in grado di permettere il controllo delle attività svolte sui dati da ciascun incaricato, e di utilizzare sistemi di cifratura e protezione dei dati. Autorità Garante per la Protezione dei Dati Personali, provvedimento del 17 gennaio 2008, in *www.garanteprivacy.it*, pubblicato in *G.U.* del 5 febbraio 2008, n. 30. Tali misure sono evidentemente apprezzabili sotto il profilo della tutela della *privacy*, ma non si può tacere il fatto che esse rappresentano per gli *ISP* un onere economico e gestionale notevole, senza che sia previsto alcun rimborso. In questi termini G. VACIAGO, *La disciplina normativa sulla* data retention, cit., p. 149. Peraltro, proprio il fatto che i costi della conservazione siano a carico dei fornitori di servizi ha determinato il successo di tale strumento di indagine che per gli investigatori, e quindi per lo Stato è molto più economico delle intercettazioni. V. M. A. ZÖLLER, *Die Vorratsspeicherung von Telekommunikationsdaten – (Deutschen) Wege und Irrwege*, *Congress on the Criminal Law Reforms in the World and in Turkey. Atti del convegno internazionale svoltosi a Istanbul-Ankara dal 26 maggio al 4 giugno 2010, Istanbul 2010*, p. 33.

[384] a) dati necessari per rintracciare e identificare la fonte di una comunicazione; b) dati necessari per rintracciare e identificare la destinazione di una comunicazione; c) dati necessari per determinare la data, l'ora e la durata di una comunicazione; d) dati necessari per determinare il tipo di comunicazione; e) dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature; f) dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile.

di "dati esterni", escluso il contenuto della comunicazione. A tal proposito, sono sorte accese polemiche aventi ad oggetto l'individuazione dei dati del traffico *Internet*, con particolare riguardo alla conservazione degli indirizzi *IP*[385]. Infatti, al di là dall'elenco contenuto nel suddetto art. 3, occorre accertare se l'indicazione dei siti visitati durante la navigazione, a prescindere da qualsiasi richiamo al contenuto delle pagine *web* consultate, rappresenti un dato esteriore della comunicazione telematica oppure abbia natura di contenuto, come tale assolutamente escluso dall'obbligo di conservazione.

7.2 Acquisizione degli indirizzi IP

La questione centrale ruota attorno alla possibilità di qualificare o meno l'indirizzo *IP* di destinazione, cioè la pagina *web* visitata dall'utente, quale dato esterno ad una comunicazione, in maniera analoga a quanto accade per il numero telefonico del destinatario di una telefonata.

Il Garante per la Protezione dei Dati Personali qualche mese prima del recepimento della direttiva 2006/24/CE nell'ordinamento interno aveva messo in guardia rispetto alle caratteristiche delle comunicazioni telematiche che presentano ulteriori e più specifiche criticità rispetto alle comunicazioni telefoniche tradizionalmente intese. Infatti, il dato apparentemente "esterno" a una comunicazione spesso identifica o rivela nella sostanza anche il suo contenuto; ciò che può permettere non solo di ricostruire relazioni personali e sociali, ma anche di desumere particolari orientamenti, convincimenti e abitudini degli interessati. *Ergo*, l'indirizzo *IP* di destinazione (l'*URL* visitato) andrebbe escluso dagli obblighi di conservazione in quanto, contrariamente a quanto *prima facie* potrebbe apparire, non può essere banalmente considerato un dato esterno della comunicazione[386].

Conseguentemente il legislatore, nel recepire la suddetta direttiva europea, ha escluso gli indirizzi *IP* di destinazione dal novero dei dati da conservare, includendovi solo gli indirizzi *IP* di origine.

[385] Vanno invece senz'altro conservati i c.d. *files* di *log*, che consentono di tenere traccia delle attività compiute su *Internet* da un determinato utente (c.d. *tracing*).
[386] Parere del Garante per la Protezione dei Dati Personali del 18 gennaio 2008, cit.

Tuttavia, se è pur vero che la pagina *web* è suscettibile di fornire più informazioni sull'utente rispetto ad un numero di telefono, bisogna altresì considerare che anche una volta individuato il sito visitato, la volatilità dei contenuti dello stesso rende indeterminabile il reale contenuto visionato e quindi difficilmente si verificheranno rischi per la *privacy*.

In considerazione di ciò, e soprattutto dell'importanza che la conoscenza dell'indirizzo *IP* di destinazione può avere ai fini delle indagini[387], la dottrina è propensa a considerarlo dato esterno di una comunicazione telematica, ascrivibile ai «dati necessari per rintracciare e identificare la destinazione di una comunicazione» (art. 3, lett. b), d. lgs. 109/2008). In nulla, quindi, una comunicazione telematica si differenzierebbe da una telefonica[388].

Il problema che si presenta è, ancora una volta, quello del bilanciamento tra esigenze diverse e contrapposte: la repressione dei reati da un lato, e la riservatezza dall'altro. Si tratta innanzitutto di capire se effettivamente l'indirizzo *IP* di destinazione sia in grado di rivelare il contenuto della navigazione, con conseguente lesione della riservatezza e, in caso di risposta affermativa, appurare se, comunque, tale conoscenza sia indispensabile per le indagini penali e come tale possa determinare un giusto sacrificio della riservatezza.

Nel fare ciò può venire in aiuto la recente sentenza del *BVerfG* sul *data retention*, laddove la Corte precisa che la tradizionale distinzione tra contenuto della comunicazione e dati esterni elaborata con riferimento alle comunicazioni telefoniche non trova applicazione nel caso delle comunicazioni telematiche[389]. Infatti, la conoscenza del sito *Internet* visitato comporta l'apprensione del contenuto

[387] Non solo, ma la possibilità di acquisire tali dati, opportunamente conservati, può rivelarsi di fondamentale importanza sia per chi sia accusato della commissione di un reato, sia per la persona offesa dal reato medesimo, garantendo la possibilità di ottenere informazioni utili e, dunque, l'acquisizione di mezzi di prova a sostegno della rispettiva posizione processuale.

[388] S. ATERNO, A. CISTERNA, *Il legislatore interviene*, cit., p. 294; F. CAJANI, Internet Protocol. *Questioni operative in tema di investigazioni penali e riservatezza*, in *Dir. Internet*, n. 2008, p. 545 ss. Secondo questo Autore, l'indirizzo *IP* è paragonabile al numero di telefono del destinatario di una comunicazione telefonica: in entrambi i casi si ha a che fare con dati esterni della comunicazione, che nulla dicono del contenuto della conversazione o della navigazione. Simili considerazioni vengono fatte anche dalla dottrina tedesca, cfr. S. KRÜGER, S. A. MAUCHER, *Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit großen Auswirkungen auf die Praxis*, in *MMR*, 2011, p. 433 ss.; P. MEYERDIERKS, *Sind IP-Adressen personenbezogene Daten?*, *ivi*, 2009, p. 8 ss.

[389] *BVerfG*, 2 marzo 2010, *1BvR 256/08*, *1 BvR 263/08*, *1 BvR 586/08*, reperibile anche su *www.bundesverfassungsgericht.de*. Sul punto si avrà modo di tornare approfonditamente, *infra*, par. 7.5.

della comunicazione. Pertanto l'indirizzo *IP* di destinazione va escluso dal novero dei dati da conservare in quanto rientra nell'ambito di tutela dell'art. 10 *GG* che garantisce la segretezza della comunicazione.

Se, tuttavia, gli investigatori dovessero per altra ragione già essere a conoscenza dell'indirizzo *IP* di destinazione e volessero per suo tramite risalire all'utente che ha visitato quella pagina *web*, potrebbero farlo, a condizione che ciò sia necessario per il perseguimento di un grave reato, previa autorizzazione del pubblico ministero e attraverso una procedura trasparente che assicuri l'informazione all'interessato. Così si è pronunciato il *BVerfG* nel dichiarare l'incostituzionalità del § 113a, secondo periodo *TKG* che non rispettava tali prescrizioni.

Al di là della declaratoria di incostituzionalità, che verrà approfondita nel prosieguo della trattazione, ciò che preme fin da ora evidenziare è il ragionamento della Corte in tema di bilanciamento tra esigenze investigative e diritti fondamentali. L'idea di partenza è che non tutte le intromissioni nello stesso diritto fondamentale - nella specie l'art. 10 *GG*, ma il discorso vale in generale - richiedono il rispetto degli stessi presupposti. Questo è l'approccio da seguire, la soluzione non è proibire determinate attività di indagine, ma effettuare un corretto bilanciamento degli interessi in gioco. Ciò evidentemente presuppone la previa individuazione dei diritti fondamentali coinvolti e dei rispettivi confini[390] e, soprattutto, del loro nucleo essenziale, insuscettibile di bilanciamento.

Quindi, l'indirizzo *IP* rientra nell'ambito di tutela dell'art. 10 *GG*, ma non nel nucleo essenziale della riservatezza, e pertanto può essere limitato al ricorrere di presupposti meno stringenti rispetto a quelli previsti per l'intercettazione di comunicazioni[391].

[390] Ciò è ben descritto dal *BVerfG* nella sentenza sulla *Online Durchsuchung*. V. *supra*, capitolo I, par. 5.1.

[391] Si tratta di conclusione analoga a quella raggiunta dalla nostra Corte costituzionale in materia di c.d. tabulati telefonici, i quali, pur ricadendo sotto la tutela dell'art. 15 Cost., non esigono per la loro apprensione un procedimento analogo a quello previsto per le intercettazioni. Si veda *supra*, capitolo I, par. 1.2.

7.3 L'acquisizione di dati di traffico ai sensi dell'art. 132 codice privacy *tra finalità repressive e preventive*

L'art. 10 legge 48/2008 ha inserito i commi 4 *ter*, 4 *quater*, 4 *quinquies* all'interno dell'art. 132 d. lgs. 196/2003 dando esecuzione agli artt. 16, 17 e 18 della Convenzione di Budapest, che impongono agli Stati di adottare misure volte a garantire la conservazione e l'integrità di dati informatici e di traffico, anche se detenuti presso terzi.

In particolare, il comma 4 *ter* disciplina una peculiare ipotesi di investigazione preventiva avente ad oggetto i dati relativi al traffico telematico e attribuisce al Ministro dell'Interno o, su sua delega, alle forze di polizia, il potere di ordinare, anche su richiesta avanzata da un'autorità straniera, ai fornitori e agli operatori di servizi informatici e telematici la conservazione e protezione per novanta giorni, prorogabili sino a sei mesi, dei dati di traffico telematico, con esclusione dei contenuti, per lo svolgimento delle investigazioni di cui all'art. 226 norme att. c.p.p., ovvero per l'accertamento e la repressione di specifici reati. Si tratta di un'attività di carattere eccezionale ed urgente rimessa all'iniziativa della polizia giudiziaria in una fase antecedente all'instaurazione del procedimento penale, finalizzata alla conservazione e protezione di dati vulnerabili, suscettibili di modificazione e cancellazione[392].

Tale comma prevede una peculiare ipotesi di "congelamento" – *freezing* secondo la terminologia anglosassone - di dati telematici, che si differenzia da quella già contemplata dal primo comma dello stesso art. 132 codice *privacy*[393].

Il comma 1 dell'art. 132 impone, per finalità di accertamento e repressione dei reati, ai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, l'obbligo di conservazione dei dati relativi al traffico telefonico per ventiquattro mesi dalla data della comunicazione e di quelli relativi al traffico telematico per dodici mesi dalla stessa data, escluso comunque il contenuto delle comunicazioni.

[392] Tale attività viene denominata anche *data preservation*, per distinguerla da quella di *data retention*.
[393] Per i rapporti tra tale particolare ipotesi di acquisizione di dati di traffico e il sequestro di dati informatici di cui all'art. 254 *bis* c.p.p., v. *infra*, par. 7.4.

La differenza tra le due disposizioni è apprezzabile sotto due differenti aspetti. Innanzitutto, il nuovo comma 4 *ter* contempla la possibilità che il provvedimento che dispone la conservazione imponga ai fornitori di servizi specifiche modalità di conservazione dei dati. Si tratta, quindi, di un'attività che va ben oltre la mera conservazione di dati e richiede specifiche cognizioni tecniche al fine di tutelare un patrimonio di informazioni suscettibili di cancellazione o modificazione. La disposizione dà piena attuazione all'art. 16 Convenzione di Budapest, che impone alle parti contraenti di adottare misure legislative e di altra natura per consentire la protezione rapida di specifici dati informatici quando vi è motivo di ritenere che gli stessi siano particolarmente vulnerabili e soggetti a cancellazione o modificazione.

Inoltre, le due disposizioni si differenziano circa le finalità: in entrambi i casi si tratta di strumenti di accertamento e repressione di reati, tuttavia, la conservazione dei dati disciplinata dal comma 1 è finalizzata all'acquisizione degli stessi e alla conseguente utilizzabilità processuale, mentre la conservazione e protezione dei dati di cui al comma 4 *ter,* per espressa disposizione di legge, ha di mira altresì lo svolgimento delle investigazioni preventive previste dall'art. 226 disp. att. c.p.p. Si tratta in questo caso di un'attività eccezionale ed urgente, rimessa al potere discrezionale delle forze di polizia e dei servizi segreti, esperibile con finalità di prevenzione. In nessun caso i risultati di tali indagini potranno essere utilizzati in un successivo procedimento penale (art. 226, comma 5 disp. att. c.p.p.).

Una questione particolarmente delicata che si è posta è quella dell'individuazione dei soggetti destinatari del provvedimento di *freezing*. Infatti, l'art. 132, comma 4 *ter* codice *privacy* si limita a far riferimento genericamente a fornitori di servizi informatici o telematici. Tra questi sono astrattamente annoverabili non solo i fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazioni accessibile al pubblico, ma anche tutti i soggetti che offrono direttamente o indirettamente servizi di comunicazione elettronica, i gestori di siti *Internet* che diffondono contenuti sulla rete (c.d. *content provider*) e i gestori di motori di ricerca. I dati di traffico telematico trattati da queste ultime due categorie di soggetti consentono di "tracciare" agevolmente le operazioni compiute dall'utente in rete e spesso rivelano, nella sostanza, il contenuto della comunicazione; non

possono, pertanto, essere qualificati come meri "dati esterni del traffico", analogamente a quelli di cui all' art. 132, comma 1. Infatti, mentre questi ultimi sono relativi per lo più alle registrazioni degli accessi (c.d. *files* di *log* degli indirizzi *IP*) e sono simili a quelli di telefonia, in quanto individuano il *computer* che si è connesso alla rete e registrano l'associazione tra indirizzo *IP* assegnato all'utente e numero telefonico chiamante, i dati di cui al comma 4 *ter* afferiscono ai servizi forniti dai *provider* e spesso svelano l'oggetto della comunicazione. Sul punto è intervenuto il Garante per la Protezione dei Dati Personali che ha precisato che «devono ritenersi tenuti alla conservazione dei dati ai sensi dell'art. 132 d. lgs. 196/2003 i soggetti che realizzano esclusivamente, o prevalentemente, una trasmissione di segnali su reti di comunicazione elettroniche, a prescindere dall'assetto proprietario della rete, e che offrono servizi a utenti finali secondo il principio di non discriminazione»; sono invece espressamente esclusi i *content provider* e i gestori di motori di ricerca, in quanto i dati di traffico telematico che essi trattano consentono di identificare il "contenuto" della comunicazione[394].

Il neo-introdotto art. 132, comma 4 *quinquies* stabilisce che i provvedimenti adottati a norma del precedente comma 4 *ter* siano comunicati per iscritto, senza ritardo o comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione, il quale, se ne ricorrono i presupposti, li convalida.

Le disposizioni esaminate – art. 132, commi 4 *ter* e 4 *quinquies* - contemplano una specifica ipotesi di investigazione preventiva che, in quanto tale, dovrebbe rispettare le prescrizioni dell'art. 226 disp. att. c.p.p. Tuttavia, il comma 4 *ter* non individua i presupposti subordinatamente ai quali il magistrato inquirente può legittimamente emettere il decreto di convalida e, pur prevedendo la possibilità che il provvedimento originario sia prorogato per motivate esigenze, non richiede, analogamente all'art. 226 disp. att. c.p.p., che l'autorizzazione alla prosecuzione delle operazioni sia data con decreto motivato, nel quale deve essere dato chiaramente atto dei motivi che rendono necessaria la prosecuzione delle operazioni. Non solo, ma il "congelamento" dei dati informatici di cui al comma 4 *ter* non è ancorato alla

[394] Cfr. parere del Garante per la Protezione dei Dati Personali del 18 gennaio 2008, modificato il 24 luglio 2008, in *www.garanteprivacy.it*.

preesistenza di «elementi investigativi che giustificano l'attività di prevenzione» e alla «necessità», requisiti entrambi previsti dall'art. 226 disp. att. c.p.p.

Fondamentale è comunque che, trattandosi di investigazione preventiva, venga rispettato il divieto di utilizzazione nel procedimento penale prescritto dal comma 5 dell'art. 226 disp. att. Tale esigenza è soddisfatta dal testuale richiamo, contenuto nelle disposizioni in esame, ai «fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989».

Un ultimo cenno merita il comma 4 *quater* dell'art. 132 che sanziona con le pene previste dall'art. 326 c.p. i soggetti destinatari dell'obbligo di conservazione e protezione dei dati informatici in caso di rivelazione del segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte. Tale norma si ricollega al comma 5 dell'art. 226 disp. att. c.p.p. che stabilisce che le attività di intercettazione preventiva e le notizie acquisite a seguito delle attività medesime non possono essere menzionate in atti di indagine, né costituire oggetto di deposizione, o essere altrimenti divulgate.

I nuovi commi dell'art. 132 sembrano conferire alla polizia giudiziaria un potere limitato ai casi eccezionali ed urgenti, sottoposto al controllo del pubblico ministero, da esercitarsi in un arco di tempo limitato. Tuttavia, più opportunamente, il legislatore avrebbe potuto indicare specifici reati per l'accertamento e la repressione dei quali utilizzare tale strumento, analogamente a quanto dispone l'art. 226 disp. att. c.p.p. In mancanza dell'indicazione di specifiche modalità di esecuzione e di rigorosi limiti di ammissibilità, è attuale il rischio che tale attività di indagine si tramuti in uno strumento di ricerca della *notitia criminis*. Evidenti ne sono i riflessi sulla tutela della riservatezza, che, inviolabile, può essere limitata solo per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge. Ciò soprattutto considerando che, nel bilanciamento tra riservatezza e indagini penali, la prima può soccombere solo di fronte a fondate esigenze di accertamento di reati, meglio se di particolare gravità.

7.4 Acquisizione (art. 132 codice privacy*) e sequestro (art. 245* bis *c.p.p.)*

Come accennato, di assoluto interesse è il rapporto tra acquisizione dei dati relativi al traffico, disciplinata dall'art. 132 d. lgs. 196/2003, e sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni, disciplinato dall'art. 254 *bis* c.p.p.

Le due disposizioni si segnalano, infatti, per una sovrapposizione *ratione materiae*: i "dati di traffico o di ubicazione" che devono essere conservati per le finalità di cui all'art. 132 codice *privacy*, possono essere oggetto di sequestro ai sensi dell'art. 254 *bis* c.p.p.[395].

Non mancano, tuttavia, elementi di distinzione tra le due fattispecie. Innanzitutto, l'àmbito di applicazione soggettivo dell'art. 254 *bis* c.p.p. è più ampio prestandosi a ricomprendere non solo i fornitori di reti e servizi di comunicazione elettronica di cui all'art. 4 d. lgs. 259/2003 (i fornitori di servizi di telecomunicazione, ossia operatori di accesso e *Internet service providers*), bensì anche quei gestori che comunque impiegano nella loro attività imprenditoriale reti o servizi di comunicazione elettronica (fornitori di servizi informatici e telematici). Il riferimento è a istituti bancari che offrono ai propri clienti l'accesso e l'utilizzo via *Internet* dei conti correnti, alle compagnie aeree o ferroviarie che consentono prenotazioni e acquisti *online*, ad aziende che operano nel settore del commercio elettronico[396].

Inoltre, è opportuno sottolineare che i dati, sia pure di traffico o di ubicazione, che possono essere sequestrati ai sensi dell'art. 254 *bis* c.p.p. devono, secondo la previsione generale, costituire «corpo del reato o cose pertinenti al reato necessarie per l'accertamento dei fatti» (art. 253 c.p.p.); ciò che non è richiesto dall'art. 132 codice *privacy*.

Infine, è bene ricordare che l'art. 2 d. lgs. 109/2008 ha abrogato il comma 4 dell'art. 132 codice *privacy* e ha con ciò esautorato il giudice da qualsivoglia potestà

[395] L'art. 254 *bis* c.p.p. fa generico riferimento a «dati detenuti [da fornitori di servizi informatici, telematici e di telecomunicazione], compresi quelli di traffico e di ubicazione». La domanda che si pone è quali siano questi "altri dati", diversi da quelli di traffico e di ubicazione suscettibili di sequestro. Essi sono stati individuati nei dati personali e identificativi di cui all'art. 4 lett. b) e c) codice *privacy*. V. S. VENTURINI, *Sequestro probatorio*, cit., p. 138.
[396] A. MONTI, *La nuova disciplina*, cit., p. 211.

in ordine alle procedure di acquisizione dei dati di traffico ivi regolate[397]. Ne consegue che solo il pubblico ministero ha facoltà di attingere alla banca dati costituita dai gestori di servizi informatici o telematici. Al contrario l'art. 254 *bis* c.p.p. fa riferimento all'autorità giudiziaria, con ciò assegnando anche al giudice, e non solo al titolare dell'accusa, uno strumento di apprensione dei dati di traffico.

Secondo alcuni Interpreti un ulteriore elemento di distinzione tra i due strumenti investigativi risiederebbe nel fatto che solo il sequestro *ex* art. 254 *bis* c.p.p. sarebbe impugnabile dinanzi alla giurisdizione cautelare (art. 257 c.p.p.)[398]. In base ad una diversa impostazione, invece, il provvedimento di acquisizione *ex* artt. 256 c.p.p. e 132 codice *privacy* sarebbe impugnabile proprio alla luce della sua assimilazione al sequestro probatorio[399]. Pur apprezzabile, tale interpretazione si scontra con il principio di tassatività dei mezzi di impugnazione.

Gli elementi di sovrapposizione tuttavia restano. A tal proposito gli sforzi dottrinali sono stati nel senso di limitare l'applicazione dell'art. 254 *bis* c.p.p. in modo da evitare che faccia lettera morta del disposto dell'art. 132 codice *privacy*[400]. Si è suggerito di leggere l'art. 254 *bis* c.p.p. in coordinamento con l'art. 254 c.p.p. che disciplina il sequestro di corrispondenza, ciò che sarebbe imposto dall'inciso iniziale «quando dispone il sequestro». Ne conseguirebbe che le condizioni a cui può essere disposto il sequestro presso fornitori di servizi sarebbero quelle fissate dall'art. 254 c.p.p., mentre l'art. 254 *bis* c.p.p. disciplinerebbe solo le modalità con cui poi in concreto si procederà all'esecuzione del provvedimento.

7.5 La sentenza del BVerfG *sul* data retention

Come si è già anticipato, il *Bundesverfassungsgericht* ha con una storica decisione dichiarato incostituzionali, per contrasto con l'art. 10, comma 1 *GG*, i §§ 113a e 113b *TKG* e il § 100g, comma 1, primo periodo *StPO*, introdotti dal *Gesetz*

[397] Anteriormente a questo intervento, il codice *privacy* prevedeva un complesso sistema diarchico, ripartito tra pubblico ministero e giudice, in funzione del periodo temporale in relazione al quale l'acquisizione dei dati doveva retroagire (ventiquattro o quarantotto mesi per il traffico telefonico, sei o dodici mesi per quello telematico).
[398] S. ATERNO, A. CISTERNA, *Il legislatore interviene*, cit., p. 289; G. DI PAOLO, (voce) *Prova informatica*, cit., p. 24.
[399] M. DANIELE, *Caratteristiche*, cit. p. 209.
[400] Propone di attribuire all'art. 254 *bis* c.p.p. valore residuale, G. VACIAGO, *La disciplina normativa*, cit., p. 148.

zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen del 21 dicembre 2007 in attuazione della direttiva 2006/24/CE[401].

Il § 113a *TKG* obbligava i fornitori di servizi pubblici di comunicazione elettronica a conservare *tout court* per sei mesi i dati di traffico telefonico (rete fissa, mobile, *fax*, *sms*, *MMS*), *e-mail* e servizi *Internet*, comprese tutte le informazioni necessarie per risalire a chi, quando, per quanto tempo, con chi e dove aveva effettuato o tentato di effettuare la comunicazione. Non andava invece archiviato il contenuto della comunicazione e quindi nemmeno i dettagli sulle pagine *Internet* visitate dall'utente (ossia l'indirizzo *IP* di destinazione). Decorsi i sei mesi, i dati dovevano essere cancellati entro un mese.

Il § 113b TKG individuava i possibili scopi per cui potevano essere acquisiti i dati conservati ai sensi del § 113a, ossia il perseguimento dei reati, la difesa da gravi minacce alla sicurezza pubblica, l'adempimento di compiti istituzionali delle autorità di protezione della Costituzione della Federazione o di un *Land*, nonché dei servizi federali e di *intelligence*. Inoltre permetteva l'utilizzazione indiretta dei dati nella forma di una richiesta di informazioni al *service provider* per identificare l'indirizzo *IP*. Ossia, se l'autorità fosse stata già a conoscenza di un indirizzo *IP* poteva per suo tramite ottenere ulteriori informazioni sull'utente titolare dello stesso.

Infine, il § 100g, comma 1, primo periodo *StPO* disciplinava l'utilizzo diretto, e all'insaputa dell'interessato, dei dati conservati a norma del § 113a *TKG* qualora fosse necessario per la repressione di gravi reati (rinviando per la loro individuazione

[401] *BVerfG*, 2 marzo 2010, cit. Cfr., K. DE VIRES, R. BELLANOVA, P. DE HERT, *Proportionality overrides Unlimited Surveillance. The German Constitutional Court Judgment on data retention*, in *CEPS*, 2010, p. 1 ss.; C. OHLER, D. KLESCZEWSKI, *Anmerkung BVerfG 2.3.2010*, in *JZ*, 2010, p. 25 ss. Tale sentenza interviene a breve distanza da quella della Corte costituzionale della Romania (*Curtea Constituţională*, 8 ottobre 2009) e della Corte suprema amministrativa della Bulgaria (*SAC*, 11 dicembre 2008) e precede quella della Corte costituzionale della Repubblica Ceca (31 marzo 2011). Si tratta in tutti i casi di decisioni che hanno dichiarato incostituzionale la normativa interna di recepimento della direttiva 2006/24/CE. Per un'analisi della sentenza del *BVerfG* a confronto con quella della *Curtea Constituţională*, si veda R. FLOR, Data retention *e limiti al potere coercitivo dello Stato in materia penale: le sentenze del* Bundesverfassungsgericht *e della* Curtea Constituţională, in *Cass. pen.*, 2011, p. 1952 ss.; ID., *La tutela dei diritti fondamentali della persona nell'epoca di* Internet*. Le sentenze del* Bundesverfassungsgericht *e della* Curtea Constituţională *su investigazioni ad alto contenuto tecnologico e* data retention, in F. RUGGIERI, L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale*, cit., p. 32 ss.

al § 100a, comma 2 *StPO*)[402] o di reati commessi con mezzi di telecomunicazione. In realtà tale norma permetteva l'utilizzo di tutti i dati salvati dai *service providers*, anche quelli conservati per ragioni diverse (tra cui l'effettuazione di operazioni commerciali). Infatti, il legislatore non aveva distinto tra utilizzo dei dati conservati a norma del § 113a *TKG* e altri dati di traffico, permettendo l'acquisizione di tutti i dati conservati, a prescindere da una lista di reati presupposto.

Secondo il *BVerfG* tali norme rappresentano un'intromissione nella segretezza delle telecomunicazioni – *Fernmeldegeheimnis* - tutelata dall'art. 10, comma 1 *GG*. Infatti, anche se non si apprende il contenuto delle comunicazioni, tali dati permettono di ottenere informazioni sulla sfera intima di una persona e di creare profili della personalità e tracciare i movimenti degli utenti: destinatario, data, luogo, orario di una comunicazione permettono, se combinati tra loro, e se la conservazione riguarda un lasso di tempo apprezzabile, di ottenere dettagliate informazioni ad esempio sull'affiliazione politica o religiosa, sulle relazioni sociali o sulle inclinazioni personali. Tale indiscriminata conservazione ingenera nei cittadini l'impressione di vivere in una società del controllo di orwelliana memoria e comporta il rischio che vengano sottoposti ad indagine soggetti, senza che essi vi abbiano dato in alcun modo occasione e di abusi da parte delle autorità[403].

Cionondimeno, il contrasto con l'art. 10, comma 1 *GG* non è assoluto, soprattutto in considerazione dell'importanza che tali dati possono avere ai fini dello svolgimento delle indagini penali. Occorre però, nell'ambito del tradizionale *test* di proporzionalità, che vengano rispettati determinati requisiti.

Si tratta a questo punto di distinguere tra la raccolta e la conservazione da un lato e l'acquisizione dall'altro: siamo, infatti, in presenza di due distinte intromissioni nella *vita privata*[404].

Quanto alla prima, il problema principale è dato dal fatto che i dati sono conservati indiscriminatamente, quindi senza uno scopo e a prescindere dalla commissione di un reato e riguardano tutte le persone. Ciò che rende tale previsione

[402] Tale norma contiene un elenco di reati gravi per il perseguimento dei quali può essere disposta l'intercettazione di comunicazioni.
[403] La Corte precisa che il fatto che i fornitori di servizi pubblici di comunicazione elettronica siano nella maggior parte soggetti privati non può far sorgere dubbi circa l'interferenza con l'art. 10, comma 1 *GG*, poiché essi svolgono un'attività di rilevanza pubblica.
[404] J. ECKHARDT, M. SCHÜTZE, *Vorratsdatenspeicherung nach BVerfG: "Nach dem Gesetz ist vor dem Gesetz…"*, in *CR*, 2010, p. 226.

compatibile con l'art. 10, comma 1 *GG* è la decentralizzazione della conservazione. Infatti, fintantoché i dati sono conservati dai singoli fornitori di servizi di comunicazione elettronica e non direttamente dallo Stato, essi restano distinti e separati, e diminuisce il rischio di "profilazione" degli utenti. Inoltre la Corte ritiene che sei mesi non siano un periodo eccessivamente lungo, soprattutto in considerazione dell'importanza di tali dati per le indagini (proporzionalità)[405].

Per quanto riguarda l'acquisizione dei dati, essa è compatibile con l'art. 10, comma 1 *GG* solo se sono rispettati quattro requisiti: sicurezza dei dati, limitazione dell'utilizzo, trasparenza del procedimento acquisitivo, tutela giurisdizionale effettiva.

La sicurezza dei dati in realtà riguarda anche la loro conservazione. La preoccupazione della Corte deriva in questo caso dal fatto che i fornitori di servizi di comunicazione elettronica sono soggetti privati che sottostanno alle regole del mercato e alla pressione dei costi. Il rischio che per risultare competitivo risparmi proprio sulle misure di sicurezza dei dati sconsiglia di lasciare al singolo *service provider* la determinazione di tali procedure. Al contrario, il legislatore deve adottare misure tecniche uniformi e vincolanti che garantiscano *standard* elevati di sicurezza.

Questione centrale è quella degli scopi per cui i dati possono essere acquisiti ed utilizzati. La Corte censura la scelta del legislatore di non prevedere un catalogo tassativo di reati presupposto e lo invita ad introdurlo in futuro. A tal fine, seguendo l'impostazione già adottata nella sentenza sulla *Online Durchsuchung*, fa un elenco

[405] Le disposizioni sulla mera conservazione dei dati rappresentano un terreno minato per il giudizio di costituzionalità. Infatti, mentre la direttiva europea lascia agli Stati ampia discrezionalità circa l'individuazione delle modalità di accesso e utilizzazione dei dati, lo stesso non vale per gli obblighi di conservazione. Pertanto, la Corte preferisce non incentrare l'attenzione su questo aspetto, di cui sicuramente riconosce la problematicità, e non sostiene l'incompatibilità con il *Grundgesetz* della conservazione per sei mesi dei dati di traffico. Il *BverfG* si è occupato solo delle misure strettamente processuali di diritto interno, evitando così il conflitto con la Corte di Giustizia. Pertanto, l'incostituzionalità del § 113a *TKG* deriva non dall'obbligo in sé, ma dal fatto che non sono previste misure tecniche a tutela della sicurezza dei dati.
A tal proposito, giova ricordare le conclusioni presentate dall'avvocato generale, Pedro Cruz Villalòn, nelle cause riunite C-293/12, *Digital Rights Ireland Ltd contro The Minister for Communications, Marine and Natural Resources e altri* e C-594/12, *Kärntner Landesregierung Michael Seitlinger* e *Christof Tschohl*, che ha ritenuto la direttiva incompatibile con gli artt. 7 e 52, comma 1 della Carta proprio perché la durata degli obblighi di conservazione dei dati di traffico non risultava proporzionata. Egli ritiene che, pur dovendosi riconoscere al legislatore nazionale un certo margine di discrezionalità nel fissare la durata della conservazione, un periodo della durata di due anni è sicuramente eccessivo rispetto alla finalità perseguita. Infatti, più i dati sono risalenti, e quindi appartengono al passato di una persona, più la loro conservazione è percepita come invasiva della riservatezza della vita privata. *Supra*, capitolo I, par. 4.

di beni giuridici la cui messa in pericolo può giustificare l'acquisizione di dati di traffico: il corpo, la vita o la libertà di una persona, l'esistenza o la sicurezza dello Stato federale o di un *Land*. Ciò tuttavia ancora non basta a rendere l'intromissione nei diritti fondamentali proporzionata, e quindi ammissibile. Occorre altresì che vi sia un fondato sospetto di commissione di uno dei reati presupposto o che la situazione di pericolo sia concreta[406]. Infine, una volta che i dati non siano più utili per il procedimento penale, devono essere immediatamente cancellati.

Altrettanto importante è garantire la trasparenza del procedimento acquisitivo, ciò che in ultima istanza serve a rendere la misura meno invasiva della sfera privata: sapere quali dati e per quale motivo vengono acquisiti fa sicuramente diminuire la sensazione di pervasivo controllo. L'interessato va quindi informato dell'acquisizione dei suoi dati e degli scopi della stessa. Nel caso di indagini penali è ammessa un'acquisizione segreta, solo se ciò sia necessario, e previa autorizzazione del giudice. In questa ipotesi va comunque garantita una comunicazione successiva.

Infine, l'acquisizione dei dati di traffico dai *service providers* deve essere disposta dal giudice e va garantito il diritto al contraddittorio dell'interessato o già in fase acquisitiva o attraverso un procedimento successivo. La Corte ammette che il legislatore nella sua discrezionalità introduca deroghe a questo regime e quindi preveda che alcune informazioni possano essere fornite anche indipendentemente dai limiti descritti, purché ciò sia previsto per legge. Vanno poi predisposte, per il caso di violazioni, adeguate sanzioni, quali divieti di utilizzazione probatoria o il diritto al risarcimento del danno in sede civile[407].

---

[406] Qui risiede uno dei punti critici della decisione in esame. Nella famosa sentenza sul censimento – *Volkszählungsurteil* – la Corte aveva affermato che «*un obbligo di conservazione di dati personali presuppone che il legislatore indichi in maniera specifica e precisa lo scopo per cui verranno utilizzati e che tale raccolta sia adeguata e necessaria per il perseguimento di quello scopo. La raccolta di dati non ancora resi anonimi per scopi non determinati o non determinabili non sarebbe compatibile* [con il *Grundgesetz*]». Nel caso della conservazione e acquisizione dei dati di traffico, come già accennato, siamo in presenza di due attività diverse e quindi di due intromissioni nei diritti fondamentali. E la conservazione è di fatto indiscriminata. Il *BVerfG*, precisando – o superando? - la sua precedente giurisprudenza, afferma che la conservazione indiscriminata dei dati di traffico non è per ciò stesso incompatibile con il divieto di raccolta di dati senza scopo, a condizione che essi siano acquisiti e utilizzati per finalità ben precisate. Si crea così un forte collegamento tra le due attività, in forza del quale la conservazione è legittima in quanto lo Stato può ottenere quelle informazioni solo per scopi specifici e determinati. In quest'ottica si spiega perché la Corte ritenga importante assicurare la decentralizzazione della conservazione. Cfr. J. ECKHARDT, M. SCHÜTZE, *Vorratsdatenspeicherung*, cit., p. 226.

[407] Per completezza va menzionata la *dissenting opinion* del Giudice Schluckerbier, il quale ritiene la conservazione dei dati di traffico per sei mesi del tutto compatibile con l'art. 10, comma 1 *GG* poiché

In conseguenza della declaratoria di incostituzionalità delle norme impugnate, i dati di traffico fino a quel momento conservati sono stati cancellati.

Tale sentenza è particolarmente apprezzabile e si inserisce in un filone di decisioni con cui il *BVerfG* ha tracciato il difficile equilibrio tra interesse statale alla repressione – e prevenzione – dei reati e diritti fondamentali della persona[408]. La Corte costituzionale tedesca, infatti, è da tempo consapevole della particolare insidiosità delle nuove tecniche di indagine, capaci di mettere in crisi i diritti della personalità e le loro tradizionali manifestazioni[409], e cionondimeno importanti - se non addirittura imprescindibili - per le indagini.

Va segnalato, tuttavia, che a tutt'oggi la Germania è priva di una disciplina sul *data retention*, risultando così inadempiente agli obblighi comunitari, con inevitabili riflessi anche in tema di cooperazione giudiziaria[410].

---

non comporta l'acquisizione del contenuto della comunicazione. Inoltre, i dati rimangono nella disponibilità degli *Internet Service Providers*, e gli utenti possono, in forza del rapporto contrattuale che intrattengono con questi ultimi, fare affidamento sul fatto che i dati saranno trattati in maniera confidenziale e saranno protetti. Infine, il Giudice fa notare come la conservazione dei dati non sarebbe paragonabile, quanto ad intromissione nella sfera privata a misure quali le intercettazioni telefoniche e ambientali o le perquisizioni *online* e pertanto la vigente disciplina rispetterebbe il principio di proporzionalità.

[408] Il riferimento è alla sentenza sulle intercettazioni ambientali - "*Großer Lauschangriff*" – (*BVerfG*, 3 marzo 2004, *1BvR* 2378/98, *1BvR* 1024/99, *BVerfGE* 109, 279), sulla investigazione computerizzata per finalità di prevenzione di polizia – *Rasterfahndung* – (*BVerfG*, 4 aprile 2006, *1BvR* 518/02, *BVerfGE* 115, 320) e sulle perquisizioni online - *Online Durchsuchung* – (*BVerfG*, 27 febbraio 2008, cit.), tutte reperibili su *www.bundesverfassungsgericht.de*. Cfr. M. A. ZÖLLER, *Die Vorratsspeicherung von Telekommunikationsdaten*, cit., p. 40. Si veda anche R. FLOR, *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, p. 359 ss.

[409] Emblematico, come si è visto, è il caso del diritto alla garanzia della riservatezza e integrità dei sistemi informatici, che il *BVerfG* ha coniato, estrapolandolo dall'interpretazione degli artt. 2, comma 1 e 1, comma 2 *GG* perché la tutela offerta dal diritto all'autodeterminazione informativa, anch'esso espressione della dignità umana (art. 1, comma 1 *GG*) e dello sviluppo della personalità (art. 2, comma 1 *GG*), non offriva protezione adeguata di fronte alle sfide del progresso tecnologico. *Supra*, capitolo I, par. 5.1.

[410] È interessante sottolineare che l'attuale ministro della giustizia, *Sabine Leutheusser-Schnarrenberger*, faceva parte degli oltre 30.000 ricorrenti che hanno adito il *BVerfG* per ottenere la declaratoria di incostituzionalità delle norme in materia di conservazione e acquisizione dei dati di traffico. Ciò spiega, in parte, i ritardi del legislatore nel mettere a punto una nuova disciplina.

CAPITOLO III
INDAGINI INFORMATICHE NON DISCIPLINATE DALLA LEGGE

SOMMARIO: *1. Indagini informatiche non previste dalla legge: prova atipica o prova incostituzionale? 2. Localizzazione satellitare 2.1 Pedinamento satellitare e diritti fondamentali della persona 2.2 Il caso* Uzun v. Germany *deciso dalla Corte Europea dei Diritti dell'Uomo e i suoi riflessi nell'ordinamento italiano 3. Localizzazione in tempo reale del telefono cellulare 4. Perquisizioni* online *4.1 Inquadramento giuridico. L'esperienza tedesca 4.2 Inquadramento giuridico in Italia 4.3 Perquisizioni* online*: prova atipica o prova incostituzionale?*

1. Indagini informatiche non previste dalla legge: prova atipica o prova incostituzionale?

I mezzi di ricerca della prova tipici esaminati nel precedente capitolo non esauriscono il novero delle c.d. indagini informatiche. Infatti, da un lato è oggi possibile svolgere attività di indagine tradizionalmente atipiche, quali il pedinamento, tramite nuovi strumenti tecnologici, dall'altro si sono sviluppati inediti mezzi di ricerca della prova, quali l'infiltrazione in un sistema informatico, ai fini dell'installazione di un particolare *software* di indagine che permette agli investigatori di esplorare il contenuto di un *computer* e monitorarne l'uso da parte dell'utente, ogni qualvolta questi si connetta ad *Internet*.

L'indagine volta ad individuare la corretta qualificazione giuridica di tali strumenti investigativi non potrà che prendere le mosse dall'esame dei diritti fondamentali coinvolti. Ciò consentirà innanzitutto di verificare se sia possibile, e – in caso di risposta affermativa – in che termini, inquadrare i "nuovi" strumenti di acquisizione probatoria nell'ambito di istituti tipici. In secondo luogo, nel caso di esito negativo, si potrà vagliare la possibilità di considerarli mezzi di ricerca della prova atipici, tenendo a mente che il primo limite di ammissibilità di una prova «non disciplinata dalla legge» (art. 189 c.p.p.) è proprio la sua legittimità costituzionale[411].

[411] Non si dubita dell'applicabilità dell'art. 189 c.p.p anche alla fase delle indagini preliminari; come correttamente osservato in dottrina, le disposizioni generali collocate nel titolo I del libro III costituiscono un catalogo di principi guida in materia probatoria, come tali applicabili «all'intero arco del procedimento, anche in via analogica, fuorché nei casi in cui norme speciali dettate per le diverse fasi, o peculiari previsioni di legge, non le deroghino». Cfr. M. NOBILI, sub *art. 189 c.p.p.*, in AA.VV., *Commento al nuovo codice di procedura penale*, coordinato da M. CHIAVARIO, tomo II,

Dal tipo di diritto fondamentale coinvolto e dall'intensità della limitazione dipenderà poi la concreta applicabilità dell'art. 189 c.p.p.

Esemplificativa è la giurisprudenza in tema di riprese video: in mancanza di una disciplina *ad hoc*, le riprese effettuate nel domicilio sono vietate, in quanto lesive dell'art. 14 Cost.[412], mentre quelle che avvengono in "luoghi riservati", tutelati dall'art. 2 Cost., sono legittime a condizione che siano autorizzate con decreto motivato dell'autorità giudiziaria[413].

Analogamente, da tempo la giurisprudenza ricomprende nell'ambito di tutela dell'art. 15 Cost. l'acquisizione dei tabulati telefonici, ma poiché non si apprende il contenuto della comunicazione, ma solo le sue circostanze esterne, non si richiede l'applicazione degli artt. 266 ss. c.p.p., essendo sufficiente anche in questo caso un provvedimento motivato del pubblico ministero[414].

Torino, 1990, p. 387. *Contra* N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Padova, 1992, p. 213, secondo la quale da un lato il termine «assunzione» sarebbe riferibile solo alle prove e dall'altro l'art. 189 c.p.p. richiede un contraddittorio anticipato che non risulta attuabile in riferimento agli atti investigativi atipici. Proprio quest'ultima osservazione ha indotto altri a ritenere che l'art. 189 c.p.p. sia applicabile agli atti investigativi atipici per la sola parte in cui richiede che siano soddisfatti i requisiti dell'idoneità ad assicurare l'accertamento dei fatti e del divieto di pregiudizio alla libertà morale della persona. Cfr. A. LARONGA, *L'utilizzabilità probatoria del controllo a distanza eseguito con sistema satellitare* g.p.s., in *Cass. pen.*, 2002, p. 3050 ss. La giurisprudenza ammette che l'art. 189 c.p.p. sia applicabile alle indagini atipiche, in quanto «*il contraddittorio previsto dall'art. 189 c.p.p. non riguarda la ricerca della prova, ma la sua assunzione e interviene dunque* […] *quando il giudice è chiamato a decidere sull'ammissione della prova*». Così, in tema di riprese visive, Cass., Sez. un. 28 marzo 2006, n. 26795, Prisco, con nota di M. L. DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni Unite*, e di F. RUGGIERI, *Riprese visive e inammissibilità della prova*, in *Cass. pen.* 2006, p. 3937 s.; e di A. CAMON, *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento ed alcuni dubbi nuovi*, in *Riv. it. dir. e proc. pen.* 2006, p. 1550 ss.

[412] C. cost., sentenza 24 aprile 2002, n. 135, in *Giur. cost.*, 2002, p. 1062 ss., con osservazioni di F. CAPRIOLI, *Riprese visive nel domicilio e intercettazioni «per immagini»*. Va precisato, tuttavia, che la Corte costituzionale fa riferimento a riprese di comportamenti non comunicativi, mentre i comportamenti comunicativi, in quanto equiparabili alle intercettazioni ambientali, vanno sottoposti in via interpretativa alla disciplina di tale mezzo di ricerca della prova che, nel rispetto delle prescrizioni costituzionali (artt. 14 e 15 Cost.), è sottoposto a doppia riserva, di legge e di giurisdizione. Si tenga presente inoltre che, secondo l'orientamento della Corte costituzionale (sentenza 7 maggio 2008, n. 149, in *Giur. cost.*, 2008, p. 1832, con osservazioni di F. CAPRIOLI, *Nuovamente al vaglio della Corte costituzionale l'uso degli strumenti di ripresa visiva*), affinché scatti la protezione dell'art. 14 Cost., non basta che un certo comportamento venga tenuto in luoghi di privata dimora, ma occorre altresì che esso venga tenuto in condizioni tali da renderlo tendenzialmente non visibile a terzi. Per un approfondito esame di tale materia, con interessanti spunti comparatistici, si rinvia a G. DI PAOLO, "*Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Padova, 2008.

[413] Cass., sez. un., 28 marzo 2006, Prisco, cit.

[414] C. cost. 11 marzo 1993, n. 81, in *Giur. cost.*, 1993, p. 731; C. cost., n. 281 del 1998, *ivi*, 1998, p.; Cass., sez. un., 23 febbraio 2000, D'Amuri, in *Cass. pen.*, 2000, p. 2594; Cass., sez. un., 21 giugno 2000, Tammaro, *ivi*, 2000, p. 3259. Il legislatore è intervenuto nel 2003 e ha disciplinato espressamente la materia (art. 132 d. lgs. 196/2003, modificato con d.l. 27 luglio 2005, n. 144,

Qualora si dovesse concludere nel senso che le attività di indagine non disciplinate dalla legge siano in contrasto con la Costituzione, esse devono considerarsi vietate e i relativi risultati probatori inutilizzabili, secondo la nota teoria delle prove incostituzionali.

L'esistenza di tale categoria è peraltro controversa. L'origine del concetto si fa tradizionalmente risalire alla prima sentenza della Corte Costituzionale in materia di intercettazioni, dove venne espresso il principio per cui «*attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione e a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito*»[415].

A seguito di tale pronuncia, gli interpreti si sono divisi tra quanti ritenevano che il giudice penale potesse fare diretta applicazione di tale principio, escludendo dal materiale valutabile le prove raccolte in violazione delle norme costituzionali[416], e coloro che, al contrario, negavano che la norma costituzionale potesse fungere da "contenitore" di divieti probatori, e quindi operare direttamente, potendo l'ammissibilità della prova essere valutata solo alla stregua di norme processuali[417].

Successivamente, la stessa Corte Costituzionale ha preso posizione in tale *querelle*, precisando che il giudice penale, di fronte ad un procedimento probatorio che ritenga lesivo di un diritto inviolabile, deve dichiarare egli stesso l'inutilizzabilità[418]; infatti, un sistema processuale che permettesse di utilizzare prove

convertito in legge con modificazioni nella legge 31 luglio 2005, n. 155). Per un quadro completo dell'evoluzione giurisprudenziale e normativa, cfr. A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005, p. 594 ss.; F. RUGGIERI, *Divieti probatori e inutilizzabilità della disciplina delle intercettazioni telefoniche*, Milano, 2001, p. 83 ss. Cfr., *Supra*, Capitolo I, par. 1.2.

[415] C. cost., 6 aprile 1973, n. 34, in *Giur. cost.*, 1973, p. 338, con nota di V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*.

[416] G. ALLENA, *Riflessioni sul concetto di incostituzionalità della prova nel processo penale*, in *Riv. it. dir. e proc. pen*., 1989, p. 506 s.; V. GREVI, *Insegnamenti, moniti*, cit., p. 341; G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Milano, 1983, p. 137 ss.

[417] F. CORDERO, *Prove illecite,* in *Tre studi sulle prove penali*, Milano, 1963, p. 154; N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Padova, 1992, p. 204 ss.

[418] C. cost., sentenza 26 febbraio-11 marzo 1993, n. 81, in *Giur. it.* 1995, I, c. 117 s., con nota di S. DI FILIPPO, *Dati esteriori delle comunicazioni e garanzie costituzionali*; C. cost., sentenza 151 del 1993, in *Riv. pol.* 1994, p. 96 s, con nota di P. DUBOLINO, *La convalida del sequestro di polizia giudiziaria dopo la sentenza n. 151 del 1993 della Corte costituzionale*.

ottenute infrangendo le regole poste dagli artt. 13, 14 o 15 della Carta fondamentale sarebbe in conflitto con la Costituzione[419].

Con l'entrata in vigore del nuovo codice di procedura penale, e in particolare dell'art. 191 c.p.p., infatti, i termini della questione sono mutati: si è sostenuto che attraverso tale norma farebbero ingresso nel sistema processuale i divieti probatori ricavabili dalla Costituzione, poiché difficilmente potrebbe negarsi che il termine «legge» faccia riferimento anche, e soprattutto, alla legge fondamentale[420].

Con particolare riferimento al rapporto tra prova incostituzionale e prova atipica, merita di essere segnalato un recente orientamento della Cassazione, secondo cui l'attività probatoria non disciplinata dalla legge, che violi principi fondamentali, prima ancora che incostituzionale e, quindi, inutilizzabile, sarebbe inammissibile. Infatti, l'art. 189 c.p.p. presuppone logicamente la formazione lecita della prova e soltanto in questo caso la rende ammissibile, poiché non può considerarsi non vietata dalla legge la prova basata su un'attività che la legge vieta[421]. In realtà, come correttamente sostenuto, la mancata adesione alla teoria delle prove costituzionali da parte del giudice di legittimità sarebbe meramente di facciata. Infatti, la Corte pur non volendosi occupare della questione, è costretta a fare uso di tale categoria ermeneutica per trasportare il divieto costituzionale dentro al processo e farlo funzionare come presupposto negativo dell'art. 189 c.p.p.[422].

---

[419] Sarebbe quindi sufficiente una semplice operazione ermeneutica per ritenere direttamente operative tali prescrizioni. Così A. CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen.*, 1999, p. 1208.

[420] Cfr. A. CAMON, *Le riprese visive*, cit. p. 1211; S. TESORIERO, *Uno strano ordine di esibizione della corrispondenza sospeso tra sequestro ed intercettazione,* in *Cass. pen.* 2008, p. 673. In giurisprudenza si veda Cass., sez. un., 13 luglio 1998, Gallieri, in *Giust. pen.*, 1999, III, c. 614 ss., dove si afferma che l'art. 191 c.p.p. sarebbe una «*norma-valvola* [in forza della quale] *la fattispecie tipica del diritto inviolabile sarebbe in grado di esercitare un'efficacia immediata nel sistema probatorio*».

[421] Nel caso delle prove atipiche, il vaglio di ammissibilità è attività preliminare: prima dell'ammissione la prova atipica non esiste, e, se viene ritenuta inammissibile, non occorre nemmeno interrogarsi sulla sua utilizzabilità.

[422] Così, S. TESORIERO, *Uno strano ordine*, cit., p. 672. Si veda anche A. CAMON, *Le Sezioni unite sulla videoregistrazione*, cit. p. 1561. C'è anche chi ha accolto con favore l'opportuna differenziazione tra prove tipiche e prove atipiche con riguardo alla provenienza normativa del divieto: nel primo caso la fonte è il codice di procedura penale; rispetto alle prove atipiche, invece, sarà opportuno ricercare in altre parti dell'ordinamento eventuali divieti. Irrilevante è poi la circostanza che la legge impositiva del divieto possa essere non solo quella ordinaria ma anche quella costituzionale. Cfr. M. L. DI BITONTO, *Le riprese video domiciliari*, cit., p. 3937.

2. Localizzazione satellitare

Il pedinamento, classica attività atipica e informale di polizia, tradizionalmente realizzato attraverso l'annotazione manuale e la documentazione per immagini di spostamenti e contatti personali, viene oggi condotto servendosi della tecnologia, che lo ha reso contestualmente più efficace e più invasivo. È infatti possibile seguire i movimenti della persona da controllare in maniera continuativa e senza timore di perderne le tracce, né di essere scoperti. Lo stesso risultato può essere raggiunto attraverso la ricostruzione *ex post* degli spostamenti del soggetto, mediante l'acquisizione dei dati di traffico telefonico, comprensivi anche dei c.d. dati di ubicazione, o dei tabulati del *telepass*, nonché di telecamere di sorveglianza installate sulla pubblica via da enti pubblici o privati per il perseguimento dei propri fini istituzionali.

Oggetto della presente analisi sarà solo il controllo in tempo reale dei movimenti di un soggetto.

Il pedinamento c.d. "elettronico" può essere realizzato sfruttando dispositivi già in possesso del soggetto monitorato, ciò che accade nel caso in cui venga localizzato un cellulare attraverso il tracciamento in tempo reale delle celle che esso aggancia, ovvero servendosi di strumenti *ad hoc*, quale il sistema satellitare *GPS*, acronimo di *Global Positioning System*. Tale strumento permette di rilevare la posizione del soggetto, sfruttando una costellazione di satelliti artificiali in orbita[423]. Esso si compone di tre segmenti: un segmento satellitare, un segmento di controllo e un segmento utente o ricevitore. In particolare, i satelliti trasmettono costantemente un segnale radio contenente informazioni riguardanti l'ora di emissione, il codice identificativo, la posizione del satellite. Queste informazioni vengono ricevute da un apposito apparecchio di ricezione che localizza almeno quattro satelliti, calcola la distanza da ognuno di essi e tramite un algoritmo individua latitudine, longitudine ed altitudine del *tracker GPS*. Tali dati vengono quindi trasmessi al terminale – solitamente un *computer* - in possesso degli investigatori, il quale per mezzo di un

[423] Le costellazioni satellitari sfruttate a fini di localizzazione sono in realtà quattro, oltre alla *GPS*, gestita dagli Stati Uniti, si possono annoverare la russa *GLONASS*, la cinese *COMPASS* e la costruenda costellazione europea Galileo. A prescindere dai satelliti effettivamente utilizzati, è ormai invalso l'uso del termine *GPS*, dal nome della prima costellazione utilizzata. Il grado di accuratezza è molto elevato, si parla infatti di un margine di errore nell'ordine di quindici metri.

apposito *software* elabora una mappa cartografica elettronica, poi trasferita su un supporto informatico.

Il dispositivo *GPS* può essere appositamente installato sul o nel veicolo in uso al sospettato, sempre che l'automobile non ne sia già dotata (si pensi ad esempio ad alcuni sistemi di antifurto)[424], oppure si può sfruttare quello ormai presente in tutti i cellulari di nuova generazione – *smartphones.*

[424] Proprio sulla distinzione tra collocazione del dispositivo e successivo monitoraggio si basava la giurisprudenza della Suprema Corte Americana in tema di pedinamento satellitare. Infatti, per la realizzazione della prima operazione era richiesta l'emissione di un mandato, essendo in gioco un *physical trespass*, e quindi un'intromissione tipica nel diritto garantito dal IV Emendamento – che tutela contro *unreasonable searches and seizures* -, mentre la seconda non sarebbe qualificabile come *search* poiché consiste in un'attività di captazione di informazioni che vengono volontariamente esposte al pubblico. Si tratta di un'applicazione della *open fields doctrine*, teoria elaborata dalla Corte Suprema in *United States v. Hester* (*265 U.S. 57 (1924)*), secondo la quale la speciale tutela del IV Emendamento non si estende agli spazi pubblici. In forza di questa argomentazione la Corte Suprema ha negato che il tracciamento tramite *beeper*, antecedente tecnologico del *GPS*, fosse riconducibile al IV Emendamento; con un ragionamento simile a quello della giurisprudenza italiana – vedi *infra* -, essa ritiene infatti irrilevante la circostanza che le capacità percettive siano potenziate attraverso l'uso della tecnologia: l'osservazione di ciò che è in *plain view* non costituisce comunque *search* (*United States v. Knotts, 460 U.S. 276 (1983)*). Solo qualora il *beeper* sia portato all'interno di luoghi costituzionalmente protetti – in particolare della privata abitazione - e riveli, quindi, dettagli che non si sarebbero potuti captare attraverso la sorveglianza tradizionale, si ravvisa una violazione della legittima aspettativa di *privacy* del soggetto monitorato. Tale distinzione è stata espressamente superata nella recente sentenza *U.S. v Jones* (*132 S.Ct. 945 (2012)*) in cui si afferma che installazione e successivo monitoraggio si implicano a vicenda e non possono quindi essere considerate separatamente: un'invasione della proprietà oppure un'intromissione nella legittima aspettativa di *privacy* non sono da considerarsi *search* a meno che non siano effettuate per ottenere informazioni, così come l'ottenimento di informazioni non può essere considerata un'attività protetta dal IV Emendamento, se non implica una limitazione del diritto di proprietà o della *privacy*. La conseguenza è che l'installazione e successivo utilizzo di un dispositivo *GPS* per monitorare gli spostamenti di un individuo costituisce una perquisizione ai sensi del IV Emendamento, e deve quindi essere autorizzata da un mandato del giudice. La portata innovativa del caso *Jones*, tuttavia, si riduce se si considera che il *dictum* della Corte Suprema è applicabile solo a casi in cui sia necessario installare fisicamente il dispositivo *GPS*. Le ipotesi in cui, al contrario, si sfrutti un dispositivo già in dotazione dell'automobile o del cellulare del soggetto da monitorare, e si realizzi quindi un'intrusione solo "elettronica" nella proprietà o nella *privacy* dell'interessato, rimangono "disciplinate" dal precedente *case law*. Infatti, se è pur vero che con la decisione *Kyllo v. United States* (*533 U.S. 27 (2001)*) la Corte Suprema ha ricompreso nell'ambito di tutela del IV Emendamento anche l'equivalente tecnologico del *physical trespass*, va altresì sottolineato che si trattava in quel caso di un'intrusione nel domicilio, luogo che gode della massima protezione da parte della giurisprudenza. È lecito, quindi, dubitare che tale precedente sia applicabile al caso in esame poiché la Corte Suprema, come la nostra Corte di Cassazione, distingue tra domicilio, aree costituzionalmente protette e luoghi pubblici, e nella decisione *Jones* essa si limita a qualificare l'automobile quale *effect*, con ciò sostanzialmente sanzionando una violazione del diritto di proprietà, senza prendere posizione sulla questione nodale della sussistenza o meno di una ragionevole aspettativa di *privacy* anche in luoghi pubblici. Il timore è che continui a farsi applicazione della *open fields doctrine* e, quindi, a negarsi la necessità di un mandato per condurre attività di pedinamento "elettronico" nel caso in cui manchi un *physical trespass*. Verosimilmente continueranno ad applicarsi i precedenti *United States v. Knotts* e *United States v. Karo* e a ritenersi necessario un mandato solo qualora il tracciamento coinvolga il domicilio.
Per un commento della sentenza *U.S. v. Jones*, si veda anche V. FANCHIOTTI, U.S. v. Jones*: Una soluzione tradizionalista per il futuro della* privacy*?*, in *Dir. pen. proc.*, 2012, p. 381 ss.

Due sono i problemi che si sono posti con riferimento a questa particolare tecnica di indagine. Innanzitutto, quello dell'esatto inquadramento giuridico, stante la mancanza di un'espressa disciplina legislativa; inoltre, quello dell'utilizzabilità probatoria dei risultati ottenuti.

Con riferimento a quest'ultimo quesito, ci si è domandati, in particolare, se si tratti di attività irripetibile e quindi se i relativi verbali vadano inseriti nel fascicolo del dibattimento ai sensi dell'art. 431, lett. b) c.p.p. Pur nell'incertezza della nozione di atto irripetibile[425], non sembra potersi negare tale caratteristica all'attività di pedinamento, che monitora una realtà non riproducibile con le stesse modalità in un contesto spazio-temporale diverso[426].

Ulteriori interrogativi derivano dal fatto che in realtà l'attività di pedinamento non è documentata tramite verbale, bensì attraverso annotazioni o relazioni di servizio. A tal proposito si è affermato che l'art. 431, lett. b) c.p.p. accoglie una nozione sostanziale e non formale di verbale, per cui, a condizione che l'attività sia irripetibile e che l'atto di documentazione, a prescindere dal *nomen iuris*, soddisfi i requisiti di cui all'art. 136 c.p.p., esso è a buon titolo inseribile nel fascicolo del dibattimento[427].

---

[425] È sufficiente in tal sede richiamare l'orientamento delle Sezioni Unite della Cassazione, secondo cui l'irripetibilità di un atto procedimentale è riscontrabile soltanto ove si ravvisi l'esistenza di un risultato ulteriore ed estrinseco rispetto alla mera attività investigativa della polizia giudiziaria, il quale non sia più riproducibile in dibattimento se non con la perdita dell'informazione probatoria o della sua genuinità. Cass., sez. un., 17 ottobre 2006, Greco, in *Dir. pen. proc.*, 2007, p. 1155 ss., con nota di F. CERQUA, *Le Sezioni Unite fissano i criteri per stabilire quando gli atti investigativi non sono ripetibili*. Si veda *supra*, capitolo II, par. 4.1.

[426] Aderiscono a questo orientamento A. LARONGA, *L'utilizzabilità probatoria*, cit., p. 3050 ss.; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007, p. 252; P. PERETOLI, *Controllo satellitare con* GPS*: pedinamento o intercettazione?*, in *Dir pen. proc.*, 2002, p. 93; A. SCAGLIONE, *Attività atipica di polizia giudiziaria e controllo satellitare*, in *Foro it.*, 2002, III, p. 635; M. STRAMAGLIA, *Il pedinamento satellitare: ricerca ed uso di una prova "atipica"*, in *Dir. pen. proc.*, 2011, p. 213 ss. In giurisprudenza, si veda Cass., sez. VI, 8 giugno 2004, Aiuto, in *C.E.D. Cass.*, n. 230375 che considera irripetibili «*tutti gli atti che non possono essere rinnovati nella loro ontologica essenza, pur se rievocabili, tramite lettura del verbale, in un'occasione cronologicamente successiva*». Si tratta delle stesse conclusioni raggiunte in tema di videoriprese eseguite in ambito pubblico. Per tale rilievo si veda G. DI PAOLO, *"Tecnologie del controllo"*, cit., p. 252, a cui si rinvia anche per l'esaustivo esame della tematica delle videoriprese. Peraltro, va dato atto di una diversa impostazione della giurisprudenza, la quale applica la stessa regola già utilizzata per il pedinamento classico, ossia quella dell'escussione dibattimentale degli agenti di polizia giudiziaria che hanno effettuato l'attività di indagine. Cfr. Cass., sez. VI, 11 aprile 2008, Sitzia e altri, in *C.E.D. Cass.*, n. 239635.

[427] A. LARONGA, *L'utilizzabilità probatoria*, cit.; M. STRAMAGLIA, *Il pedinamento satellitare*, cit. Cfr. anche Cass., sez. un., Greco, cit., laddove si afferma che «*le relazioni di servizio sono acquisite al fascicolo del dibattimento a condizione che siano redatte nella forma del verbale o, benché redatte*

Infine, il testuale riferimento al verbale, non sembra essere di ostacolo all'inserimento nel fascicolo per il dibattimento anche dei supporti informatici (*DVD*, *CD*, *etc.*) su cui sono stati registrati i dati relativi al pedinamento. Infatti, essi sembrano ascrivibili alla categoria delle riproduzioni audiovisive che, ai sensi dell'art. 134, comma 4 c.p.p. possono essere aggiunte al verbale, quando assolutamente indispensabili[428].

2.1 Pedinamento satellitare e diritti fondamentali della persona

Le difficoltà di inquadramento giuridico derivano, come accennato, dalla mancanza di una disciplina espressa di tale particolare mezzo di ricerca della prova. Esclusa l'applicabilità in via interpretativa delle disposizioni riguardanti attività investigative nominate[429], occorre quindi verificare se essa possa considerarsi un'attività atipica, senza dimenticare che primo requisito per far ricorso a tale categoria è la legittimità della prova che si intenda assumere, «*non potendo considerarsi non disciplinata dalla legge, una prova che la legge vieta*»[430]. E tale legittimità incontra, come primo e basilare metro di valutazione, le direttrici iscritte nella Carta fondamentale.

Diverse le soluzioni date da giurisprudenza e dottrina.

---

nella forma dell'annotazione, rechino la sottoscrizione del pubblico ufficiale redigente e non lascino incertezza assoluta sulle persone intervenute».

[428] Infatti, i supporti informatici costituiscono parte integrante dei verbali che di regola non riportano l'intero tracciato degli spostamenti. Cfr. S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. e proc. pen.*, 2012, p. 580 ss.

[429] Peraltro non è mancato chi ha proposto di applicare la disciplina delle intercettazioni, sul presupposto di un'analoga intrusione nel diritto alla riservatezza. Cfr. L. G. VELANI, *Nuove tecnologie e prova penale: il sistema di individuazione satellitare* g.p.s., in *Giur. it.*, 2003, p. 2375 ss. Cfr. anche D. IACOBACCI, *Sulla necessità di riformare la disciplina delle intercettazioni prendendo le mosse dalle esitazioni applicative già note*, in *Giust. pen.*, III, 2011, c. 365 ss. Seppur si tratti di sforzo apprezzabile e sintomatico della comprensione della maggior intrusività del pedinamento satellitare rispetto a quello classico, non siamo di fronte ad una «*comunicazione riservata tra due o più persone*», che secondo la giurisprudenza costituisce oggetto dell'intercettazione. Ciò è confermato dal *leading case* della Cassazione in materia di pedinamento satellitare (Cass., Sez. V, 27 febbraio 2002, Bresciani e altri, in *Cass.pen.*, 2002, p. 3049), ove si afferma che «*il concetto di intercettazione, pur mai esplicitamente definito dal legislatore, è relativo ad un'attività di ascolto (o lettura) e captazione di comunicazioni tra due o più persone. Consiste, in un certo senso, nel sequestro di un bene immateriale: il contenuto di una comunicazione. Ad esso rimane estranea l'attività di indagine volta a seguire i movimenti sul territorio di un soggetto, a localizzarlo e dunque a controllare – a distanza – non il flusso delle comunicazioni che lo stesso invia e riceve, ma la sua presenza in un determinato luogo in un certo momento, nonché dell'itinerario seguito, degli incontri avuti*».

[430] Cass., sez. un., 28 marzo 2006, Prisco, cit.

La Corte di Cassazione nega esplicitamente che l'attività diretta a localizzare e monitorare gli spostamenti di un soggetto sul territorio realizzi una compressione del diritto alla libertà e segretezza delle comunicazioni di cui all'art. 15 Cost., e che si possa applicare in via analogica la disciplina delle intercettazioni. Esclusa ogni interferenza con diritti costituzionali, considera tale attività una «*modalità tecnicamente caratterizzata di pedinamento*», come tale rientrante nell'ordinaria attività di controllo e accertamento demandata alla polizia giudiziaria dagli artt. 55, 347 e 370 c.p.p., senza necessità di un provvedimento motivato dell'autorità giudiziaria[431]. Si tratterebbe di un mezzo di ricerca della prova c.d. atipico o innominato, i cui risultati probatori sarebbero ammissibili alle condizioni stabilite dall'art. 189 c.p.p. Non si dubita, infatti, né della sua idoneità all'accertamento[432], né dell'assenza di un pregiudizio alla libertà morale, stante l'inconsapevolezza della persona monitorata[433].

Quest'ultima affermazione non può essere condivisa; infatti, come acutamente osservato dalla dottrina nordamericana, anche la sola idea di poter essere sottoposto a continua sorveglianza induce nell'individuo cambiamenti nello stile di vita, influisce sulla sua libertà di scelta e di autodeterminazione (c.d. effetto *Panopticon*)[434].

---

[431] In tal senso da ultimo, Cass., sez. I, 10 gennaio 2012, n. 14529, *inedita*. Conformi, Cass., sez. V, 10 marzo 2010, Z.B., in *Dir. pen. proc.*, 2010, p. 1464; Cass., sez. I, 7 gennaio 2010, Congia e altri, in *C.E.D. Cass.*, n. 246774; Cass., sez. VI, 11 aprile 2008, Sitzia e altri, cit.; Cass., sez. IV, 29 gennaio 2007, Navarro, in *Cass. pen.*, 2008, p. 1137; Cass., sez. IV, 28 gennaio 2007, Bresin, in *C.E.D. Cass*., n. 238679; Cass., sez. V, 7 maggio 2004, Massa, in *Cass. pen.*, 2005, p. 3036; Cass., sez. V, Bresciani e altri, cit., con nota di A. LARONGA, *L'inutilizzabilità probatoria*, cit.

[432] Afferma S. SIGNORATO, *La localizzazione satellitare*, cit., che l'astratta idoneità accertativa della localizzazione satellitare è già stata ampiamente dimostrata dalla scienza, secondo la quale il margine di errore sarebbe assai ridotto. Quanto alla idoneità in concreto, l'Autrice sostiene che sarà sufficiente verificare che non siano stati utilizzati dai criminali dispositivi in grado di compromettere il funzionamento del *tracker GPS*. Il riferimento è al c.d. *GNSS spoofing*, che è in grado di influenzare l'attività del GPS inducendolo ad elaborare dati di ubicazione delle coordinate errati e perciò inattendibili.

[433] Tale orientamento è condiviso anche da parte della dottrina. Cfr. A. LARONGA, *L'utilizzabilità probatoria*, cit., p. 3059 ss.; C. MARINELLI, *Intercettazioni processuali*, cit., p. 252 ss.; P. PERETOLI, *Controllo satellitare*, cit., p. 99 ss.; A. SCAGLIONE, *Attività atipica*, cit., p. 635 ss.

[434] Il riferimento è alla metafora del *Panopticon* di Jeremy Bentham, una prigione costruita in modo tale che ogni prigioniero fosse sempre visibile alle guardie, ovunque si trovasse. Bentham dimostrò che la semplice idea di essere costantemente sorvegliati aveva lo stesso effetto sui prigionieri che tenerli incatenati all'interno della loro cella. Cfr. D. J. GLANCY, *Privacy on the Open Road*, *30 Ohio N. U. L. Rev. 295 (329)*, in particolare, p. 320; J. H. REMAIN, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, in *11 Santa Clara Computer & High Tech. L. J. 27 (1995)*; C. SLOBOGIN, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonimity*, in *72 Miss. L. J. 213 (202)*, p. 240, il quale

Inoltre, seppur si condivide l'affermazione per cui il pedinamento "elettronico" non interferisce con la libertà e segretezza delle comunicazioni, l'art. 15 Cost. non esaurisce il novero dei diritti fondamentali con cui tale attività d'indagine potrebbe interferire.

Diverse le ipotesi prospettate dalla dottrina. Innanzitutto, si è ritenuto che l'automobile, in quanto ambito spaziale isolato dall'esterno e destinato allo svolgimento della vita privata, sia un luogo meritevole di protezione costituzionale. Se è vero che la giurisprudenza ne esclude il carattere "domiciliare" e quindi nega il coinvolgimento dell'art. 14 Cost. [435], è altresì vero che essa ha elaborato la categoria dei "luoghi di privata dimora diversi dal domicilio", tutelati dall'art. 2 Cost.[436]. L'inquadramento dell'automobile all'interno di quest'ultima categoria comporterebbe la necessità che il pedinamento "elettronico" venga autorizzato quantomeno da un provvedimento del pubblico ministero[437].

Inoltre, si è sottolineato come il pedinamento satellitare, fungendo da remora a certi spostamenti, sia in grado di comprimere la libertà di circolazione di cui all'art. 16 Cost., intesa come comprensiva del "diritto a non essere localizzati". Poiché la

---

teorizza quindi l'esistenza di un *right to anonimity*, inteso come diritto costituzionalmente garantito «*to be free from intensive government scrutiny even in public, absent suspicious conduct*». In Italia per simili rilievi si veda G. DI PAOLO, *Tecnologie*, cit., p. 268, secondo la quale il controllo sistematico sugli spostamenti delle persone incide su libertà fondamentali proiettate pubblicamente: libertà di riunione funzionale all'esercizio della libertà di opinione, delle libertà politiche, della libertà di culto, della libertà personale. Non si possono invece condividere le affermazioni di chi sostiene che l'indagine satellitare, sebbene più precisa ed efficace, sarebbe comunque meno invasiva del pedinamento tradizionale, tramite cui si possono apprendere dettagli ulteriori, quali le persone incontrate o i luoghi frequentati, mentre il *tracking* GPS permetterebbe «di individuare esclusivamente - e "asetticamente" - il percorso seguito dall'autovettura monitorata». In questi termini, M. STRAMAGLIA, *Il pedinamento satellitare*, cit., p. 224. V. anche S. SIGNORATO, *La localizzazione satellitare*, cit., p. 589. Tale impostazione omette di considerare che l'innovazione tecnologica ha comportato un mutamento non solo quantitativo, ma anche qualitativo dell'attività di indagine. Infatti, è oggi possibile raccogliere, conservare, incrociare un'enorme quantità di dati. Così, G. DI PAOLO, (voce) *Prova informatica (diritto processuale penale)*, in *Enc. dir.,* Annali VI*,* Milano, 2013, p. 751.

[435] Cfr. *supra*, capitolo I, par. 1.1. Parte della dottrina, come si è visto, ritiene di poter qualificare l'automobile come domicilio, ossia come «spazio isolato dall'ambiente esterno, […] adibito allo svolgimento degli atti della vita privata e dal quale il soggetto o i soggetti titolari abbiano inteso normalmente escludere la presenza di terzi». Così, G. BORRELLI, *Riprese filmate nel bagno di un pubblico esercizio e garanzie costituzionali*, in *Cass. pen.*, 2001, p. 2453. Sulla base di questo presupposto si afferma quindi che la localizzazione satellitare viola l'art. 14 Cost. tutte le volte in cui l'intrusione nell'automobile sia necessaria per installare il dispositivo. Cfr. A. LARONGA, *L'utilizzabilità probatoria*, cit., p. 3056; A. SCAGLIONE, *Attività atipica*, cit., p. 635. Si tratta di un ragionamento simile a quello fatto dalla Corte Suprema Americana nella sentenza *Jones*, cit.

[436] Tale categoria è stata elaborata, con riferimento alle videoriprese da Cass., sez. un., 28 marzo 2006, Prisco, cit.

[437] Così, G. DI PAOLO, *Tecnologie*, cit., p. 256.

riserva di legge prevista da tale norma non può dirsi sicuramente soddisfatta dalla generica previsione di un'attività d'indagine atipica, risultante dall'interpretazione degli artt. 55, 347, 348, 370 e 189 c.p.p., in attesa dell'auspicato intervento del legislatore, si è suggerito che essa sia riempita attraverso il rinvio alle norme dettate dal codice della *privacy* per l'acquisizione al procedimento penale dei tabulati telefonici, i quali comprendono anche i dati di ubicazione[438].

Infine, si è sostenuto che l'attività d'indagine in esame incida sulla libertà personale tutelata dall'art. 13 Cost., intesa anche quale libertà morale, e che conseguentemente eventuali limitazioni della stessa possano avvenire solo «per atto motivato dell'autorità giudiziaria e nei soli casi e modi previsti dalla legge»; la mancanza di una specifica disciplina renderebbe quindi incostituzionale il pedinamento "elettronico", e imporrebbe al giudice, secondo l'insegnamento ormai consolidato della Corte costituzionale, di dichiarare inutilizzabili i relativi risultati probatori[439].

Nell'attuale sistema multilivello di tutela dei diritti fondamentali, l'indagine volta ad individuare i limiti dell'attività di pedinamento satellitare non può, tuttavia, arrestarsi ai diritti costituzionali in senso stretto, ma deve necessariamente andare oltre i confini nazionali.

2.2 Il caso Uzun v. Germany *deciso dalla Corte Europea dei Diritti dell'Uomo e i suoi riflessi nell'ordinamento italiano*

Ulteriori spunti di riflessione derivano, infatti, da una recente sentenza della Corte Europea dei Diritti dell'Uomo, che ha dichiarato che l'utilizzo a fini investigativi del sistema satellitare *GPS* interferisce con la vita privata tutelata dall'art. 8 CEDU[440]. In particolare, i Giudici di Strasburgo hanno riconosciuto che

[438] Così A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. e proc. pen.*, 2005, p. 633.
[439] In questi termini, L. FILIPPI, *Il* GPS *è una prova incostituzionale? Domanda provocatoria, ma non troppo, dopo la sentenza* Jones *della Corte Suprema* U.S.A., in *Arch. pen.*, 2012, n. 1. Si veda, *supra*, par. 1.3.
[440] Corte Europea dei Diritti dell'Uomo, *Uzun v. Germany*, 2 settembre 2010, ric. n. 35623/05. Il caso trae origine dal ricorso presentato da Bernard Uzun, cittadino tedesco, sospettato di aver partecipato a tentati omicidi e attentati terroristici organizzati dalla cellula terroristica denominata *Antiimperialistische Zelle*, un movimento terrorista di estrema sinistra che aveva come obiettivo la lotta armata perseguita fino al 1992 dalla *Rote Armee Fraktion*. Uzun era stato sottoposto a partire dal

esiste una sfera privata meritevole di protezione anche nella vita pubblica e di relazione; infatti, l'art. 8 CEDU tutela non solo il diritto all'identità e allo sviluppo della personalità, ma altresì il diritto di stabilire e sviluppare relazioni umane[441]. Ne segue che il c.d. pedinamento "elettronico", come le altre misure che interferiscono con l'esercizio di tale diritto, deve essere previsto dalla legge e costituire «una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la sicurezza pubblica, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute della morale, o per la protezione dei diritti e delle libertà degli altri» (art. 8, comma 2 CEDU).

La Corte, tuttavia, riconosce che l'interferenza con la vita privata cui dà vita il monitoraggio tramite *GPS* è minore rispetto a quella determinata da altre tecniche di sorveglianza visiva o acustica, le quali rivelano più informazioni relative al comportamento, alle opinioni e ai sentimenti della persona controllata, e quindi ammette che i requisiti che la legge nazionale[442] deve avere per essere considerata rispettosa dell'art. 8 CEDU siano più ampi di quelli previsti per le norme che disciplinano le intercettazioni. Tale "legge" deve garantire un'adeguata protezione da interferenze arbitrarie con la vita privata ed essere chiara circa i suoi presupposti applicativi; essa deve indicare la natura, lo scopo, la durata della misura e i motivi per cui può essere adottata, individuare l'autorità competente ad autorizzare,

---

1993 a osservazione tramite videoriprese, intercettazioni e controllo della corrispondenza; nel 1995 era stato installato un trasmettitore sulla macchina di uno dei suoi complici. A seguito della scoperta e distruzione di tale trasmettitore da parte di Uzun e del complice, la polizia federale aveva installato un *tracker GPS* sull'autovettura del ricorrente. La Corte d'Appello di *Düsseldorf* aveva condannato Uzun e rigettato l'eccezione di inutilizzabilità delle prove ottenute attraverso il pedinamento satellitare sostenendo che non fosse necessaria una specifica autorizzazione per tale ultima attività di indagine in quanto si trattava di una forma di sorveglianza che andava ad aggiungersi alle altre già autorizzate. Dopo essere ricorso sia al *Bundesgerichtshof* che al *Bundesverfassungsgericht*, Uzun ha quindi adito la Corte EDU lamentando la violazione del diritto al rispetto della vita privata tutelato dall'art. 8 CEDU e del diritto ad un processo equo *ex* art. 61, § 1 CEDU.

[441] Già in passato la Corte di Strasburgo aveva ammesso che la raccolta e conservazione sistematica di dati interferisse con la vita privata anche se l'attività oggetto di controllo veniva svolta in pubblico e non aveva natura intima. Cfr. Corte Europea dei Diritti dell'Uomo, *Peck v. United Kingdom*, 23 gennaio 2003, ric. n. 44647/98, §§ 57-59; Corte Europea dei Diritti dell'Uomo, *P.G. and J.H. v. United Kingdom*, 25 settembre 2001, ric. n. 44787/98, §§ 56-57; Corte Europea dei Diritti dell'Uomo, *Perry v. United Kingdom*, 17 luglio 2003, ric. n. 63737/00, §§ 36-38; *Rotaru v. Romania*, 4 maggio 2000, ric. n. 28341/95, §§ 43-44. V. anche S. ALLEGREZZA, *Giustizia penale e diritto all'autodeterminazione dei dati personali nella regione Europa*, in D. NEGRI (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 69 ss.

[442] Si tenga presente che il termine «legge» comprende non solo la legge formale, ma anche la normativa ad essa subordinata e il diritto di creazione giurisprudenziale.

condurre, nonché supervisionare la sorveglianza, e contemplare dei rimedi per l'interessato[443]. Alla luce di tali considerazioni, la Corte ritiene il sistema tedesco rispettoso dell'art. 8 CEDU[444].

La sentenza in parola è particolarmente apprezzabile innanzitutto in quanto supera l'idea che la segretezza sia un presupposto della tutela della *privacy*[445]; inoltre perché riconosce che ci possono essere diversi gradi di limitazione della vita privata, in ragione del tipo di informazioni che si apprendono e del luogo in cui vengono captate, con la conseguenza che la necessaria disciplina delle diverse tecnologie del controllo può, anzi deve, essere differenziata quanto a presupposti applicativi e autorità competente ad adottarle[446].

Pur trattandosi di una sentenza riguardante un caso tedesco, essa ha riflessi importanti anche nel nostro ordinamento.

Infatti, secondo l'insegnamento della Corte costituzionale, i diritti fondamentali riconosciuti dalla CEDU, così come interpretati dalla Corte di Strasburgo, integrano quali "norme interposte" il parametro costituzionale espresso dall'art. 117, comma 1 Cost., nella parte in cui impone la conformazione della legislazione interna ai vincoli derivanti dagli ordinamenti internazionali, e da questo ripetono il loro rango all'interno del sistema delle fonti[447].

---

[443] La Corte specifica che, poiché l'interferenza con la vita privata è minore di quella causata dalle intercettazioni, sarebbe sufficiente anche un controllo giudiziale *ex post*.

[444] La misura era stata adottata ai sensi del *§ 100c, Abs. 1, n. 2(b) StPO*, il quale ammette la possibilità di adottare all'insaputa dell'interessato altre - rispetto a quelle tipizzate - tecniche di sorveglianza, nel caso in cui le indagini riguardino reati di particolare gravità e strumenti diversi si rivelino inefficaci. Questa la norma oggetto del sindacato della Corte di Strasburgo. Si segnala, tuttavia, che nel 2000 è stato introdotto nel codice di procedura penale tedesco il *§ 163f*, il quale espressamente disciplina la sorveglianza a lungo termine (oltre ventiquattro ore continuative) di persona sospettata di aver commesso un reato, prevedendo che tale misura possa essere adottata solo nel caso in cui si stia procedendo per reati di particolare gravità e se l'utilizzo di altri mezzi di indagine abbia poche prospettive di successo. Competente ad adottare la misura è il pubblico ministero se la durata è inferiore ad un mese; oltre tale termine, occorre un provvedimento del giudice.

[445] Analoga consapevolezza si percepisce nella *concurring opinion* della giudice Sotomayor nella sentenza *U.S. v. Jones*, cit., laddove si afferma che il progresso tecnologico impone un ripensamento e un adeguamento alla contemporaneità delle garanzie offerte dal IV Emendamento: la «*secrecy*» non andrebbe intesa come «*prerequisite for privacy*», e all'individuo andrebbe accordata una *reasonable expectation of privacy* rispetto alle informazioni volontariamente svelate al pubblico.

[446] Particolarmente interessante sotto questo profilo è il parallelo che la Corte fa con la disciplina delle intercettazioni. Cfr. §§ 65, 66 della sentenza.

[447] C. cost., 24 ottobre 2007, n. 348, in *Giur. cost.*, 2007, p. 3475 ss., con nota di C. PINELLI, *Sul trattamento giurisdizionale della CEDU e delle leggi con essa confliggenti*; C. cost., 24 ottobre 2007, n. 349, *ivi*, 2007, p. 3535 ss., con nota di M. CARTABIA, *Le sentenze "gemelle": diritti fondamentali, fonti, giudici*. Precisano che norme costituzionali e norme convenzionali danno vita ad un sistema integrato di tutela dei diritti fondamentali, il quale mira alla massima espansione delle garanzie, C.

Da ciò derivano due conseguenze: innanzitutto, l'impossibilità per la nostra giurisprudenza di ulteriormente negare che simile attività d'indagine interferisca con diritti fondamentali (*rectius*: costituzionali) [448]; inoltre, la necessità che il pedinamento "elettronico" sia previsto dalla legge e sia necessario per perseguire uno o più degli scopi legittimi indicati dall'art. 8 CEDU.

In termini generali, affinché un'attività d'indagine sia considerata «prevista dalla legge», occorre che essa abbia una base nel diritto interno – di creazione legislativa o giurisprudenziale - sia conoscibile dall'interessato e, soprattutto, che questi sia in grado di prevedere le conseguenze derivanti dall'applicazione della misura nei suoi confronti (*foreseeability*)[449]. Con particolare riferimento all'uso del *GPS* per monitorare gli spostamenti di un soggetto, la Corte Europea dei Diritti dell'Uomo, come si è visto, ha avuto modo di precisare che l'art. 8 è rispettato se la «legge» indica la natura, lo scopo, la durata della misura e i motivi per cui può essere adottata, individua l'autorità competente ad autorizzare, condurre, nonché supervisionare la sorveglianza e prevede dei rimedi per l'interessato.

Tali parametri non paiono rispettati dalla disciplina derivante dall'interpretazione degli artt. 55, 347, 348, 370 e 189 c.p.p., che definisce un'attività d'indagine atipica, condotta dalla polizia giudiziaria senza bisogno di alcun provvedimento autorizzativo; il diritto vivente contrasta quindi con gli artt. 8 CEDU e 117 Cost.

Ciò, tuttavia, ancora non autorizza i giudici a ritenere inutilizzabili, in quanto derivanti da attività d'indagine incostituzionale, i risultati ottenuti a seguito di tracciamento tramite *GPS*. Infatti, secondo la recente giurisprudenza della Corte costituzionale, il diritto convenzionale, a differenza di quello dell'Unione europea,

---

cost., 26 novembre 2009, n. 311, *ivi*, 2009, p. 4657 ss., con nota di M. MASSA, *La "sostanza" della giurisprudenza europea sulle leggi retroattive* e C. cost. 4 dicembre 2009, n. 317, *ivi*, 2009, p. 4747 ss., con nota di G. UBERTIS, *Sistema multilivello dei diritti fondamentali e prospettiva abolizionista del processo contumaciale*. Cfr. *Supra*, capitolo I, par. 3.1.

[448] Già parte della dottrina aveva affermato che il pedinamento satellitare interferisse con il diritto alla riservatezza. Cfr. D. GENTILE, *Tracking satellitare mediante GPS: attività atipica di indagine o intercettazione di dati?*, in *Dir. pen. proc.*, 2010, p. 1472 ss.; P. PERETOLI, *Controllo satellitare*, cit., p. 96 ss.; L. G. VELANI, *Nuove tecnologie*, cit., p. 2373 ss. Per le considerazioni in merito alla tutela multilivello del diritto alla riservatezza, si rinvia a quanto detto *supra*, capitolo I.

[449] Per quanto riguarda attività d'indagine attuate all'insaputa dell'interessato, tra cui rientra anche il pedinamento "elettronico", il requisito della prevedibilità è rispettato se la legge è sufficientemente chiara da permettere ai cittadini di sapere in quali casi e a quali condizioni la misura può essere adottata nei loro confronti.

non ha effetto diretto nel nostro ordinamento, per cui in caso di contrasto tra una norma interna e una norma CEDU, il giudice deve innanzitutto verificare la praticabilità di un'interpretazione del diritto interno conforme alla Convenzione, e solo in caso di esito negativo, essendo impossibilitato a risolvere il conflitto semplicemente non applicando la norma interna contrastante, sollevare questione di legittimità costituzionale[450].

Contrariamente a quanto ritenuto dalla giurisprudenza di legittimità, non costituisce interpretazione conforme alla Convenzione l'applicazione ad attività d'indagine non tipizzate dal legislatore di quel "livello minimo di garanzie", rappresentato da un provvedimento motivato dell'autorità giudiziaria. Tale orientamento è stato seguito in materia di acquisizione dei tabulati telefonici[451], di videoriprese eseguite in luoghi riservati diversi dal domicilio[452], e infine di registrazioni fonografiche eseguite da uno degli interlocutori con strumenti di captazione forniti dalla polizia giudiziaria[453], e muove dall'assunto che in questi casi il grado di intrusione nella sfera privata sarebbe inferiore rispetto a quello causato dallo strumento tipico, ossia le intercettazioni, e giustificherebbe quindi un livello di garanzia minore, soddisfatto da un decreto motivato del pubblico ministero.

Simile operazione ermeneutica, se adottata con riferimento al pedinamento "elettronico", non sarebbe comunque sufficiente ad evitare il sindacato della Corte costituzionale. Infatti, l'art. 8 CEDU richiede che il diritto nazionale – non necessariamente di fonte legislativa, ma anche giurisprudenziale purché si tratti di un orientamento costante e pacifico che dia quindi vita ad una disciplina conoscibile e prevedibile - indichi non solo l'autorità competente, ma anche la natura, lo scopo, la

[450] C. cost., 11 marzo 2011, n. 80, in *Giur. cost.*, 2011, p. 1224 ss. Nessuna diversa conclusione può trarsi, ad avviso della Corte, dalla prevista adesione dell'Unione europea alla CEDU, che avrebbe l'effetto di attribuire a tale Convenzione lo stesso valore giuridico dei Trattati (art. 6 TFUE), innanzitutto perché essa non è ancora avvenuta, inoltre, poiché in ogni caso l'applicazione diretta dei principi generali dell'Unione europea, di cui a seguito dell'adesione anche la CEDU farà parte, rimane comunque limitata alle materie di competenza dell'Unione. Cfr., *supra*, capitolo I, par. 3.1.

[451] Cass., sez. un., 23 febbraio 2000, D'Amuri, in *Giur. it.*, 2001, p. 1707 ss.

[452] Cass., sez. un., 28 marzo 2006, Prisco, cit.

[453] Cass., sez. IV, 7 aprile 2010, Angelini, in *C.E.D. Cass.*, n. 247384. In tale pronuncia la Cassazione afferma espressamente che «*il provvedimento motivato dell'autorità giudiziaria, sia esso giudice o pubblico ministero, è altresì idoneo a garantire il rispetto dell'art. 8 della CEDU, nella interpretazione che ne è stata data dalla Corte Europea dei Diritti dell'Uomo, offrendo un'adeguata tutela contro le ingerenze arbitrarie dei pubblici poteri nella vita privata*». Cfr. il commento di P. GAETA, *Per utilizzare registrazioni fra presenti fatte dalla Pg è sufficiente un decreto del pubblico ministero*, in *Guida dir.*, 2010, p. 75 ss.

durata della misura e i motivi per cui può essere adottata, oltre ai rimedi per l'interessato.

Nell'attesa di un non più rinviabile intervento del legislatore[454], l'unica strada praticabile è quindi quella di sollevare questione di legittimità costituzionale, per contrasto con gli artt. 8 CEDU e 117 Cost., del diritto vivente, ossia di quell'interpretazione giurisprudenziale che, sulla base degli artt. 55, 347, 370 e 189 c.p.p., considera il pedinamento "elettronico" un mezzo atipico di ricerca della prova, lasciato all'iniziativa della polizia giudiziaria[455].

3. Localizzazione in tempo reale del telefono cellulare

Come si è accennato, il monitoraggio in tempo reale degli spostamenti di un soggetto sul territorio può essere realizzato anche mediante acquisizione dei dati di ubicazione del telefono cellulare. Ciò è possibile a condizione che tale dispositivo sia acceso, anche a prescindere dal fatto che venga utilizzato per effettuare o ricevere una telefonata[456]. Infatti, il codice *privacy* (artt. 126 e 127) ammette il trattamento dei dati di ubicazione, anche se diversi dai dati di traffico[457].

L'inquadramento giuridico dell'attività volta al tracciamento dei soli dati di ubicazione è problematico. Non pare potersi fare diretta applicazione dell'art. 132

[454] Non solo la Germania, ma anche alcuni Stati degli USA (California, Hawaii, Oregon, Pennsylvania, Tennessee, Texas, Utah,) e il Canada (Sezione 492.1 del *Criminal Code*, introdotta nel 1993) si sono dotati di una specifica disciplina riguradante il pedinamento "elettronico" tramite *GPS*, la quale individua i presupposti, la durata e i motivi per cui può essere adottata simile misura, nonché l'autorità competente ad autorizzarla. Cfr. G. DI PAOLO, *Judicial investigations and gathering of evidence in a digital online context*, in *IRPL*, 2009, p. 226 ss. e D. J. GLANCY, *Privacy*, cit., p. 351.

[455] Volendo si veda già, F. IOVENE, *Pedinamento satellitare e diritti fondamentali della persona*, in *Cass. pen*., 2012, p. 3556 ss.

[456] Qualora i dati di ubicazione siano relativi ad una telefonata, essi saranno qualificabili come «dati relativi al traffico telefonico». In materia di acquisizione dei dati esteriori delle comunicazioni tradizionalmente si distingue tra acquisizione – *ex post* - dei tabulati telefonici e "tracciamento dell'utenza" – in tempo reale -. Nel primo caso l'acquisizione avviene ai sensi dell'art. 132 codice *privacy*. Quanto alla seconda ipotesi, in mancanza di una disciplina espressa, si è sostenuta l'applicazione dei principi elaborati dalla giurisprudenza della Corte costituzionale (sentenze 81/1993 e 281/1998) e dalle Sezioni Unite (Cass, sez. un., D'Amuri, cit. e Cass., sez. un., 21 giugno 2000, Tammaro, in *Cass. pen.*, 2000, p. 3259) in tema di tabulati telefonici, e quindi il monitoraggio sarebbe lecito solo in presenza di un decreto autorizzativo dell'autorità giudiziaria. Cfr. G. DI PAOLO, *Tecnologie*, cit., p. 259.

[457] Cfr. A. CAMON, *L'acquisizione dei dati*, cit., p. 631-632; G. DI PAOLO, *Tecnologie*, cit., p. 260.

codice *privacy* che fa riferimento a dati preesistenti[458], né della disciplina di cui agli artt. 266 ss. c.p.p. in quanto, innanzitutto non si apprende il contenuto di una comunicazione, in secondo luogo i dati di ubicazione sono generati e acquisiti a prescindere da una comunicazione in corso. Questo peraltro non significa che tali dati siano acquisibili dalla polizia giudiziaria di propria iniziativa.

Valgono le riflessioni in tema di diritti fondamentali svolte a proposito del pedinamento satellitare. Inoltre, occorre in questo caso prendere in considerazione un profilo di criticità ulteriore.

Infatti, i dati di ubicazione sono *ex ante* impossibili da distinguere dai dati di traffico, non potendo sapere gli inquirenti quando il telefono posto sotto controllo sarà utilizzato per effettuare o ricevere telefonate. Pertanto di norma il tracciamento del cellulare comporterà l'acquisizione di dati di natura mista. Ciò che ha indotto parte della dottrina a ritenere «ragionevole che il regime di garanzia previsto per il tracciamento delle comunicazioni telefoniche vada esteso *tout court* ad ogni ipotesi di monitoraggio dinamico sul posizionamento del telefono cellulare»[459].

Tuttavia, non si può dimenticare che il tracciamento del cellulare presenta forti analogie con il pedinamento satellitare, il che induce a concludere, alla luce di quanto sopra detto, che non sia sufficiente un provvedimento motivato dell'autorità giudiziaria, ma che la legge debba disciplinare la natura, lo scopo, la durata della misura e i motivi per cui può essere adottata, oltre ai rimedi per l'interessato.

Pertanto, sarebbe forse più opportuno garantire una disciplina unitaria di tutte le forme di monitoraggio in tempo reale: "tracciamento dell'utenza", localizzazione in tempo reale del telefono cellulare, pedinamento satellitare.

---

[458] Si veda però A. CAMON, *L'acquisizione dei dati*, cit., p. 631-632, il quale ammette una lettura estensiva dell'art. 132 codice *privacy* per ricomprendervi il pedinamento satellitare. Analoga operazione potrebbe essere fatta anche per il tracciamento del cellulare.

[459] E quindi occorrerebbe un provvedimento motivato dell'autorità giudiziaria. Cfr. G. DI PAOLO, *Prova informatica*, cit., p. 753. Secondo l'Autrice, infatti, poiché il dispositivo posto sotto controllo è uno strumento di comunicazione, il tracciamento si pone in conflitto con il diritto tutelato dall'art. 15 Cost., nel cui ambito da tempo la giurisprudenza fa rientrare i dati esterni delle comunicazioni. Tuttavia, come correttamente osservato da altra parte della dottrina, il dato concernente il luogo in cui si trova l'utente al momento della comunicazione «non riguarda la libertà di comunicazione e corrispondenza, ma semmai la *privacy*». Così, R. ORLANDI, *Lodo "Maccanico": attuazione dell'art. 68 Cost. e sospensione dei processi per le alte cariche. Profili di diritto processuale*, in *Dir. pen. proc.*, 2003, p. 1214.

4. Perquisizioni online

Con il termine perquisizione *online* – dal tedesco *Online Durchsuchung* – si fa riferimento a quell'insieme di operazioni di esplorazione e monitoraggio di un sistema informatico, rese possibili dall'infiltrazione segreta nello stesso. Attraverso l'installazione, in locale o in remoto, di uno specifico *software*[460] sul *computer* oggetto di osservazione è infatti possibile, ogniqualvolta l'utente si colleghi a *Internet*, "perquisire" l'*hard disk* ed ottenerne copia, rilevare e registrare i siti *web* che vengono visitati, decifrare quel che viene digitato sulla tastiera, "intercettare" le comunicazioni *VoIP*, attivare le periferiche audio e video per sorvegliare il luogo in cui si trova il *computer*.

L'installazione in remoto di tale programma può avvenire attraverso l'inoltro via *e-mail* di un c.d. *trojan horse*. Si tratta, come suggerisce il nome stesso - "cavallo di Troia" - di un particolare tipo di programma con funzionalità note all'utente (diversamente dai *virus* è, in questo caso, egli stesso che volontariamente installa il programma), ma che cela al suo interno un codice "segreto" che viene eseguito sul *computer* ad insaputa dell'utente stesso; viene quindi creato un particolare collegamento tra il *computer* su cui è stata installata la *backdoor* e un *computer* remoto, che fa sì che l'utente di quest'ultimo abbia il pieno controllo del primo sistema informatico[461].

L'installazione in locale presuppone, invece, la collocazione di tale programma direttamente sul *computer*, il che può avvenire nelle stesse forme con cui si installano microspie in una stanza ai fini delle intercettazioni ambientali (non a

[460] Il programma in questione è una *backdoor* che può essere installata in locale o in remoto sul *computer* che si intende perquisire. La *backdoor* è un particolare tipo di *malware* (dall'inglese *malicious software*, ovverosia "programma malvagio") che consente di prendere il controllo di un altro *computer*, sfruttando una connessione *Internet*, quando l'utente vi si colleghi (di qui il termine perquisizioni *online*).

[461] Tale tecnica presenta un ulteriore aspetto problematico. Infatti, non si può mai essere certi che la *e-mail* contenente il *trojan* venga "intercettata" unicamente dal destinatario della stessa e non da altri soggetti; inoltre, non si può sapere a priori da quale *computer*, o altro dispositivo mobile di nuova generazione, il messaggio di posta elettronica venga aperto e quindi dove, concretamente, il *malware* venga eseguito. Si pensi, ad esempio, a chi controlla la casella di posta elettronica personale dal *computer* "aziendale" o viceversa, a chi controlli l'indirizzo *e-mail* usato per lavoro, sul *computer* di casa: verrà, in questo caso, perquisito il *computer* sbagliato. La perquisizione *online* può essere eseguita anche servendosi di *keyloggers*, *spyware* o *sniffers*.

caso la *backdoor* è stata definita "una sorta di microspia informatica"[462]) oppure, addirittura, attraverso l'inserimento di simile "porta di servizio" direttamente sui *computers* di serie, ciò, ovviamente, a seguito di un accordo tra Governo e produttori di *computer* e *software*.

Già questi primi cenni sono sufficienti a mettere in evidenza da un lato le enormi potenzialità per la repressione – e in ipotesi prevenzione – dei reati insite in tale poliedrico strumento d'indagine, dall'altro la particolare invasività di simile mezzo di ricerca della prova, capace di minare le fondamenta dei "classici" diritti fondamentali.

L'accesso "segreto" ad un sistema informatico è suscettibile di ledere, a più livelli, la sfera privata di ogni individuo. Vengono in rilievo delicati profili di garanzia della libertà e segretezza delle comunicazioni (art. 15 Cost.) e dell'inviolabilità del domicilio (art. 14 Cost.), di tutela della riservatezza (artt. 2 Cost., 8 CEDU, 7 CDFUE) e dei dati personali (art. 8 CDFUE, art. 16 TFUE)[463].

I diritti costituzionali sono il frutto di una determinata epoca storica, ma i beni che tutelano non sono cristallizzati, al contrario, devono necessariamente essere aggiornati alla luce degli sviluppi della società, solo così potendosi garantire effettività di tutela. Tuttavia, di fronte al progresso tecnologico la doverosa interpretazione evolutiva del dettato costituzionale non basta. Ciò è evidente nel caso delle perquisizioni *online*, che non solo coinvolgono contestualmente diversi beni costituzionalmente protetti, richiedendo all'interprete un'opera di definizione dei confini e dei rapporti reciproci tra le previsioni costituzionali – ma rappresentano una forma a tal punto intensa e nuova di limitazione di tali beni, da richiedere la messa a punto di un nuovo diritto della personalità.

---

[462] S. MARIOTTI, S. TACCONI, *Riflessioni sulle problematiche investigative e di sicurezza connesse alle comunicazioni* VoIP*,* in *Dir. Internet*, 2008, p. 561.

[463] Sull'*hard disk* di un *computer* sono salvati una serie di dati personali, quali, a titolo meramente esemplificativo, fotografie, pagine di diario, documenti medici, la corrispondenza con il difensore. Come si è già messo in luce nel precedente capitolo a proposito delle perquisizioni informatiche, la tecnologia ancora non consente di programmare questo specifico *software* di indagine in modo che venga eseguito sul *computer* in modo selettivo, cioè evitando di accedere ai dati personali, irrilevanti per le indagini.

4.1 Inquadramento giuridico. L'esperienza tedesca

Le perquisizioni *online* rappresentano un istituto di natura ibrida e di difficile inquadramento giuridico. Si tratta di un'attività di indagine che assomma le caratteristiche e le funzioni di diversi mezzi di ricerca della prova tipici, pur non essendo riconducibile ad alcuno di essi, e che presenta altresì caratteri di originalità[464].

L'istituto, non disciplinato dal legislatore italiano, è stato al centro di un vivace dibattito giurisprudenziale e dottrinale in Germania, dove è culminato nella più volte menzionata decisione del *Bundesverfassungsgericht* del 27 febbraio 2008, di cui è opportuno dare conto[465]. Tale sentenza aveva infatti ad oggetto, tra le altre[466], la questione di costituzionalità del *§ 5, Abs. 2, n. 11*, della Legge sulla protezione della Costituzione del *Land Nord Rhein Westfalen* cha autorizzava un organismo di *intelligence* a "protezione della costituzione" (*Verfassungsschutzbehörde*) ad effettuare due tipi di indagine: il monitoraggio e la ricognizione segreti di *Internet* e l'accesso segreto a sistemi informatici.

Già prima dell'intervento del *BVerfG* la dottrina tedesca si interrogava sui delicati rapporti tra perquisizioni *online* e diritti costituzionalmente garantiti e su come armonizzare tale strumento con il dettato codicistico.

L'ordinamento tedesco distingue, infatti, tra *offene Ermittlungsmaßnahmen*, cioè mezzi di ricerca della prova "palesi", cui appartengono le ispezioni, le perquisizioni e i sequestri, e *verdeckte Ermitttlungsmaßnahmen*, mezzi di ricerca della prova "segreti", tra cui rientrano le intercettazioni di comunicazioni e le intercettazioni ambientali[467].

---

[464] Cfr. B. SCHRÖDER, C. SCHRÖDER, *Die Online-Durchsuchungen. Rechtliche Grundlagen, Technik, Medienecho, Telepolis*, 2008; S. HOLZNER, *Die Online-Durchsuchung: Entwicklung eines neuen Grundrechts*, Freiburg im Breisgau, 2009; D. KOHLMANN, *Online-Durchsuchungen und andere Maßnahmen mit Technikeinsatz*, Baden-Baden, 2012; F. ROGGAN, *Online-Durchsuchung – Rechtliche und tatsächliche Konsequenzen des BVerfG – Urteils vom 27. Februar 2008, Berliner Wissenschaftsverlag, Juli* 2008. Si veda anche S. W BRENNER, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, in 81 *Miss. L. J.*, 1 (2011).

[465] V. *Supra*, capitolo I, par. 5.1.

[466] Il ricorso aveva ad oggetto altresì il *§ 7, Abs. 1, § 5, Abs. 3, § 5a, Abs. 1 e § 13* del *Gesetz über den Verfassungsschutz in Nordrhein-Westfalen - NRW-VerfSchG*, in materia di raccolta e trattamento dei dati degli utenti, in specie da sistemi informatici e attraverso la rete.

[467] Vedi W. BÄR, *Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen*, in *MMR*, 2008, p. 215 ss.; D. KLESCZEWSKI, *Strafprozessrecht*, Carl Heymanns Verlag 2007, p. 61 ss.; C. ROXIN, B. SCHÜNEMANN, *Strafverfahrensrecht*, *26. Auflage*, München, 2009, p. 209 ss.

Proprio il carattere segreto della perquisizione *online* aveva indotto taluno a ritenere applicabile la disciplina delle intercettazioni, andando oltre il *nomen iuris*[468]. Altri invece ritenevano applicabili proprio le norme relative alle perquisizioni in base ad un'asserita identità di scopo - la ricerca del corpo del reato o di cose pertinenti al reato - e al fatto che la presenza fisica dell'autorità procedente sul luogo e al momento della perquisizione non fosse requisito necessario della fattispecie[469]. Infine, vi era chi sosteneva la non riconducibilità delle perquisizioni *online* ad alcun mezzo di ricerca della prova e predicava la necessità di una disciplina *ad hoc*.

Già nel 2005 Manfred Hofmann, Procuratore Generale presso il

[468] La disciplina delle intercettazioni è contenuta nei paragrafi 100a e 100b del codice di procedura penale (novellati nel 2008 dal *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen* e di attuazione della direttiva 2006/24/CE). Le intercettazioni possono essere disposte in presenza di gravi indizi di uno dei reati indicati nel secondo comma del § 100a *StPO*, se l'accertamento dei fatti o la ricerca del luogo in cui si trattiene l'imputato possano essere notevolmente aggravati dall'uso di altri mezzi di ricerca della prova "palesi" (principio di proporzione in senso stretto) o se l'uso di tali ultimi mezzi appaia senza prospettive (principio di sussidiarietà). La misura può rivolgersi solo nei confronti dell'imputato o di altra persona della quale si ha ragione di sospettare che riceva o trasmetta messaggi per conto dell'imputato, ovvero della quale l'imputato utilizzi il collegamento telefonico. Nel caso in cui vi siano fondati motivi di ritenere che, attraverso l'utilizzo di tale misura, si venga a conoscenza esclusivamente di elementi che attengono alla sfera privata, le intercettazioni sono illecite, i fatti privati che si siano incidentalmente appresi non sono utilizzabili ai fini delle indagini e le registrazioni che li riguardano vanno cancellate (§ 100a *StPO*). La competenza a disporre tale misura spetta al giudice su richiesta del pubblico ministero; in caso di *periculum in mora* anche un provvedimento dispositivo del pubblico ministero è lecito, ma perde efficacia se non è confermato dal giudice entro tre giorni lavorativi. Le intercettazioni possono avere una durata massima di tre mesi, prorogabili di altri tre nel caso in cui, alla luce dei risultati d'indagine ottenuti, ne persistano i presupposti. Il provvedimento dispositivo ha forma scritta e deve contenere, per quanto possibile, il nome e l'indirizzo dell'imputato, il numero telefonico o altro elemento atto ad identificare l'utenza sottoposta ad intercettazione, la natura, il contenuto e la durata della misura, con particolare riguardo al termine finale della stessa. Nel momento in cui ne vengano meno i presupposti, l'intercettazione deve essere interrotta senza ritardo e dei risultati della stessa deve essere data comunicazione al giudice che l'ha disposta (§ 100b *StPO*).

[469] Il codice di procedura penale tedesco distingue tra perquisizioni presso indiziato di reato (§ 102 *StPO*, *Durchsuchung beim Verdächtigen*) e perquisizioni presso terzi (§ 103 *StPO*, *Durchsuchung bei anderen Personen*). Le perquisizioni presso l'indiziato, personali o locali, possono essere disposte sia al fine dell'arresto dello stesso, sia quando si presuma di poter rinvenire cose di rilevanza probatoria sulla persona dell'indiziato o nei luoghi di cui egli ha la disponibilità. Le perquisizioni presso terzi, solo locali, possono essere disposte ai fini dell'arresto dell'imputato, della ricerca di tracce di reato ovvero del sequestro di determinati oggetti, quando vi sia fondato motivo di ritenere che l'imputato, le tracce del reato o gli oggetti da sequestrare si trovino presso il terzo. In entrambe le ipotesi la perquisizione è disposta dal giudice e, solo in caso di *periculum in mora,* dal pubblico ministero (§ 105 *StPO*); il decreto di perquisizione deve indicare il reato per cui si procede, la persona indiziata/imputata e gli oggetti da sequestrare. Colui che ha la disponibilità dei locali perquisiti ha diritto di essere presente e, se non può esserlo, di farsi sostituire dal difensore o da altra persona di fiducia (§ 106 comma 1 *StPO*); inoltre, se la perquisizione avviene presso un terzo, questi ha diritto di essere informato, all'inizio, dello scopo della stessa (§ 106 comma 2 *StPO*). Al termine della perquisizione, il destinatario del provvedimento può richiedere il rilascio di un verbale contenente il motivo della perquisizione nonché l'indicazione del reato per cui si procede (§ 107 *StPO*).

Bundesgerichtshof[470]*,* si interrogava sulla possibilità di qualificare le perquisizioni *online*, tecnicamente esperibili solo quando l'utente del *computer* utilizzi *Internet,* alla stregua di intercettazioni telefoniche: come queste ultime richiedono un collegamento telefonico, le prime presuppongono un allacciamento al *web.* Infatti, se per telecomunicazione si intende «il procedimento tecnico di invio, trasmissione, ricezione di dati di ogni tipo sotto forma di segni, parole, immagini o suoni, attraverso apparecchi di comunicazione» (§ 3 Nr. 22 TKG), essa ricomprende senza dubbio i dati contenuti nella memoria di un *computer*, che costituiscono l'oggetto tipico di una perquisizione. Dal momento che intercettazioni e perquisizioni *online* sono entrambi mezzi di ricerca della prova che riguardano le telecomunicazioni, sarebbe senz'altro consentito far ricadere il nuovo strumento d'indagine sotto la disciplina dei paragrafi 100a e 100b *StPO*.

Lo stesso Autore è anche dell'avviso che nulla osti all'applicazione della disciplina delle perquisizioni *tout court*; egli afferma infatti, in disaccordo con altri, che i §§ 102 e 103 *StPO* non presuppongano la presenza fisica dell'autorità inquirente sul luogo di esecuzione della misura, e che non si tratti di un mezzo di ricerca della prova ispirato a principi di pubblicità. Inoltre, le disposizioni dei §§ 105, 106, 107 *StPO*, i quali prevedono che l'interessato sia messo al corrente per iscritto dello scopo della perquisizione e che abbia il diritto di essere presente al suo svolgimento, sono norme meramente processuali, la cui violazione non comporta alcuna conseguenza; da ciò si fa derivare la possibilità di individuare un *tertium genus* di perquisizione, con le stesse finalità – la perquisizione tende a ricercare tracce o altre cose pertinenti al reato, e tra queste possono a pieno titoli rientrare i dati salvati sull'*hard disk* - e la stessa denominazione di quello disciplinato dalle suddette norme, ma con una diversa procedura attuativa.

In realtà, pur chi condivide l'asserita identità di scopo tra perquisizioni *online* e perquisizioni *tout court*, non può trascurare la circostanza per cui le prime vengono condotte con modalità tali da renderle più affini alle intercettazioni telefoniche, poiché l'attività investigativa determina una maggiore invasività nella sfera privata. Inoltre, il fatto che le perquisizioni *online* vengano attuate in modo incompatibile con quanto stabilito dai §§ 105-107 *StPO*, svela l'inadeguatezza della disciplina ordinaria

[470] M. HOFMANN, *Die Online-Durchsuchung-staatliches "Hacken" oder zulässige Ermittlungsmaßnahme?*, in *NZtS*, 2005, p. 121 ss.

delle perquisizioni a tutelare il soggetto destinatario della misura stessa, il quale, proprio a causa della segretezza dell'accesso, subisce una sensibile invasione della propria riservatezza, ciò che non va assolutamente trascurato.

Diversa è la soluzione da altri prospettata: si evidenzia, infatti, come sarebbe possibile far rientrare le perquisizioni *online* sotto la disciplina dei §§ 102 ss. *StPO* solo a costo di una forzatura, o meglio, di un'interpretazione analogica dei §§ 102 e 103 *StPO* che li renda applicabili ad un mezzo di ricerca della prova con identiche finalità, ma modalità di attuazione diverse. Tuttavia, si ritiene che l'applicazione analogica di una norma che disciplina un'intromissione in un diritto fondamentale equivalga ad un'elusione del principio di riserva di legge fissato dalla costituzione come presupposto di intromissioni nei diritti fondamentali di libertà. Logica conseguenza di tale impostazione è l'impossibilità di ricondurre le perquisizioni *online* sotto la disciplina delle perquisizioni *tout court*[471].

Infine c'è stato anche chi, analizzando le disposizioni codicistiche relative alle perquisizioni e alle intercettazioni, ha optato per una loro generale inidoneità a disciplinare il nuovo strumento d'indagine[472]. Nel primo caso perché la presenza fisica dell'autorità procedente sul luogo perquisito e il rispetto di principi di pubblicità sarebbero requisiti indispensabili della disciplina di cui ai §§ 102 ss. *StPO*. Nel secondo perché le intercettazioni riguardano l'accesso ad una comunicazione in corso, e quindi, le disposizioni dei §§ 100a e 100b *StPO* sarebbero inidonee a permettere un'attività d'indagine sui dati che, a seguito di una conversazione, rimangono salvati sul *computer*.

Il *BVerfG*, chiamato a pronunciarsi sulla legittimità costituzionale della *Online Durchsuchung*, ha dichiarato la disciplina contenuta nel *NRW-VerfSchG* illegittima in quanto non rispettosa dei principi di proporzionalità e determinatezza, ma non ha escluso in assoluto l'ammissibilità di tale strumento di indagine.

Interessante l'argomento reputato decisivo per la citata declaratoria di illegittimità. Ritenendo insufficienti le garanzie offerte dalle norme costituzionali a tutela della segretezza delle telecomunicazioni (art. 10 *GG*) e dell'inviolabilità del domicilio (art. 13 *GG*) e, altresì, del diritto all'autodeterminazione informativa -

[471] M. JAHN, H. KUNDLICH, *Die strafprozessuale Zulässigkeit der Online-Durchsuchung*, in *JR*, 2007, p. 57 ss.
[472] M. GERCKE, *Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit*, in *CR*, 2007, p. 245 ss.

Informationelles Selbstbestimmungsrecht - precedentemente messo a punto nel 1983 con la nota sentenza sul censimento (*Volkzählungsurteil*), il *Bundesverfassungsgericht* ha preso atto dell'esistenza di un nuovo diritto fondamentale "alla garanzia della segretezza e integrità dei sistemi informatici" (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*). Un diritto di rango costituzionale, ricavato da quella sorgente di diritti inviolabili che è la *Menschenwürde* (artt. 1, comma 1 e 2, comma 1 *GG*)[473].

Consapevole delle peculiarità proprie dello strumento informatico rispetto ai tradizionali mezzi di comunicazione, la Corte Costituzionale tedesca ha ritenuto opportuno predisporre una tutela ulteriore e sussidiaria rispetto a quella già vigente. Di fronte alle sfide lanciate dal progresso tecnologico, infatti, la semplice, quanto doverosa, interpretazione evolutiva del dettato costituzionale non basta, le tradizionali garanzie della segretezza delle telecomunicazioni e dell'autodeterminazione informativa non sono sufficienti.

Sulla base di queste premesse la Corte ha stabilito che operazioni investigative suscettibili di comprimere tale nuovo diritto della personalità possono essere giustificate, non solo da finalità di repressione di reati, ma anche da finalità preventive[474], a condizione che siano rispettati il principio di proporzionalità – la Corte fa un elenco di beni giuridici per tutelare i quali è consentita l'intromissione in sistemi informatici o telematici[475] – e la riserva di giurisdizione – occorre un provvedimento autorizzativo del giudice, che poi sorvegli tale attività, come peraltro è normalmente previsto per le altre operazioni limitative della libertà personale - .

Non solo, ma il *Bundesverfassungsgericht*, rivolgendosi al legislatore tedesco che voglia disciplinare questo particolare strumento, auspica l'adozione di un adeguato sistema di misure tecniche preventive che impediscano di avere accesso a dati personali, irrilevanti per le indagini o comunque la previsione di garanzie *ex post*

[473] *Supra*, capitolo I, par 5.1.
[474] Il passaggio è molto delicato perché rimanda al pericolo che le perquisizioni si trasformino in mezzi di ricerca della *notitia criminis*, pericolo peraltro che nell'ordinamento tedesco è ridimensionato dall'esistenza di una norma specifica, il § 108 *StPO*, che disciplina il sequestro di cose, rinvenute nel corso della perquisizione, pertinenti ad un reato diverso da quello per cui si procede.
[475] La vita, l'incolumità fisica, la libertà dei singoli, e i beni della collettività la cui minaccia tocca il fondamento dello Stato, il suo mantenimento o la base dell'esistenza umana. Il rispetto del principio di proporzionalità richiede infatti che la compressione dei diritti fondamentali persegua uno scopo legittimo e sia idonea, necessaria ed opportuna quale mezzo per il raggiungimento di questo scopo.

consistenti nell'immediata cancellazione di tali dati e nella sanzione processuale dell'inutilizzabilità.

Alla luce di quanto riferito, unica soluzione rispettosa e del dettato costituzionale, e dell'assetto codicistico, appare dunque quella dell'introduzione di una norma *ad hoc*, che tenga conto della peculiare natura delle perquisizioni *online* e dell'incisività che queste hanno sulla sfera privata, disciplinandole in modo da conciliare le esigenze di indagine, che sempre più spesso richiedono l'utilizzo di strumenti che permettono la raccolta di prove all'insaputa del destinatario delle misure stesse, con i diritti costituzionalmente garantiti alla riservatezza della sfera privata e alla garanzia della segretezza e integrità dei sistemi informatici, così come da ultimo affermato dal *Bundesverfassungsgericht*.

4.2 Inquadramento giuridico in Italia

Le perquisizioni *online* non sono disciplinate nell'ordinamento giuridico italiano, né sono assimilabili ad uno dei mezzi di ricerca della prova tipici. Esse non sembrano riconducibili né alla disciplina delle perquisizioni, né a quella delle ispezioni, né infine a quella delle intercettazioni, configurando piuttosto un *tertium genus*.

Anche dopo le modifiche introdotte con la legge di ratifica della Convenzione *Cybercrime*, l'art. 247 c.p.p. non pare applicabile a questo innovativo strumento di indagine. Tale norma, infatti, si limita a rendere possibili le tradizionali perquisizioni, volte alla ricerca del corpo del reato o di cose pertinenti al reato anche in ambiente informatico, autorizzando la perquisizione di sistemi informatici o telematici «quando vi è motivo di ritenere che ivi si trovino dati, informazioni, programmi informatici o tracce comunque pertinenti al reato». Ma la relativa disciplina rimane quella classica di uno strumento di indagine a sorpresa, ma "palese". Stabilisce l'art. 250 c.p.p. che «nell'atto di iniziare le operazioni copia del decreto di perquisizione locale è consegnata all'imputato, se presente, e a chi abbia l'attuale disponibilità del luogo, con l'avviso della facoltà di farsi rappresentare o assistere da persona di fiducia purché questa sia prontamente reperibile e idonea». Inoltre, in base al disposto dell'art. 365 c.p.p., il destinatario della perquisizione viene invitato a

nominare un difensore di fiducia - se ne è privo gliene viene assegnato uno d'ufficio – il quale ha diritto a partecipare al compimento dell'atto, pur senza preavviso. Tali disposizioni sono inapplicabili alla c.d. perquisizione *online* che viene condotta all'insaputa dell'interessato. Inoltre, si è rilevato che tale strumento di indagine può prescindere dalla ricerca del corpo del reato e/o delle cose pertinenti al reato e non sfocia necessariamente in un sequestro[476]. L'osservazione coglie senz'altro nel segno, e mette in evidenza uno tra i tanti aspetti problematici delle perquisizioni *online*: il rischio che si trasformino in uno strumento di ricerca della *notitia criminis*. Rischio tanto più attuale in quanto manca nel nostro ordinamento una previsione – analoga al § 108 *StPO* - che disponga in merito alle cose casualmente trovate nel corso di una perquisizione che siano pertinenti ad un reato diverso rispetto a quello per il quale la perquisizione è stata disposta.

Ma nemmeno pare potersi applicare la disciplina delle ispezioni informatiche, novellata nel 2008. Infatti, esse servono a fotografare la realtà esistente, senza alcuna apprensione di dati[477].

Il carattere segreto della perquisizione *online* potrebbe allora indurre a ritenere tale attività assimilabile a quella di intercettazione informatica o telematica (art. 266 *bis* c.p.p.). Tale disciplina è *prima facie* sicuramente più adatta a soddisfare le esigenze di tutela della riservatezza del destinatario della perquisizione *online*. Essa prevede innanzitutto una delimitazione dei reati per la repressione dei quali tale strumento può essere utilizzato[478], rigidi presupposti di applicazione (gravi indizi di reato e indispensabilità dell'intercettazione ai fini della prosecuzione delle indagini). Inoltre, contempla una serie di disposizioni poste a vario titolo a tutela del destinatario della misura: da quelle che dispongono in merito al quando e al come

[476] S. MARCOLINI, *Le cosiddette perquisizioni* online *(o perquisizioni elettroniche)*, in *Cass. pen.*, 2010, p. 2855 ss.

[477] *Ibidem*, p. 2858. Così già, R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *del 27 febbraio 2008 sulla c.d.* Online Durchsuchung*. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona. Aspetti di diritto penale sostanziale*, in *Riv. trim. dir. pen. ec.*, 3, 2009, p. 695 ss.

[478] La dottrina tedesca si è altresì interrogata in merito all'individuazione dei reati per la repressione dei quali tale strumento d'indagine può essere utilizzato. Partendo dal presupposto che, trattandosi di una misura caratterizzata da forte incisività sui diritti fondamentali del destinatario, l'utilizzo che se ne possa fare debba essere limitato a reati di particolare gravità o allarme sociale, la dottrina si è divisa tra chi ha individuato tali reati in quelli di terrorismo internazionale, di pedopornografia e di sfruttamento sessuale, e chi, al contrario, e più opportunamente, ha ricompreso nell'elenco anche i reati economici, finanziari e tributari. Sul punto si veda M. KEMPER, *Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten*, in *ZRP*, 2007, p. 105 ss.

questi è ammesso a conoscere prima dell'esistenza dell'intercettazione e poi del suo contenuto, a quelle che prevedono divieti di utilizzazione e conseguenti obblighi di distruzione dei risultati di intercettazioni eseguite in violazione delle disposizioni di legge.

Tuttavia, le perquisizioni *online* non si limitano a rendere possibile una captazione occulta del contenuto di comunicazioni. Ciò è ben colto dal giudice costituzionale tedesco laddove afferma che la protezione accordata dal *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* è sussidiaria rispetto a quella offerta dall'art. 10 *GG* – che tutela la segretezza delle comunicazioni - e non trova applicazione quando il *software* installato sul *computer* permetta di intercettare comunicazioni in corso[479].

La giurisprudenza in materia è pressoché inesistente; merita però di essere segnalata una sentenza della Corte di Cassazione del 2009 avente ad oggetto l'installazione sul *computer* dell'indagato di un c.d. captatore informatico (*gosth*) in grado di acquisire in remoto copia dei *files* esistenti e di registrare in tempo reale tutti i *files* elaborandi[480]. Il *software* in questione permetteva quindi di monitorare in modo occulto e continuativo il *computer* dell'indagato. Simile attività di indagine era stata disposta con decreto del pubblico ministero ai sensi dell'art. 234 c.p.p.

La Suprema Corte ha respinto le eccezioni sollevate dal ricorrente, il quale sosteneva innanzittutto che si sarebbe dovuta applicare la disciplina delle intercettazioni informatiche, e che in ogni caso l'attività posta in essere violava gli artt. 14 e 15 Cost. e doveva pertanto considerarsi una prova incostituzionale, e i relativi risultati inutilizzabili ai sensi dell'art. 191 c.p.p.

Quanto alla prima eccezione, la Corte, ha ritenuto che per flusso di comunicazione ai sensi dell'art. 266 *bis* c.p.p. deve intendersi «*la trasmissione, il trasferimento, di presenza o a distanza, di informazioni da una fonte emittente ad un*

[479] L. DRALLÉ, *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, *Lorenz-von-Stein-Institut*, 2010, p. 142 ss.

[480] Cass., sez. V, 14 ottobre 2009, n. 16556, in *C.E.D. Cass*., n. 246954. Cfr. S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, p. 955 ss. La sentenza è altresì interessante perché la Cassazione ha escluso che tali operazioni di indagine dovessero essere compiute seguendo la disciplina degli accertamenti tecnici irripetibili, poiché «*l'attività di riproduzione dei* files *memorizzati non aveva comportato l'alterazione, né la distruzione dell'archivio informatico, rimasto immutato, quindi consultabile ed accessibile nelle medesime condizioni, anche dopo l'intervento della polizia giudiziaria*». Trattandosi di attività reiterabile, non era necessaria la presenza del difensore. Sul punto, sia consentito rinviare alle osservazioni svolte *supra*, capitolo I, par. 4.1.

ricevente, da un soggetto ad altro, ossia il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi infornatici o telematici, non potendo ritenersi sufficiente l'elaborazione del pensiero e l'esternazione, anzichè mediante simboli grafici apposti su un supporto cartaceo, in un documento informatico realizzato mediante un sistema di videoscrittura ed in tal modo memorizzato». Correttamente quindi i giudici di merito avevano escluso l'applicazione della disciplina di cui agli artt. 266 ss. c.p.p., in quanto il decreto del pm non aveva ad oggetto un flusso di comunicazioni, bensì «*una relazione operativa tra microprocessore e video del sistema elettronico, ossia un flusso unidirezionale di dati confinato all'interno dei circuiti del* personal computer».

Non trattandosi di comunicazione, non trovava quindi applicazione la tutela di cui all'art. 15 Cost. Né la Corte riscontra una violazione dell'art. 14 Cost. in quanto il *computer* monitorato non si trovava all'interno del domicilio – inteso come luogo di privata dimora – ma in un luogo aperto al pubblico, ossia «*nei locali di un ufficio pubblico comunale ove sia l'imputato sia gli altri impiegati avevano accesso per svolgere le loro mansioni ed ove potevano fare ingresso, sia pure in determinate condizioni temporali, il pubblico degli utenti ed il personale delle pulizie, insomma una comunità di soggetti non particolarmente estesa, ma nemmeno limitata o determinabile a priori in ragione di una determinazione personale dell'imputato*».

Se si può convenire sull'esclusione della garanzia di cui all'art. 15 Cost., l'argomentazione con cui la Corte esclude l'applicabilità dell'art. 14 Cost. appare troppo frettolosa. In ogni caso poi, tali prescrizioni costituzionali non esauriscono il novero dei diritti fondamentali che simile attività di indagine comprime. Se anche, nelle parole della Corte, «*quanto riprodotto in copia non era un testo inoltrato e trasmesso col sistema informatico, ma soltanto predisposto per essere stampato su supporto cartaceo e successivamente consegnato sino al suo destinatario*», persistono comunque esigenze di tutela della riservatezza, bene giuridico di rango costituzionale, che avrebbero richiesto un esame più approfondito della vicenda.

Oltre alle riserve di carattere costituzionale, anche la riconduzione dell'attività in questione all'acquisizione della prova documentale lascia perplessi. Infatti, l'art. 234 c.p.p. fa riferimento a documenti, ancorchè informatici, preesistenti al provvedimento acquisitivo stesso e non a quelli costituendi. Ora, è ben vero che il

decreto del pm prevedeva l'acquisizione dei *files* memorizzati sul *computer*, ma è altresì vero che tale generica formula, unitamente al fatto che il monitoraggio si è protratto per otto mesi, fanno ritenere del tutto verosimile l'apprensione di documenti formati dopo il provvedimento *de quo*.

4.3 Perquisizioni online*: prova atipica o prova incostituzionale?*

Il fatto che la c.d. perquisizione *online* non sia riconducibile ad alcuno dei mezzi di ricerca della prova specificamente disciplinati dal codice di rito non significa che si possa concludere nel senso della sua atipicità e quindi ammissibilità alle condizioni stabilite dall'art. 189 c.p.p. Infatti, come si è già messo in luce a proposito del pedinamento satellitare, il primo presupposto di validità di una prova atipica è la sua legittimità costituzionale. Occorre quindi verificare quali diritti fondamentali siano coinvolti in tale attività di indagine. Ciò consentirà di delineare i presupposti e i confini entro cui iscrivere tale mezzo di ricerca della prova, tenendo presente che essi variano non solo in relazione al tipo di bene giuridico tutelato – segretezza delle comunicazioni, riservatezza (informatica), dati personali – ma anche e soprattutto in funzione dell'intensità della limitazione cui danno vita.

Tale operazione ermeneutica è resa più impegnativa nel caso delle perquisizioni *online* dal fatto che esse racchiudono in sé diversi strumenti di indagine.

Viene sicuramente in rilievo il diritto alla libertà e segretezza delle comunicazioni (art. 15 Cost.) che, tuttavia, estende il suo ambito di tutela alle sole comunicazioni che avvengano tramite il *computer* (conversazioni *VoIP*, *e-mail*, *chat*), nonché sulla base della giurisprudenza della Corte costituzionale in materia di tabulati telefonici, anche ai dati esterni di tali comunicazioni, ossia ai dati di traffico telematico.

Quanto all'art. 14 Cost., se per domicilio si intende «uno spazio isolato dall'ambiente esterno, adibito allo svolgimento di atti della vita privata e dal quale il soggetto o i soggetti titolari abbiano inteso normalmente escludere la presenza di terzi»[481], difficilmente può negarsi la sua operatività nella fase di intromissione nel

[481] Così, G. BORRELLI, *Riprese filmate*, cit., p. 2453.

sistema informatico[482]. Infatti, in considerazione dell'importanza essenziale nella vita di tutti i giorni che il *computer* è venuto assumendo, al punto che la Corte costituzionale tedesca lo ha considerato uno strumento attraverso cui l'individuo sviluppa liberamente la propria personalità, esso può considerarsi un "domicilio informatico", soprattutto quando sia protetto da *password*.

L'analisi non si può tuttavia arrestare a questa prima e più immediata interpretazione estensiva della tutela del domicilio tradizionale. Come si è visto nella prima parte del presente lavoro, il sistema informatico viene in rilievo quale contenitore di dati personali, quale perimetro ideale di una serie di informazioni che si vogliono sottorarre alla conoscenza altrui. Oggetto di protezione sono i dati, rivelatori di aspetti fondamentali della vita privata del soggetto. Dati che, privi di una dimensione fisica, sono spesso salvati nel *cyberspace*. In quest'ottica, la tutela del domicilio si rivela inadeguata: pur tutelando «la persona riflessa in una certa sfera spaziale volta a preservare il carattere intimo, domestico, o quanto meno privato di determinati comportamenti soggettivi», essa rimane pur sempre legata ad un ambiente fisico, all'interno del quale si svolge la vita privata. A venire in rilievo è piuttosto l'esigenza di riservatezza, *sub specie* di riservatezza informatica, dell'utilizzatore di un sistema informatico. Sia consentito qui richiamare le conclusioni sopra svolte in merito a elaborazione, contenuto, e rango nel sistema delle fonti di tale diritto fondamentale "di nuova generazione"[483].

Parte della dottrina che si è occupata del tema ha concluso quindi per l'inutilizzabilità (o inammissibilità) costituzionale delle perquisizioni *online*. Infatti, se «fossero effettuate in un procedimento penale italiano, [esse] 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 […] esige la previa determinazione, da parte del legislatore ordinario, dei casi e dei modi di aggressione

[482] Come precisato anche dalla Corte costituzionale nella sentenza 24 aprile 2002, n. 135, cit., l'elenco dei mezzi di ricerca della prova attraverso cui la pubblica autorità può interferire nella libertà domiciliare non è tassativo. Argomenti in tal senso non si possono desumere nemmeno dall'art. 8 CEDU o dagli artt. 7 e 52 CDFUE. Inoltre, l'art. 14 Cost. «*nell'ammettere intrusioni nel domicilio per finalità di giustizia non prende posizione sul carattere palese o occulto delle intrusioni stesse. La configurazione di queste, e in particolare delle ispezioni, come atto palese*», prosegue la Corte, «*emerge esclusivamente a livello di legislazione ordinaria*».

[483] V. *Supra*, capitolo I, par. 1.1, 2 e 5.2.

di quel bene»[484].

Tuttavia, l'affermare che la perquisizione *online* è attualmente un prova incostituzionale non rappresenta una conclusione, ma un punto di partenza. Infatti, l'obiettivo non è quello di negare cittadinanza a tale strumento nel nostro ordinamento, ma di stabilire a quali condizione esso sia legittimo. Di ciò è ben consapevole il *BVerfG*, che infatti ha creato il nuovo diritto della personalità con funzione di garanzia dell'individuo rispetto ad attività di indagine quali quelle cui danno vita le perquisizioni *online*.

Se si accoglie l'idea che il nuovo bene giuridico riservatezza informatica è tutelato dagli artt. 2, 117, comma 1 Cost., 8 CEDU e 7 CDFUE, eventuali limitazioni dello stesso ad opera della pubblica autorità potranno avvenire solo se rispettose delle prescrizioni di cui agli articoli 8, comma 2 CEDU e 52, comma 1 CDFUE. Esse dovranno quindi essere previste dalla legge, perseguire uno scopo legittimo e rispettare il principio di proporzionalità, fatta salva l'intagibilità del nucleo essenziale di tale diritto fondamentale.

Una volta messa a punto la cornice costituzionale di riferimento, è quindi compito del legislatore intervenire, dettando una disciplina *ad hoc*, che raggiunga un equo bilanciamento tra diritti costituzionalmente protetti. Essa dovrà innanzitutto individuare i casi e modi dell'intromissione in un sistema informatico: elenco di reati presupposto[485], provvedimento motivato dell'autorità giudiziaria – in questo caso del giudice su richiesta del pubblico ministero –, modalità di svolgimento delle operazioni. A quest'ultimo riguardo dovranno essere introdotte specifiche garanzie a tutela dei dati personali irrilevanti per le indagini, e apposite sanzioni di inutilizzabilità del materiale probatorio acquisito illegittimamente o irrilevante. Infine, è opportuno stabilire se il ricorso a tale strumento sia consentito anche per finalità preventive.

L'intervento del legislatore non pare più procrastinabile. Il fatto che nessun caso sia fino ad ora giunto all'attenzione della Corte di cassazione non significa che le perquisizioni *online* non siano usate nella prassi. Infatti, sempre più spesso gli investigatori avvertono la necessità di "introdursi" segretamente in un sistema

[484] Così, S. MARCOLINI, *Le cosiddette perquisizioni*, cit., p. 2861.
[485] Si dovrà trattare di reati posti a tutela di beni giuridici particolarmente rilevanti, tali da giustificare la limitazione di altrettanto rilevanti diritti costituzionali.

informatico per svolgere preziose indagini. In mancanza di una disciplina specifica, gli investigatori più virtuosi, consapevoli delle potenzialità lesive di tale strumento, faranno ricorso alla disciplina delle intercettazioni che, tra i vari mezzi di ricerca della prova, è quella senz'altro più garantista[486]. Che gli artt. 266 ss. c.p.p. siano inadeguati ad offrire sufficiente tutela dei nuovi diritti fondamentali è già stato evidenziato. Quindi, seppur si comprendono le esigenze investigative di chi spesso si trova a dover contrastare gravi forme di criminalità informatica con gli scarsi mezzi messi a disposizione dell'ordinamento, simile *modus procedendi* non può essere né condiviso, né assecondato. Esso, tuttavia, evidenzia una volta di più l'urgenza di un intervento del legislatore. Ciò anche in considerazione degli impulsi che vengono dall'Unione europea. A tal proposito si segnalano le conclusioni del Consiglio del 27 novembre 2008 relative ad una strategia di lavoro concertata e a misure pratiche di lotta alla criminalità informatica[487], che contengono un espresso invito agli Stati membri ad agevolare la perquisizione a distanza, se prevista dalla legislazione nazionale, in quanto essa consente ai servizi investigativi, con l'accordo del Paese ospite, di accedere rapidamente alle informazioni. Tale disposizione sembra infatti fare indiretto riferimento all'istituto delle perquisizioni *online*, il quale difficilmente potrà essere trascurato dai legislatori nazionali in futuro, data la sua fondamentale importanza per le indagini su materiale informatico e via *Internet*.

[486] Si adotteranno a ben vedere due provvedimenti, uno di intercettazione, autorizzato dal GIP, ed uno emesso dal pm, di sequestro del materiale rilevante rinvenuto sul *computer* oggetto di indagine.
[487] *GUUE* del 17 marzo 2009, C 62/16.

CAPITOLO IV
INVESTIGAZIONI INFORMATICHE TRANSNAZIONALI E TUTELA DEI DIRITTI FONDAMENTALI

SOMMARIO: *1. Indagini informatiche transfrontaliere 2. Cooperazione giudiziaria nell'ambito del Consiglio d'Europa: la Convenzione* Cybercrime *2.1 L'accesso transfrontaliero diretto a dati informatici 3. Cooperazione giudiziaria nell'ambito dell'Unione europea: mutuo riconoscimento* vs. *armonizzazione? 3.1 Le iniziative post-Lisbona: l'Ordine Europeo di Indagine Penale 3.2 (segue) Le* Model Rules *per la futura Procura Europea 4. Quale tutela per i diritti fondamentali? 4.1 La protezione dei dati personali nella Regione Europa 4.2 La giurisprudenza della Corte di Strasburgo come base per l'armonizzazione europea*

1. Indagini informatiche transfrontaliere

Lo studio dei mezzi di ricerca della prova che sfruttano le tecnologie informatiche non può prescindere dall'analisi dei profili di cooperazione giudiziaria. Infatti, lo spazio informatico è globale e refrattario a limitazioni nazionali. I dati digitali sono spesso salvati su *servers* o *personal computers* dislocati in Paesi diversi da quello in cui le indagini vengono svolte. Si pensi all'uso sempre più diffuso che viene fatto di servizi di *cloud computing*; in questo caso i dati sono salvati direttamente in *Internet*, e spesso vengono spostati dal gestore del *cloud* da un *server* ad un altro, per esigenze organizzative, tecniche o economiche (c.d. *load balancing*). Inoltre, l'utilizzatore stesso non si collega sempre al medesimo *server* per accedere ai suoi dati[488]. La conseguenza è che la localizzazione dei dati, "tradizionalmente" utilizzata per individuare lo Stato a cui rivolgere una richiesta di assistenza giudiziaria, si potrebbe rivelare inutile. Infatti, anche una volta individuato il *service*

[488] Il *cloud computing* può essere in via di prima approssimazione definito come un sistema informatico che consente di memorizzare, archiviare, elaborare dati, grazie all'utilizzo di risorse *hardware* e *software* distribuite in rete, in un'architettura tipica *client-server*. *Hardware*, *software*, dati, sono quindi salvati direttamente in *Internet*. Evidenti sono i vantaggi per l'utente che può accedere ai suoi dati ovunque egli si trovi, da qualunque dispositivo – c.d. ubiquità dei dati -, nonché beneficiare di una riduzione dei costi di manutenzione perché *hardware* e *software* sono gestiti dal fornitore del servizio di *cloud computing*. Tra i sistemi più diffusi e noti di *cloud computing*, basti ricordare *Dropbox* o *Google Mail*; anche i *social networks*, come *Facebook*, sono basati sul *cloud computing*.

provider che fornisce il servizio di *cloud computing*, ancora non si sa nulla su dove i dati siano concretamente salvati[489].

Alla difficoltà, se non impossibilità, di localizzazione dei dati e alla necessità di acquisirli rapidamente a causa della loro volatilità, fa da contraltare la possibilità tecnica di accedervi direttamente, ovunque essi si trovino. Ciò è possibile sia attraverso l'utilizzo di uno specifico *software* d'indagine installato sul *computer* del destinatario della misura[490], sia "forzando" il sistema di sicurezza per ottenere la *password* che protegge l'accesso ai dati.

L'accesso transfrontaliero diretto ai dati può determinare una violazione di principi cardine in materia di cooperazione penale internazionale quali la doppia incriminazione e la possibilità di rifiutare l'assistenza richiesta se ciò violi l'ordine pubblico nazionale. Ciononostante, non si può trascurare la circostanza che esso sempre più spesso costituisce una necessità per l'autorità procedente e che la tecnologia oggi lo rende possibile. L'art. 32 della Convenzione *Cybercrime* prevede proprio la possibilità di accesso diretto ai dati se disponibili pubblicamente, oppure «con il consenso legale e volontario della persona legalmente autorizzata a divulgare i dati». Tuttavia, più di dieci anni sono passati dall'adozione di tale Convenzione e il contesto tecnologico è cambiato, rendendo inadeguata tale previsione, pur sempre legata alla previa localizzazione dei dati[491]. È oggi avvertita la necessità di superare il principio della territorialità e quindi della sovranità come limite allo svolgimento di indagini transfrontaliere, e di introdurre regole nuove a livello sovranazionale che consentano di accedere ai dati informatici, anche se non si sa dove essi si trovino.

Trovare un punto di equilibrio tra esigenze investigative e tutela dei diritti fondamentali nel contesto digitale è delicato già a livello nazionale; quando si tratta di cooperazione internazionale, la sfida è ancora più impegnativa. In una concezione liberale del rito penale, infatti, il potere investigativo costituisce un'eccezione alla regola della libertà: «sono i diritti fondamentali della persona a definire i limiti dell'interesse statuale alla attività *lato sensu* istruttoria, di accertamento processuale.

[489] Spesso gli stessi *cloud provider* non sono in grado di sapere dove i dati o pacchetti di dati si trovino. Cfr. *Discussion Paper "Cloud Computing and Cybercrime Investigations: Territoriality vs. the Power of Disposal?"*, reperibile su *www.coe.int/cybercrime*.
[490] Si tratta del *software* utilizzato in Germania per condurre le c.d. perquisizioni *online*. *Supra*, capitolo III, par. 4 ss.
[491] Sono infatti attualmente in corso discussioni per la modifica dell'art. 32. *Infra*, par. 2.1

All'autorità giudiziaria è vietato qualsiasi atto che incida sui diritti della persona, tranne ciò che è esplicitamente permesso»[492]. Pertanto, ogni Stato ha differenti regole di acquisizione delle prove, nel rispetto dei presupposti e delle garanzie contenute nei rispettivi testi costituzionali. E i singoli sono adeguatamente tutelati nella misura in cui l'autorità inquirente rispetti le condizioni per la limitazione dei diritti fondamentali previsti dalla legislazione statale[493].

Diritti fondamentali quali la libertà personale, l'inviolabilità del domicilio, la libertà e segretezza delle comunicazioni e della corrispondenza, sono riconosciuti in tutti gli Stati della tradizione giuridica occidentale. Discorso parzialmente diverso vale per diritti di nuova generazione, come quelli di *privacy* (riservatezza, autodeterminazione informativa, c.d. riservatezza informatica), dei quali, come si è visto nella prima parte del presente lavoro, non è possibile affermare un generalizzato rango costituzionale. Si tratta in ogni caso di diritti non assoluti, bilanciabili con esigenze di pari livello costituzionale, quali quelle di indagine. E i presupposti di simile bilanciamento, ossia le condizioni che rendono legittima una limitazione dei suddetti diritti fondamentali, variano da Stato a Stato. Non solo, ma in alcuni casi, accade che in un ordinamento una determinata tecnica di indagine sia ritenuta lesiva di diritti fondamentali, e in un altro no[494]. Valga per tutti l'esempio del pedinamento satellitare, su cui ci si è soffermati nel precedente capitolo[495]. Simile divergenza nelle discipline nazionali, oltre che una potenziale violazione dei diritti fondamentali, può costituire un ostacolo alla cooperazione, spingendo gli Stati a

[492] La citazione è di F. RUGGERI, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001, p. 65, che a sua volta riprende le riflessioni svolte da M. NOBILI, *Divieti probatori e sanzioni*, in *Giust. pen.*, 1991, III, c. 641 ss. Cfr. M. PANZAVOLTA, *Intercettazioni e spazio di libertà, sicurezza e giustizia*, in F. RUGGIERI, L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, p. 70.

[493] Cfr. M. PANZAVOLTA, *Intercettazioni e spazio di libertà*, cit., p. 69.

[494] Come correttamente messo in luce da S. ALLEGREZZA, *Le misure coercitive nelle* «Model Rules for the Procedure of the European Public Prosecutor's Office», in F. RUGGIERI, T. RAFARACI, G. DI PAOLO, S. MARCOLINI, R. BELFIORE (a cura di), *Processo penale, lingua e Unione Europea*, Padova, 2013, p. 161, «con riferimento alle tecniche di sorveglianza tecnologica, l'unico elemento che pare accomunare le legislazioni nazionali è l'assenza di una disciplina puntuale nelle legislazioni nazionali».

[495] *Supra*, capitolo III, par. 2 ss. Mentre in Italia il pedinamento satellitare è considerato un'attività atipica d'indagine, che non limita alcun diritto costituzionale e che la polizia giudiziaria può portare avanti senza bisogno di alcuna autorizzazione da parte dell'autorità giudiziaria, in Germania, la sistematica e prolungata (più di ventiquattro ore) sorveglianza del sospettato necessita dell'autorizzazione dell'autorità giudiziaria, ossia del pubblico ministero se dura meno di un mese, del giudice per periodi più lunghi (§ 163 f *StPO*).

portare avanti le indagini anche oltre i limiti segnati dai loro confini territoriali, fin quando ciò sia tecnologicamente possibile.

Che le indagini informatiche vengano talvolta portate a termine unilateralmente dallo Stato procedente, al di fuori dei tradizionali meccanismi di assistenza giudiziaria è dimostrato dal noto caso *Ivanov-Gorshkov*, in cui agenti *FBI* di Seattle si sono "infiltrati" in *computers*, fisicamente localizzati in Russia e appartenenti a cittadini russi, e hanno scaricato sul loro *computer*, negli Stati Uniti, *files* utili per le indagini in corso[496].

Individuare regole chiare di cooperazione giudiziaria è di fondamentale importanza non solo per la tutela dei diritti fondamentali, ma anche al fine della successiva utilizzabilità della prova raccolta all'estero. La prova acquisita in violazione dei diritti fondamentali potrebbe, infatti, non essere utilizzabile in giudizio, ciò che renderebbe vano il ricorso all'assistenza giudiziaria.

Codeste criticità si acuiscono nell'ambito dell'Unione europea; l'intenzione, infatti, è quella di fondare anche la cooperazione in materia di prove sul principio del mutuo riconoscimento. Tuttavia, in assenza di una previa effettiva armonizzazione delle discipline nazionali, il mutuo riconoscimento potrebbe tradursi in una violazione dei diritti fondamentali della persona[497].

Occorre, quindi, anche nel contesto delle indagini transnazionali, innanzitutto individuare i diritti fondamentali coinvolti e fissare già a livello sovranazionale i presupposti di una limitazione legittima degli stessi per finalità d'indagine, lasciando comunque agli Stati il necessario margine di apprezzamento. Solo così si favorisce l'armonizzazione delle disposizioni processuali nazionali, e in ultima istanza si incentiva la cooperazione. Con il Trattato di Lisbona, l'Unione europea ha gli

[496] Il caso risale al 2001. *United States* v. *Gorshkov*, 23 May 2001, WL 1024026, U.S. Dist. Gli agenti FBI non erano in origine in possesso di un mandato di perquisizione, hanno però aspettato di ottenerlo prima di leggere e copiare i *files* scaricati. La *District Court* di Washington ha ritenuto non sussistente una violazione del IV Emendamento in quanto «*esso non si applica a perquisizioni e sequestri di cose di proprietà di stranieri non residenti* [negli Stati Uniti] *e che avvengano al di fuori del territorio nazionale. Nel caso di specie, i computers a cui gli agenti hanno avuto accesso erano situati in Russia, così come i dati copiati. Fino quando i dati copiati non sono stati trasmessi negli Stati Uniti, essi si trovavano fuori dal territorio di questo Paese e quindi non erano soggetti alla tutela del IV Emendamento*». Cfr. J. R. HERRERA-FLANIGAN, *Cybercrime and Jurisdiction in the United States*, in B. J. KOOPS – S. W. BRENNER (a cura di), *Cybercrime and Jurisdiction. A Global Survey*, TMC Asser Press, The Hague, 2006, p. 313 ss.

[497] Sul principio del mutuo riconoscimento è fondato il Mandato Europeo di Ricerca della Prova, che tuttavia non è ancora stato attuato e la proposta per un Ordine Europeo di Indagine Penale. *Infra*, par. 3 ss.

strumenti per promuovere tale armonizzazione. L'art. 82, par. 2 TFUE prevede infatti che «laddove necessario per facilitare il riconoscimento reciproco delle sentenze e delle decisioni giudiziarie e la cooperazione di polizia e giudiziaria nelle materie penali aventi dimensione transnazionale, il Parlamento europeo e il Consiglio possono stabilire norme minime deliberando mediante direttive secondo la procedura legislativa ordinaria» tra le altre, in materia di «ammissibilità reciproca delle prove tra gli Stati membri» (lett. a).

Il tema della cooperazione giudiziaria in materia penale è evidentemente molto ampio e complesso; quel che ci si propone di fare, nel limitato ambito del presente studio, è fornire una panoramica generale, ed inevitabilmente sintetica, degli strumenti che a livello di Consiglio d'Europa e di Unione europea si occupano di indagini informatiche transfrontaliere, con particolare attenzione al profilo della tutela dei diritti fondamentali coinvolti.

2. Cooperazione giudiziaria nell'ambito del Consiglio d'Europa: la Convenzione Cybercrime

La Convenzione *Cybercrime*, firmata a Budapest nel 2001, dedica il capitolo III alla cooperazione internazionale. Essa da un lato fa salvi eventuali accordi o strumenti internazionali sulla cooperazione in materia penale, dall'altro fissa specifiche regole per lo svolgimento di investigazioni informatiche transfrontaliere, basate sul principio della mutua assistenza (artt. 23 e 25). Giova ricordare che le disposizioni in materia processuale contenute nella Convenzione si applicano alla raccolta di prove in formato elettronico relative a qualsiasi reato.

La consapevolezza della necessità di raccogliere rapidamente la *digital evidence*, a causa della sua volatilità, emerge innanzitutto dalla possibilità di avvalersi di *fax* o posta elettronica per inviare una richiesta di mutua assistenza nei casi d'urgenza, «a condizione che tali strumenti diano adeguate garanzie di sicurezza e autenticazione» – tra cui viene espressamente annoverata la criptazione – (art. 25)[498]. Inoltre, è prevista l'istituzione della c.d. Rete 24/7, ossia di un punto di contatto in ogni Stato, disponibile ventiquattro ore su ventiquattro, sette giorni su

[498] In questo caso, peraltro, la richiesta può essere trasmessa direttamente all'autorità giudiziaria (art. 27, par. 9), anziché all'autorità centrale che ogni Stato deve designare ai sensi dell'art. 27, par. 2.

sette per assicurare un'assistenza immediata (art. 35). Si tratta di una forma di cooperazione informale che può sia precedere l'inoltro di una richiesta ufficiale di mutua assistenza, sia agevolarla. Sempre nell'ambito della cooperazione informale si inserisce la possibilità di fornire spontaneamente ad un'altra Parte informazioni ottenute nell'ambito di proprie indagini, qualora si ritenga che esse possano essere utili per l'avvio o lo svolgimento di indagini o procedimenti relativi a reati oggetto della Convenzione o ad una richiesta di mutua assistenza (art. 26).

Oltre a quelli previsti dalla legislazione della Parte richiesta o dai trattati di mutua assistenza applicabili, tra cui la doppia incriminazione (art. 25, par. 4)[499], sono espressamente previsti quale motivo di rifiuto il fatto che la domanda di assistenza riguardi un reato che lo Stato richiesto considera politico o connesso ad un reato politico e il caso in cui l'esecuzione della richiesta possa recare pregiudizio alla sovranità, sicurezza, ordine pubblico o altri interessi essenziali dello Stato (art. 27, par. 4). È inoltre possibile sospendere l'esecuzione di una richiesta se la stessa possa pregiudicare indagini o procedimenti in corso nello Stato ricevente (art. 27, par. 5)[500].

Quanto all'oggetto della domanda di mutua assistenza, si può chiedere l'adozione di misure provvisorie (artt. 29 e 30) o lo svolgimento di indagini (artt. 31-34).

Tra le misure provvisorie rientra in primo luogo la conservazione rapida di dati informatici immagazzinati attraverso un sistema informatico – c.d. *expedite preservation of computer data* (art. 29)[501]. Si tratta di una misura, che va mantenuta per un massimo di sessanta giorni, prodromica all'eventuale successiva richiesta di perquisizione, sequestro o analoghi mezzi di ricerca della prova, nonché della divulgazione dei dati. Tale richiesta deve indicare l'autorità che richiede la conservazione, il reato che costituisce oggetto di indagine e una breve esposizione dei fatti relativi, i dati informatici immagazzinati da conservare e il loro legame con

[499] Non è però consentito alla Parte richiesta rifiutare la cooperazione in relazione ai reati elencati agli artt. 2-11 della Convenzione (accesso illegale ad un sistema informatico, intercettazione abusiva, attentato all'integrità dei dati, attentato all'integrità di un sistema, abuso di apparecchiature, falsificazione informatica, frode informatica, pedopornografia, reati contro la proprietà intellettuale e diritti collegati), qualora nell'ordinamento interno essi costituiscano illeciti di natura fiscale (art. 25, par. 4).

[500] Sia nel caso di rifiuto che di sospensione, lo Stato richiesto deve preliminarmente verificare se non sia possibile subordinare l'esecuzione della richiesta a determinate condizioni che ritenga necessarie (art. 27, par. 6).

[501] La legge 48/2008 di ratifica della Convenzione di Budapest ha inserito il comma 4 *ter* nell'art. 132 codice *privacy* che consente per l'appunto il c.d. *data freezing*. Vedi *supra*, capitolo II, par. 7.3.

il reato, tutte le informazioni utili ad identificare il custode dei dati informatici immagazzinati o il luogo dove si trova il sistema informatico, la necessità della conservazione e il fatto che lo Stato richiedente intenda successivamente presentare una richiesta di mutua assistenza per la conduzione di una perquisizione, un sequestro o di altro mezzo di ricerca della prova (art. 27, par. 2).

In secondo luogo, se nel corso di una richiesta effettuata sulla base dell'art. 29 per conservare i dati relativi ad una specifica comunicazione, la Parte richiesta scopra che un *service provider* di un altro Stato sia coinvolto nella trasmissione della comunicazione, deve procedere alla c.d. *expedite disclosure of preserved traffic data*, ossia alla trasmissione dei dati di traffico relativi a tale comunicazione, al fine di consentire alla Parte richiedente di identificare, e quindi localizzare, il *service provider* e la via attraverso la quale la comunicazione è stata effettuata, per il successivo inoltro di un'ulteriore richiesta di assistenza giudiziaria (art. 30).

Tra le attività d'indagine, vengono in rilievo la richiesta di assistenza finalizzata alla perquisizione, al sequestro o alla divulgazione di dati immagazzinati in un sistema informatico, inclusi i dati conservati in base all'art. 29 (art. 31), l'accesso diretto – ossia senza autorizzazione - a dati contenuti in un sistema informatico situato nel territorio di un altro Stato, con il consenso della persona legalmente autorizzata a divulgare i dati, o se pubblicamente disponibili – *blog*, *twitter*, *forum*, *etc.* - (art. 32), la richiesta di assistenza per la raccolta in tempo reale di dati di traffico (art. 33), la richiesta di assistenza per la raccolta e la registrazione, in tempo reale, di comunicazioni trasmesse attraverso l'uso di un sistema informatico (art. 34).

Più di un decennio è passato dall'adozione della Convenzione *Cybercrime*, e il contesto tecnologico è mutato. Sono stati messi a punto nuovi dispositivi quali *smartphones* e *tablets*; è aumentata la quantità di dati spesso salvati contestualmente in *luoghi* diversi o in *non luoghi*, come il *cyberspace*; cancellare o spostare i dati digitali da un *server* ad un altro, o un sito *web* o un *URL* contente dati illegali da un *IP* ad un altro è ormai questione di pochi secondi, i dati sono estremamente volatili. Nella *cyber-society* concetti tradizionali quali sovranità, territorio, giurisdizione diventano più sfumati, fino a perdere la loro tradizionale funzione di principi fondamentali nell'ambito della cooperazione internazionale in materia penale. Nel

mondo del *Web* 2.0 si assiste a quella che è stata efficacemente definita una "*loss of location*"[502], una perdita della dimensione fisica: i dati, e quindi le prove di un qualsiasi reato, sono dislocati nel *web*, in *luoghi* che appartengono a diverse giurisdizioni, o addirittura sono in continuo movimento tra un *luogo* ed un altro, tra una giurisdizione ed un'altra. Contestualmente, è divenuto tecnologicamente possibile accedere direttamente ai dati salvati nel *web*, ovunque essi si trovino, senza bisogno di inviare una formale richiesta di assistenza giudiziaria. Evidenti sono i riflessi di una simile evenienza in tema di *data protection*[503] e tutela dei diritti fondamentali in generale.

Se molte delle disposizioni della Convenzione *Cybercrime*, grazie alla loro formulazione «tecnologicamente neutra»[504], ben si adattano al contesto odierno, altre, e in particolare l'art. 32 sull'accesso transfrontaliero diretto ai dati informatici, presentano dei limiti.

2.1 L'accesso transfrontaliero diretto a dati informatici

Già all'epoca dei negoziati della Convenzione di Budapest si avvertiva da un lato l'esigenza di permettere anche l'accesso diretto ai dati informatici oltre i confini territoriali di ciascuna giurisdizione, dall'altro si comprendevano gli effetti che simile previsione poteva avere sui tradizionali principi di cooperazione giudiziaria in materia penale. Tuttavia, il contesto tecnologico non era tale da far apparire come urgente la messa a punto di una disciplina di dettaglio in questo particolare settore e ci si è quindi accontentati di una norma di compromesso quale l'art. 32. Lungimirante, la relazione esplicativa lascia tuttavia aperta la strada a modifiche di codesta disposizione, stabilendo che ipotesi di accesso transfrontaliero diverse da quelle previste dall'art. 32 «non sono né autorizzate, né precluse» e che «le Parti si impegnano a discutere ulteriormente e prendere in considerazione situazioni diverse

[502] *Discussion Paper "Cloud Computing and Cybercrime Investigations"*, cit.
[503] A livello di Unione europea si sta cercando di armonizzare le disposizioni in materia di tutela dei dati personali e di *data retention*, con risultati ancora insoddisfacenti. *Infra*, par. 4.1
[504] A. SEGER, *The Budapest Convention 10 Years on: lessons learnt*, in S. MANACORDA, R. FLOR, J. OH JANG (a cura di), *Cybercriminality: Finding a Balance between Freedom and Security*, ISPAC, Milano, 2012, p. 167 ss., in particolare, p. 170.

da quelle disciplinate dall'art. 32 in un momento successivo, quando avranno ottenuto più informazioni e avranno più esperienza»[505].

Su tale base, la Commissione per la Convenzione *Cybercrime* (T-CY) ha investito un'apposita sub-commissione (ad-hoc *sub-group of the T-CY on jurisdiction and transborder access to data and data flows* - c.d. *"Transborder Group"*) del compito di esaminare l'uso che viene fatto dell'art. 32 in particolare e delle investigazioni transfrontaliere in *Internet* in generale, nonché le sfide che queste ultime pongono alle tradizionali regole in materia di cooperazione giudiziaria[506]. Occorre, infatti, trovare delle soluzioni condivise affinché l'autorità giudiziaria possa accedere e acquisire dati volatili, instabili e dislocati in differenti giurisdizioni.

Preso atto della circostanza che molti Stati utilizzano l'accesso transfrontaliero diretto ai dati informatici, anche oltre le limitate possibilità riconosciute dall'art. 32 della Convenzione[507], il *Transborder Group* ha individuato quattro possibili strade da percorrere per far fronte a tale situazione: una modifica dell'art. 32, lett. b)[508], una raccomandazione del Comitato dei ministri del Consiglio d'Europa[509], fornire un'interpretazione autentica della Convenzione (sia sotto forma di un formale accordo di interpretazione, che nella veste di linee guida), oppure adottare un protocollo addizionale. Tra esse, la sotto-commissione ritiene percorribili le ultime due[510].

---

[505] Par. 293 Relazione esplicativa della Convenzione di Budapest.

[506] Le relazioni delle attività di tale sub-commissione sono reperibili all'indirizzo *www.coe.int*. La sub commissione è stata formalmente istituita nella VI sessione plenaria della Commissione per la Convenzione *Cybercrime* del 23-24 novembre 2011. L'originario mandato si esauriva il 31 dicembre 2012. Esso è stata prorogato una prima volta fino al 31 dicembre 2013 e una seconda fino al 31 dicembre 2015 per permettere al *Transborder Group* di presentare le sue proposte di modifica alla Convenzione.

[507] Lo studio condotto dalla sotto-commissione ha dimostrato che in molti Stati gli investigatori accedono direttamente ai dati salvati nel *cyberspace*, senza preoccuparsi prima di localizzarli. E che alcuni tra essi procedono all'accesso diretto, senza prima ottenere il consenso, come richiederebbe l'art. 32, lett. b), anche se sanno dove i dati si trovino. Lo studio si basa sulle risposte pervenute da diciotto Stati Parte della Convenzione (Bosnia Erzegovina, Cile, Cipro, Repubblica Ceca, Finlandia, Estonia, Germania, Ungheria, Giappone, Lituania, Moldavia, Montenegro, Norvegia, Portogallo, Polonia, Svezia, Turchia, Stati Uniti d'America). Cfr. *Report of the Transborder Group, adopted by the T-CY on 6 December 2012, Transborder Access and Jurisdiction: which are the options?*, reperibile all'indirizzo *http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf*.

[508] Lo svantaggio di simile soluzione sarebbe che la nuova disposizione avrebbe efficacia vincolante per gli Stati parte solo dopo che tutti l'abbiano ratificata. E tale procedimento potrebbe durare anni.

[509] Si tratterebbe di un atto di *soft law* e quindi di limitata portata vincolante.

[510] *Report of the Transborder Group*, cit.

In un successivo documento del 5 novembre 2013[511] sono contenute le linee guida per l'interpretazione dell'art. 32. Mentre l'ipotesi di cui alla lettera a) – accesso transfrontaliero diretto a dati disponibili pubblicamente, c.d. *open content* – non presenta, secondo la sotto commissione, difficoltà interpretative né dà luogo a problemi di utilizzo, quella di cui alla lettera b) – accesso con il consenso della persona che può disporre dei dati – merita alcune puntualizzazioni. Innanzitutto si precisa che l'accesso transfrontaliero diretto, ossia senza una formale richiesta di assistenza giudiziaria, ai dati informatici di cui all'art. 32 lett. b) presuppone che sia noto il luogo in cui essi si trovano. Non è poi necessario notificare lo Stato-sede dei dati dell'avvenuto accesso, anche se nulla vieta di farlo. Inoltre, viene chiarito che la procedura e le garanzie applicabili all'attività investigativa in questione sono quelle vigenti nello Stato procedente. Infine, per quanto riguarda la persona autorizzata a divulgare i dati, potrà trattarsi sia di una persona fisica – ad esempio il titolare di una casella di posta elettronica – sia di una persona giuridica. Tra queste ultime la sotto-commissione non ritiene rientrino gli *Internet Service Providers*, in quanto non sono «legalmente autorizzati a divulgare i dati degli utenti» secondo quanto richiede l'art. 32 lett. b). I *service providers* sono quindi tenuti a fornire i dati richiesti (generalmente si tratterà di *traffic data*, *network data* o dati di registrazione degli utenti, e non di *content data*) dall'autorità giudiziaria dello Stato in cui hanno sede o nell'ambito di una formale richiesta di assistenza giudiziaria.

Alla luce di tale interpretazione dell'art. 32, la sub-commissione ritiene quindi necessario adottare un protocollo addizionale per fronteggiare, tra le altre, quelle situazioni in cui non si sa dove si trovino i dati da acquisire. Il Protocollo verrà messo a punto nel corso del biennio 2014-2015. La sotto commissione ha anticipato quali saranno le possibili soluzioni: introdurre una disposizione che consenta di accedere direttamente ai dati con il consenso della persona che può divulgarli, anche se non si sa dove essi si trovino; prevedere l'accesso diretto senza bisogno di alcun consenso, ma attraverso credenziali legittimamente ottenute; consentire l'accesso diretto senza consenso in presenza di situazioni d'urgenza; modificare l'art. 19, par. 2 della Convenzione in modo da permettere di estendere la

[511] *T-CY Guidance Note # 3. Transborder Access to Data (article 32)*, reperibile all'indirizzo *http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY(2013)7REV_GN3_transborder_V11.pdf*.

perquisizione informatica ivi disciplinata anche a dati che si trovino in sistemi informatici al di fuori del territorio nazionale[512]; basare la cooperazione nel contesto del *cloud computing* non più sul principio di territorialità, ma su quello del "potere di disposizione dei dati"[513].

3. Cooperazione giudiziaria nell'ambito dell'Unione europea: mutuo riconoscimento vs. *armonizzazione?*

La cooperazione giudiziaria penale e di polizia non faceva parte delle aspirazioni e delle politiche della Comunità europea, originariamente rivolte alla liberalizzazione del mercato interno e all'integrazione economica; solo con il Trattato di Maastricht (entrato in vigore nel 1993) la materia della cooperazione giudiziaria penale è divenuta uno degli obiettivi della neonata Unione europea nell'ambito del più ampio settore Giustizia e Affari Interni (GAI). Tale settore - c.d. Terzo Pilastro - è entrato a far parte del quadro istituzionale dell'Unione, ma a differenza delle materie costituenti il Primo Pilastro, tipicamente disciplinate secondo il più avanzato e coeso metodo comunitario, esso è rimasto prevalentemente sottoposto al metodo intergovernativo, assieme al Secondo Pilastro (Politica Estera e di Sicurezza Comune – PESC). Coerentemente, lo strumento principalmente utilizzato dagli Stati membri in questo settore era quello delle convenzioni, attraverso cui, innanzitutto, si è dato impulso alla cooperazione di stampo tradizionale[514], inoltre si sono intraprese iniziative di armonizzazione delle legislazioni penali sostanziali[515].

È stato necessario attendere il Trattato di Amsterdam (sottoscritto nel 1997, ma entrato in vigore nel 1999), affinché l'azione comune dell'Unione nell'ambito del

[512] L'art. 19, par. 2 consente, infatti, l'estensione di una perquisizione informatica ad un altro sistema informatico o parte di esso, purché presente nel proprio territorio, se vi sia motivo di ritenere che esso contenta i dati ricercati.

[513] Cfr. *Report for the Transborder Group for 2013*, reperibile all'indirizzo *http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)30_Final_transb_rep_V5.pdf*.

[514] Convenzione in materia di estradizione semplificata tra gli Stati membri dell'Unione europea del 10 marzo 1995; Convenzione relativa all'estradizione tra gli Stati membri dell'Unione europea del 27 settembre 1996 (entrambe integratrici della Convenzione del Consiglio d'Europa del 1957 e della Convenzione applicativa degli accordi di Schengen del 1985 e del 19 giugno 1990).

[515] Convenzione sull'incriminazione delle condotte di frode comportanti un danno per il bilancio comunitario del 1995; Convenzione sull'obbligo di incriminare gli atti di corruzione in cui siano coinvolti funzionari comunitari o di un altro Stato membro del 1997.

Terzo Pilastro fosse indirizzata verso un obiettivo finale: la realizzazione dello Spazio di Libertà Sicurezza e Giustizia (SLSG)[516]. Contestualmente si individuava nella decisione-quadro lo strumento normativo più adeguato al raggiungimento di tale obiettivo.[517]

Fin dalla sua nascita l'area Giustizia Affari Interni è stata caratterizzata dall'adozione di strumenti volti a rafforzare la cooperazione giudiziaria penale e di polizia attraverso lo scambio di informazioni, dati e persone in assenza di un previo rafforzamento dei diritti. Ciò era coerente con l'essenza stessa della cooperazione che, in quanto relazione tra Stati, mirava a realizzare in via primaria gli interessi di questi ultimi, ponendo in secondo piano la questione delle garanzie, connesse ad interessi dei singoli. In quest'ottica, lo stesso anno di entrata in vigore del Trattato di Amsterdam, nell'ambito del Consiglio europeo riunitosi a Tampere, si individuava nel reciproco riconoscimento delle decisioni il principio e lo strumento concettuale per realizzare più velocemente lo SLSG[518]. Il principio del mutuo riconoscimento è nato nel contesto del mercato comune, la sua origine si fa tradizionalmente risalire alla nota sentenza *Cassis de Dijon* del 1979 della Corte di Giustizia[519]. La

[516] L'art. 2 comma 1, 4° trattino TUE stabilisce che l'Unione assume come proprio obiettivo quello di «conservar(si) e sviluppar(si) […] quale spazio di libertà, sicurezza e giustizia in cui sia assicurata la libera circolazione delle persone insieme a misure appropriate per quanto concerne i controlli alle frontiere esterne, l'asilo, l'immigrazione, la prevenzione della criminalità e la lotta contro quest'ultima».

[517] Inoltre, la Corte di Giustizia assumeva un ruolo più significativo, acquistando la competenza (se gli Stati membri la accettavano) a pronunciarsi in via pregiudiziale sulla validità o l'interpretazione delle decisioni-quadro e delle decisioni, delle convenzioni stipulate nel quadro della cooperazione di polizia e giudiziaria penale e delle misure di applicazione delle stesse. La Commissione a sua volta acquistava un potere di iniziativa concorrente e il Parlamento il diritto ad una consultazione sistematica su ogni proposta normativa, pur senza alcun potere di co-decisione.

[518] Il principio viene introdotto per la prima volta nell'ambito del Consiglio europeo di Cardiff del 15 e 16 giugno 1998. Come messo in luce dalla vice Presidente della Commissione europea, Viviane Reding, nel suo intervento al convegno organizzato dalla *European Criminal Policy Initiative* di presentazione del *Manifesto on European Criminal Procedure Law*, la situazione europea pre-Lisbona può essere raffigurata come una dea Giustizia con due spade e nessuna bilancia: l'attenzione del legislatore europeo era infatti incentrata principalmente sulla sicurezza, mentre i diritti fondamentali rimanevano nell'ombra. Il primo frutto di questa nuova politica dell'Unione europea nell'ambito del Terzo Pilastro è stata la decisione-quadro 2002/584/GAI sul Mandato d'Arresto Europeo (MAE), che ha dato ottima prova di sé nell'applicazione pratica, pur sollevando una serie di interrogativi sul piano più strettamente giuridico (Cfr. *ex plurimis*, M. FICHERA, *The implementation of the European Arrest Warrant in the European Union: law, policy and practice*, Antwerpen-Oxford, 2011). Sul versante della circolazione probatoria, il principio del mutuo riconoscimento è alla base della decisione quadro 2008/978/GAI sul Mandato Europeo di Ricerca della Prova (MERP).

[519] CGCE, sentenza 20 febbraio 1979, *Rewe Zentral AG*, C-120/78. In verità, l'espressione mutuo riconoscimento compariva già nel testo del Trattato di Roma, anche se in termini limitati e non sovrapponibili a quelli di matrice giurisprudenziale. Il riferimento è all'art. 57 TCEE (ora art. 53 TFUE) sull'adozione di direttive per favorire il mutuo riconoscimento dei diplomi, certificati e altri

trasposizione di tale principio in ambito penale presenta, tuttavia, delle criticità legate da un lato al fatto che si tratta di una materia su cui gli Stati conservano gelosamente la propria sovranità, dall'altro al rapporto con i diritti fondamentali. Infatti, nella sua applicazione originaria, il mutuo riconoscimento intende facilitare le interazioni tra Stati, generando in capo agli individui delle situazioni soggettive attive. Diversamente, nello Spazio di Libertà, Sicurezza e Giustizia, la circolazione delle decisioni giudiziarie, al fine di agevolare i rapporti tra autorità di *law enforcement,* si traduce in una ulteriore restrizione dei diritti dell'individuo, che vengono limitati secondo regole e procedure diverse[520].

Presupposto del mutuo riconoscimento è la fiducia reciproca tra gli Stati membri dell'Unione, che in ambito penale si traduce nella fiducia nella capacità degli Stati membri di tutelare i diritti fondamentali nell'esercizio dei propri poteri coercitivi. Tale fiducia reciproca, tuttavia, nel settore del processo penale non è un dato acquisito, ma un obiettivo da raggiungere: a tal fine occorre muovere dall'armonizzazione delle legislazioni nazionali[521]. Il rapporto tra fiducia reciproca, mutuo riconoscimento e armonizzazione non è pacifico. Infatti, il mutuo riconoscimento è stato concepito all'inizio come un'alternativa all'armonizzazione delle decisioni nazionali e questa è stata la ragione del suo successo; si pensava che potesse agevolare la cooperazione, senza bisogno di adottare previamente strumenti di ravvicinamento delle disposizioni nazionali[522]. E che, anzi, la libera circolazione delle decisioni giudiziarie, potesse favorire l'armonizzazione.

---

titoli per l'accesso e l'esercizio di attività non salariate, e all'art. 220 TCEE (ora abrogato) che prevedeva la negoziazione di accordi tra Stati membri per facilitare il mutuo riconoscimento delle società e delle persone giuridiche.

[520] Cfr. A. KLIP, *European Criminal Law*, Antwerpen-Oxford 2009, p. 352.

[521] 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. 700 ss. Cfr. G. ILLUMINATI, *L'armonizzazione della prova penale nell'Unione Europea,* in G. ILLUMINATI (a cura di), *Prova penale e Unione europea*, Bologna, 2009, p. 9 ss.

[522] Osserva correttamente G. MELILLO, *Il mutuo riconoscimento e la circolazione della prova*, in *Cass. pen.*, 2006, p. 265 ss., che «in generale, il principio del mutuo riconoscimento postula un certo grado di armonizzazione delle legislazioni sostanziali e processuali, ma, nel contempo, si presta ad essere utilizzato anche in mancanza di tale condizione e può persino rendere inutile un'armonizzazione degli ordinamenti nazionali. Una sorta di coperta di Linus in grado di placare l'ansia derivante dalle difficoltà irrisolte». Similmente, S. ALLEGREZZA, *L'armonizzazione della prova penale alla luce del Trattato di Lisbona*, in G. ILLUMINATI (a cura di), *Prova penale e Unione* europea, cit., p. 167, secondo cui «Tale politica criminale privilegia l'imposizione di un risultato – il riconoscimento di un atto normativo formato da uno Stato estero – rispetto all'elaborazione di un'ideologia condivisa. È una classica espressione del metodo funzionalista, da sempre adottato in seno all'UE, che implica,

Al contrario, la mancanza di una previa armonizzazione ha due aspetti negativi: da un lato rischia di costituire un ostacolo alla cooperazione, con effetti negativi sulla fiducia reciproca[523]. Dall'altro, l'obbligo di adottare un atto formato in un altro Stato membro, a prescindere da come si sia formato, può comportare un livellamento verso il basso delle garanzie, e quindi una minor tutela dei diritti fondamentali della persona[524].

Le criticità legate al mutuo riconoscimento si acuiscono in ambito probatorio, dove la mancanza di armonizzazione fa sì che tale principio vada ad alterare il difficile equilibrio che ogni ordinamento traccia nel rapporto tra esigenze investigative e diritti fondamentali della persona[525]. Infatti, come già messo in evidenza, le disposizioni processuali relative ai mezzi di ricerca della prova sono concepite in ogni ordinamento come eccezione ai diritti e alle libertà iscritti nel testo costituzionale. E i presupposti che rendono legittima simile eccezione variano da Stato a Stato. Il mutuo riconoscimento fa sì che la decisione di adottare un determinato mezzo di ricerca della prova, presa nello Stato A in base alle proprie regole, venga eseguita nello Stato B, seguendo la procedura ivi vigente per l'espletamento di quella misura investigativa. Pertanto, i diritti fondamentali della persona – in ipotesi anche lo stesso diritto - vengono limitati in base a regole e presupposti diversi a seconda dello Stato in cui viene posta in essere l'attività investigativa, o parte di essa, dando vita ad un quadro probatorio *patchwork*, con possibili riflessi negativi anche in tema di ammissibilità delle prove.

---

quali ineludibili corollari, la frammentarietà e l'instabilità della giustizia penale europea». Si veda anche K. LIGETI, *The European Public Prosecutor's Office: How Should the Rules Applicable to its Procedure be Determined?*, in *EuCLR*, 2011, p. 123 ss., in particolare p. 135.

[523] Costringere uno Stata a dare attuazione ad una decisione che sente estranea per le regole che ne hanno retto la genesi, non può che portare ad una «crisi di rigetto». Così, S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento*, cit., p. 712.

[524] *Ibidem*, p. 712.

[525] S. GLESS, *Mutual Recognition, Judicial Inquiries, Due Process and Fundamental Rights*, in J. A. E. VERVAELE (a cura di), *European Evidence Warrant. Transnational Judicial Inquiries in the EU*, Antwerpen-Oxford, 2005, p. 121 ss., sottolinea come le regole di acquisizione e ammissibilità delle prove siano una specifica conseguenza delle caratteristiche di un determinato ordinamento e varino da Stato a Stato. Per questo motivo l'Autrice si mostra scettica sul funzionamento del principio del «mutuo riconoscimento delle prove». Infatti, «il mutuo riconoscimento può dare buoni frutti con riferimento a decisioni "finali", come le sentenze, mentre le decisioni che riguardano le prove – la loro acquisizione, utilizzabilità, ammissibilità – sono parte di un procedimento penale in corso, disciplinate da un complesso e delicato sistema di *checks and balances*. […] La validità di un sistema processuale può essere valutata solo nel suo complesso, e non con riferimento a sue singole sequenze».

Al pari dell'accesso diretto transfrontaliero a dati informatici, quindi, strumenti di cooperazione fondati sul mutuo riconoscimento potrebbero tradursi in una diminuzione delle garanzie individuali e in una violazione dei diritti fondamentali dei soggetti coinvolti in un procedimento penale con dimensione transnazionale[526].

La svolta securitaria che ha caratterizzato la politica dell'Unione europea dopo gli attentati terroristici dell'11 settembre 2001 e quelli di Madrid e Londra, rispettivamente del 2004 e 2005 ha accentuato lo squilibrio tra cooperazione e tutela dei diritti fondamentali. Un primo passo in direzione di un riequilibrio delle due anime della cooperazione – sicurezza e garanzie individuali – è stato fatto con il Programma dell'Aia del 2004 in cui si sottolineava l'importanza di una previa armonizzazione delle discipline nazionali, quale presupposto del mutuo riconoscimento e della libera circolazione e la necessità che il rafforzamento della sicurezza andasse di pari passo con il rafforzamento dei diritti fondamentali garantiti dalla CEDU e dalla Carta di Nizza[527].

Dopo il tentativo, naufragato per la mancata ratifica da parte di Francia e Olanda, di realizzare una Costituzione per l'Europa, l'obiettivo, tra gli altri, di migliorare il settore della cooperazione giudiziaria penale e di polizia attraverso l'abolizione del sistema a pilastri è stato perseguito dal Trattato di Lisbona. Quest'ultimo individua proprio nel principio del mutuo riconoscimento delle sentenze e delle decisioni giudiziarie il fondamento della cooperazione giudiziaria in materia penale, precisando che essa include il ravvicinamento delle legislazioni nazionali (armonizzazione). A tal fine, il Parlamento e il Consiglio possono adottare,

[526] La richiesta di una limitazione del mutuo riconoscimento, a favore di una maggiore armonizzazione è contenuta anche nel *Manifesto on European Criminal Procedure Law*, elaborato dalla *European Criminal Policy Initiative*. L'efficienza di procedimenti penali transfrontalieri, al soddisfacimento della quale è preordinato il muto riconoscimento, non è infatti assoluta, ma deve essere bilanciata, alla luce del principio di proporzionalità, con la tutela dei diritti dell'individuo, in primo luogo dell'accusato, ma anche quelli della vittima e di soggetti terzi rispetto al processo, dell'identità nazionale e dell'ordine pubblico degli Stati membri. Il Manifesto è pubblicato sul *Zeitschrift für internationale Strafrechtsdogmatik*, n. 11/2013, reperibile all'indirizzo *www.zis-online.com*. Inoltre, il principio del mutuo riconoscimento sfida il tradizionale concetto di sovranità territoriale: infatti, in mancanza di armonizzazione non c'è una base per giustificare l'effetto extra-territoriale delle decisioni giudiziarie straniere. Così, F. ZIMMERMANN, S. GLASER, A. MOTZ, *Mutual Recognition and its Implications for the Gathering of Evidence in Criminal Proceedings: a Critical Analysis of the Initiative for a European Investigation Order*, in *EuCLR*, 2011, p. 56 ss., in particolare p. 65.

[527] Il Programma dell'Aia è pubblicato in *GUUE* del 3 marzo 2005, C 53/1.

tramite direttiva, norme minime volte tra l'altro a garantire l'ammissibilità reciproca delle prove tra Stati membri (art. 82, par. 2 TFUE).

Allo stato attuale, il quadro degli strumenti esistenti a livello di Unione europea in materia di cooperazione investigativa si rivela ampiamente insoddisfacente[528], soprattutto con riferimento alle indagini informatiche, e le relazioni tra gli Stati Membri sono ancora in prevalenza affidate al complesso meccanismo delle rogatorie (salva l'applicabilità della Convenzione di Budapest)[529]. Infatti, la Convenzione sull'assistenza giudiziaria di Bruxelles del 2000, che disciplina le intercettazioni transfrontaliere[530], e che include anche le comunicazioni

[528] Cfr. J. R. SPENCER, *The problems of Trans-border Evidence and European Initiatives to Resolve Them*, in G. GRASSO, R. SICURELLA (a cura di), *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, Milano, 2008, p. 471 ss.

[529] Più avanzato appare il panorama degli strumenti europei sul versante della c.d. cooperazione informativa, ossia dello scambio di informazioni tra le autorità di *law enforcement*. La cooperazione informativa si compone di due profili, uno statico e uno dinamico, il primo costituisce il necessario presupposto del secondo. Infatti, il profilo statico realizza il canone di conservazione, prodromico ad ogni attività di successivo scambio; esso non mira tanto a tutelare i dati personali, quanto ad imporre agli Stati obblighi di conservazione ai fini della successiva circolazione dei dati, serve quindi a creare quell'armonizzazione che è presupposta dal principio del mutuo riconoscimento. Il profilo dinamico, in ossequio al mutuo riconoscimento, attua la libera circolazione secondo il principio di disponibilità e accessibilità delle informazioni. Sono state quindi create diverse banche dati a cui le autorità di *law enforcement* possono accedere per lo svolgimento di attività di *intelligence* e di repressione dei reati. Il riferimento è ai sistemi informativi *SIS* e *SIRENE* (nell'ambito del sistema informativo Schengen), *VIS* (*Visa Information System*), *CIS* (*Custom Information System*), *EURODAC* (*European Dactylographic System*), *ECRIS* (*European Criminal Records Information System*), nonché a quelli sviluppati nell'ambito di *Eurojust* e *Olaf*. Sul piano dinamico, si segnalano la decisione quadro 2006/960/GAI sull'*information sharing* (*GUUE* del 29 dicembre 2006, L 386/89), la decisione quadro 2008/615/GAI di recepimento del Trattato di Prüm sulla libera circolazione dei profili DNA, dei dati dattiloscopici e di quelli di immatricolazione dei veicoli (*GUUE* del 6 agosto 2008, L 210/1), la decisione quadro 2009/315/GAI relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario (*GUUE* del 7 aprile 2009, L 93/23). In argomento si veda G. DI PAOLO, *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in *Cass. pen.*, 2010, p. 1969 ss.; F. PERONI, M. GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell'Unione Europea*, Trieste, 2009.

[530] La Convenzione, oltre all'ipotesi classica in cui uno Stato intenda intercettare una persona che si trova all'estero, senza averne le capacità tecniche e deve dunque inviare una richiesta di assistenza giudiziaria a tale Stato (art. 18), prevede due ulteriori ipotesi. Innanzitutto quella in cui uno Stato abbia la possibilità tecnica di intercettare un'utenza all'estero, senza l'assistenza dello Stato straniero. Inoltre, il caso in cui uno Stato membro necessiti dell'assistenza di un altro Stato membro per intercettare comunicazioni sul proprio territorio nazionale (questo è il caso delle comunicazioni satellitari che possono essere intercettate solo attraverso *gateways* dedicati, che non tutti gli Stati possiedono). In quest'ultima ipotesi, la Convenzione prevede che lo Stato che non possiede tale *gateway* possa ottenere l'autorizzazione all'intercettazione senza particolari formalità. Inoltre è prevista la possibilità di ottenere un'autorizzazione "permanente" ad intercettare: in questo modo il *service provider* di un Paese può accedere al *gateway* presente sul territorio straniero, senza dover chiedere l'autorizzazione di volta in volta (art. 19). Per quanto riguarda infine l'ipotesi in cui lo Stato abbia la capacità tecnica di intercettare oltre confine, dispone l'art. 20 che tale pratica è consentita a condizione che lo Stato in cui si trova la persona le cui comunicazioni sono intercettate, sia informato prima dell'inizio delle operazioni, o non appena lo Stato intercettante diviene consapevole che il

via *Internet*[531] e secondo taluno anche l'acquisizione dei tabulati[532], non è ancora entrata in vigore per la mancata ratifica di tutti di Stati che vi hanno aderito, tra cui l'Italia. Mentre la decisione quadro sul Mandato Europeo di Ricerca della Prova, che pur non è stata ancora attuata, non si applica a forme di sorveglianza in tempo reale, né all'acquisizione di dati di traffico telefonico o telematico[533].

La situazione potrebbe mutare con l'approvazione della proposta di direttiva per un Ordine Europeo di Indagine Penale (OIE), basato sul principio del mutuo riconoscimento, e con l'istituzione di un Pubblico Ministero Europeo, dotato di autonomi poteri investigativi su tutto il territorio dell'Unione, oggi espressamente contemplata dal Trattato (art. 86 TFUE).

3.1 Le iniziative post-Lisbona: l'Ordine Europeo di Indagine Penale

Su iniziativa di alcuni Stati membri è stato proposto di introdurre un unico strumento per l'acquisizione della prova che si trovi in un altro Paese UE: l'Ordine Europeo di Indagine penale (d'ora innanzi OEI)[534]. Esso dovrebbe sostituire gli esistenti strumenti di cooperazione probatoria: la Convenzione europea sulla mutua

---

soggetto intercettato si trova in territorio straniero. La Convenzione è pubblicata in *GUUE*, 12 luglio 2000, C 197/1. In argomento si rinvia a M. PANZAVOLTA, *Intercettazioni e spazio*, cit., p. 67 ss.

[531] Così già la Relazione esplicativa della Convenzione, in *GUCE* del 29 dicembre 2000, C 379, p. 7 ss.

[532] L. SALAZAR, *La nuova convenzione sull'assistenza giudiziaria in materia penale*, in *Dir. pen. proc.*, 2000, p. 1664 ss., in particolare, p. 1667.

[533] DQ 2008/978/GAI, in *GUUE* del 30 dicembre 2008, L 350/72. Il MER è «una decisione giudiziaria [basata sul principio del mutuo riconoscimento] emessa da un'autorità giudiziaria di uno Stato membro allo scopo di acquisire oggetti, documenti e dati da un altro Stato membro [al fine di un loro utilizzo nell'ambito di un procedimento penale]» (art. 1). Esso può essere utilizzato solo per acquisire prove già esistenti, precostituite. Come anticipato, non può quindi essere emesso per l'espletamento di forme di sorveglianza in tempo reale, né per «ottenere dati sulle comunicazioni conservati dai fornitori di servizi di comunicazioni elettroniche accessibili al pubblico o di una rete pubblica di comunicazione», a meno che essi non siano «già in possesso dell'autorità di esecuzione prima dell'emissione del MER» (art. 4, §§ 2 e 4). In argomento si rinvia a G. DE AMICIS, *Limiti e prospettive del Mandato Europeo di Ricerca della Prova*, in G. GRASSO, L. PICOTTI, R. SICURELLA, *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, p. 475 ss.; J. A. E. VERVAELE, *Il progetto di decisione quadro sul mandato di ricerca della prova*, in *Prova penale e Unione Europea*, cit., p. 153 ss.; C. WILLIAMS, *Overview of the Commission's proposal for a Framework Decision on the European evidence warrant*, in J. A. E. VERVAELE (a cura di), *European Evidence Warrant. Transnational Judicial Inquiries in the EU*, Antwerpen-Oxford, 2005, p. 69 ss.

[534] La proposta per l'adozione di una direttiva riguardo all'OEI da parte del Parlamento europeo e del Consiglio è stata presentata da Belgio, Bulgaria, Estonia, Spagna, Austria, Slovenia, Svezia. In *GUUE* del 24 giugno 2010, C 165/22. Alcune modifiche sono state apportate nel corso della discussione in seno al Consiglio del 9 dicembre 2011 (18225/1/11 REV 1).

assistenza giudiziaria penale del 20 aprile 1959 (c.d. Convenzione madre) e i relativi due protocolli addizionali del 17 marzo 1978 e dell'8 novembre 2001 (oltre agli accordi bilaterali conclusi a norma dell'art. 26 di tale Convenzione), la Convenzione di applicazione degli Accordi di Schengen del 19 giungo 1990, la Convenzione sulla mutua assistenza giudiziaria in materia penale tra gli Stati membri dell'UE del 29 maggio 2000 e il relativo protocollo del 16 ottobre 2001, la decisione quadro 2003/577/GAI del 22 luglio 2003 sul congelamento dei beni da sottoporre a sequestro e confisca (limitatamente al sequestro probatorio) e la decisione quadro 2008/978/GAI sul Mandato Europeo di Ricerca della Prova[535].

L'OEI è «una decisione giudiziaria emessa da un'autorità competente di uno Stato membro (Stato di emissione) affinché siano compiuti uno o più atti di indagine specifici in un altro Stato membro (Stato di esecuzione) ai fini dell'acquisizione di prove [da utilizzare nel corso di un procedimento penale]» (art. 1). Esso si applica a tutte le misure investigative, ad eccezione dell'istituzione di squadre investigative comuni e dello svolgimento di indagini nell'ambito di tali squadre[536]. Poiché si tratta di uno strumento basato sul principio del mutuo riconoscimento, si stabilisce che l'autorità destinataria di un OEI «prend[a] immediatamente le misure necessarie per la sua esecuzione nello stesso modo e secondo le stesse modalità con cui procederebbe se l'atto d'indagine in questione fosse stato disposto da un'autorità dello Stato di esecuzione […]» (art. 8, § 1)[537]. L'OEI, come il MERP, è quindi emesso

[535] Tale iniziativa si pone quindi nel solco delle linee guida adottate dalla Commissione nel *Libro Verde* dell'11 novembre 2009 in cui si auspicava la sostituzione della vigente frammentaria disciplina in materia di ricerca e ammissibilità delle prove con un unico strumento basato sul mutuo riconoscimento ed esteso a tutti i tipi di prova. Cfr. C. HEARD, D. MANSELL, *The European Investigation Order: Changing the Face of Evidence–gathering in EU Cross-border Cases*, in *EuCLR*, 2011, p. 353 ss. A favore dell'adozione di un unico strumento per l'acquisizione delle prove nei procedimenti a dimensione transnazionale, già J. R. SPENCER, *The problems of Trans-border Evidence*, cit., p. 471 ss.

[536] L'iniziale esclusione dell'intercettazione di alcune forme di telecomunicazioni è stata eliminata nel corso delle negoziazioni in seno al Consiglio. L'OIE può quindi essere emesso anche per forme di sorveglianza continuativa e tecnologicamente assistita.

[537] L'espansione del principio del mutuo riconoscimento è massima. Vi è una drastica riduzione dei motivi di rifiuto rispetto alla decisione quadro sul MERP; essi riguardano le ipotesi di immunità, di pericolo per la sicurezza nazionale, di ricorso all'OEI al di fuori dell'ambito penale, di indisponibilità di atti di indagine ulteriori (art. 10). Inoltre, i tempi di evasione di una simile richiesta sono molto rapidi; è previsto che la decisione sul riconoscimento o sull'esecuzione venga adottata il più rapidamente possibile e comunque entro 30 giorni dalla ricezione dell'OEI e che l'atto di indagine venga compiuto entro i novanta giorni successivi. È possibile una proroga di entrambi i termini in casi specifici, previo accordo con l'Autorità emittente (art. 11). Infine, viene meno il riferimento al requisito della doppia incriminabilità. Cfr. L. PULITO, *La circolazione della prova penale in Europa dopo il Trattato di Lisbona*, in *Giust. pen.*, 2010, p. 376 ss.

secondo la legge dello Stato richiedente ed eseguito secondo quella dello Stato richiesto (*forum regit actum*). La proposta di direttiva è tuttavia apprezzabile perché, proprio per limitare il rischio di un quadro probatorio *patchwork* - e al fine di garantire la successiva ammissibilità della prova - prevede innanzitutto che l'autorità emittente possa indicare le formalità e le procedure a cui l'autorità di esecuzione deve attenersi nell'assunzione della prova, salvo che non siano contrarie ai suoi principi fondamentali (art. 8, § 2). Inoltre, si ammette la possibilità che «un'autorità competente dello Stato di emissione» partecipi all'esecuzione dell'OEI. Anche in questo caso l'autorità di esecuzione deve ottemperare alla richiesta, salvo che essa contrasti con i suoi principi fondamentali (art. 8, § 3). Il rovescio della medaglia di simili previsioni è che viene imposto alle autorità di uno Stato membro di condurre investigazioni secondo regole che non conoscono e che, in ipotesi, non appartengono alla loro tradizione giuridica[538]. Per mitigare questo possibile effetto negativo, l'art. 9 consente allo Stato di esecuzione di ricorrere ad una misura diversa da quella richiesta se «l'atto d'indagine indicato nell'OEI non è previsto dalla legislazione dello Stato di esecuzione, [se] è previsto dalla legislazione dello Stato di esecuzione ma il ricorso al medesimo è limitato ad un elenco o una categoria di reati che non comprende il reato oggetto dell'OEI, oppure se l'atto d'indagine scelto dall'autorità di esecuzione consente di ottenere lo stesso risultato dell'atto indicato nell'OEI con mezzi meno coercitivi».

La proposta per l'adozione di una direttiva relativa all'Ordine Europeo di Investigazione Penale ha il pregio di costituire un tentativo di razionalizzazione di una materia complessa e frammentaria. Tuttavia, la mancanza di una previa armonizzazione della disciplina sostanziale e processuale fa sorgere più di una perplessità sulla effettiva buona riuscita di simile strumento di cooperazione. L'eterogeneità che caratterizza le procedure di acquisizione della prova nei diversi Stati membri, soprattutto nell'ambito delle indagini informatiche, dove non vi è accordo neppure sul *se* alcune di tali tecniche interferiscano con i diritti fondamentali, costituirà alternativamente un ostacolo alla cooperazione o un

[538] Inoltre, il fatto che una misura sia, a livello domestico, legittima e rispettosa del principio di proporzionalità, non la rende automaticamente tale in un contesto transnazionale.

incentivo al c.d. *forum shopping*[539]. La proposta di direttiva non contiene alcun tentativo di individuazione di un sistema di norme comuni per la raccolta della prova e manca altresì una definizione di atto d'indagine[540]. Né viene fatto alcun riferimento alle esigenze di tutela dei dati personali. L'art. 1, § 3 stabilisce che «la direttiva non ha l'effetto di modificare l'obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti dall'articolo 6 del trattato sull'Unione europea e lascia impregiudicati gli obblighi spettanti, in materia, alle autorità giudiziarie […]». Si è già avuto modo di sottolineare come ogni Stato abbia proprie regole in materia di ricerca della prova, elaborate quale eccezione ai principi costituzionali. In mancanza di condivisione in merito ai presupposti di una limitazione legittima dei diritti fondamentali per finalità di indagine, tale norma si risolve in una petizione di principio. Occorre quindi, anche nel contesto sovranazionale, muovere dall'individuazione dei diritti fondamentali coinvolti, fissare i presupposti per una limitazione legittima da parte dell'autorità giudiziaria e individuare quantomeno uno *standard* comune – quelle «norme minime» di cui all'art. 82, par. 2 TFUE - che ogni Stato membro deve rispettare nel condurre attività di ricerca della prova.

3.2 (segue)Le Model Rules *per la futura Procura Europea*

Il tentativo di superare il principio del mutuo riconoscimento, quanto meno nell'ambito della cooperazione giudiziaria verticale, è alla base delle *Model Rules for the Procedure of the European Public Prosecutor's Office* (d'ora innanzi *Model Rules*) elaborate dall'Università del Lussemburgo[541]. Il Trattato di Lisbona fornisce infatti la base giuridica per la creazione del Pubblico Ministero Europeo (d'ora innanzi PME): ai sensi dell'art. 86 TFUE «per combattere i reati che ledono gli interessi finanziari dell'Unione, il Consiglio, deliberando mediante regolamenti

[539] Intravvedono quest'ultimo pericolo F. ZIMMERMANN, S. GLASER, A. MOTZ, *Mutual Recognition*, cit., p. 73.
[540] Cfr. G. DE AMICIS, *Limiti e prospettive*, cit., p. 509.
[541] Il progetto è stato coordinato dalla Professoressa Katalin Ligeti dell'Università del Lussemburgo; hanno collaborato al progetto, in quanto membri dello *Steering Committee* il Dr. Charles Elsen, il Prof. Ulrich Sieber, il Prof. John R. Spencer, il Prof. John A. E. Vervaele e il Prof. Thomas Weigend, oltre ad un gruppo di esperti europei. Le *Model Rules* e la Relazione introduttiva della Prof. Katalin Ligeti sono disponibili all'indirizzo *http://www.eppo-project.eu/index.php/EU-model-rules* e saranno pubblicate insieme al report finale in K. LIGETI (ed.), *Toward a Prosecutor for the European Union. Draft Rules of procedure, Volume 2*, Oxford, 2013 (in corso di pubblicazione).

secondo una procedura legislativa speciale, può istituire una Procura europea a partire da Eurojust»[542].

Non è questa la sede per entrare nel merito del dibattito sul PME[543], tuttavia va fatto un cenno alle *Model Rules*, che costituiscono un primo sforzo volto ad individuare norme comuni per lo svolgimento di indagini transnazionali, e rappresentano una sintesi delle diverse tradizioni giuridiche degli Stati membri[544]. Esse, infatti, sono precedute da uno studio comparativo delle regole processuali vigenti nei diversi ordinamenti, che potrebbe agevolare il legislatore europeo nell'adottare misure volte all'armonizzazione in vista anche della cooperazione orizzontale[545]. Inoltre, il progetto prende in considerazione l'impatto sui diritti fondamentali della persona dei nuovi strumenti d'indagine che sfruttano le innovazioni tecnologiche. E proprio il grado di coercitività e intrusività del mezzo di ricerca della prova costituisce il criterio in base al quale sono state classificate le diverse misure investigative. La convinzione è che vi debba essere una necessaria proporzione tra sacrificio dei diritti del singolo e presupposti e condizioni per

[542] L'idea di istituire un Pubblico Ministero Europeo, responsabile delle indagini relative ai reati che ledono gli interessi finanziari dell'Unione risale al progetto *Corpus Juris* (prima versione del 1997, seconda del 2000, il testo e i risultati del dibattito sono raccolti in M. DELMAS-MARTY, J. A. E. VERVAELE (a cura di), *The implementation of Corpus Juris*, Antwerpen-Groenigen-Oxford, 2000, in 4 volumi; la traduzione italiana è pubblicata in G. GRASSO, R. SICURELLA, *Il Corpus juris 2000: un modello di tutela penale dei beni giuridici comunitari*, Milano, 2003), ed è stata portata avanti dalla Commissione nel Libro Verde del 2001 sulla tutela penale degli interessi finanziari comunitari e sulla creazione di una procura europea (COM (2001) 715 def.). Con il Trattato di Lisbona è stata infine introdotta la base giuridica per la creazione del Pubblico Ministero Europeo e il 17 luglio 2013 la Commissione ha presentato una proposta di Regolamento del Consiglio che istituisce la Procura europea (COM (2013) 534 def.). La «vagheggiata figura» di un pubblico ministero europeo sta quindi acquistando contorni reali; l'espressione è di R. ORLANDI*, Qualche rilievo intorno alla vagheggiata figura di un pubblico ministero europeo*, in L. PICOTTI (a cura di), *Possibilità e limiti di un diritto penale europeo*, Milano, 1999, p. 209 ss. ed è riferita alla proposta contenuta nel progetto *Corpus juris* 2000.

[543] Per una panoramica sulle possibili soluzioni istituzionali per la Procura europea, si rinvia a K. LIGETI, M. SIMONATO, *The European Public Prosecutor's Office: Towards a Truly European Prosecution Service?*, in *NJECL*, Vol. 4, Issue 1-2, 2013, p. 7 ss.

[544] Così la Relazione introduttiva alle *Model Rules*. Ciò che contraddistingue le *Model Rules* all'interno dei vari progetti che negli anni si sono susseguiti intorno alla figura del PME è che esse riguardano esclusivamente i profili procedurali del futuro PME. L'obiettivo dichiarato è quello di stimolare il dibattito su come dovranno essere regolamentati i suoi poteri di indagine e di accusa. La strada prescelta è quella più impegnativa: dotare il nuovo organismo di autonomi poteri investigativi, individuando le garanzie procedurali che dovrebbero assistere il loro compimento. Cfr. G. DI PAOLO, *Note a margine della recente proposta di istituzione di una Procura europea contenuta nelle* Model Rules for the Procedure of the European Public Prosecutor's Office, in F. RUGGIERI, T. RAFARACI, G. DI PAOLO, S. MARCOLINI, R. BELFIORE (a cura di), *Processo penale,* cit., p. 129 ss., in particolare p. 131,132.

[545] I *reports* nazionali sono pubblicati in K. LIGETI (*ed.*), *Toward a Prosecutor for the European Union. A comparative analysis*, *Volume 1*, Oxford, 2012.

l'adozione della misura, che ad un maggior grado di intrusività debbano corrispondere maggiori garanzie sul piano processuale[546]. In ciò le *Model Rules* sono tributarie della giurisprudenza della Corte Europea dei Diritti dell'Uomo.

I mezzi di ricerca della prova sono stati quindi suddivisi in tre macro categorie, caratterizzate da un progressivo grado di interferenza con i diritti fondamentali: misure investigative non coercitive, misure coercitive senza previa autorizzazione giudiziaria, misure coercitive con previa autorizzazione giudiziaria.

Innanzitutto si stabilisce che tutte le decisioni del PME che incidono sui diritti fondamentali dell'individuo sono soggette a controllo da parte della «*European Court*» (*Rule 7, § 1*)[547]. A tal fine, le misure che non necessitano della previa autorizzazione del giudice, sono disposte dal PME con provvedimento scritto e motivato (*Rule 31*). Quelle appartenenti al terzo gruppo, sono invece adottate previa autorizzazione scritta e motivata del giudice, salvo che ragioni d'urgenza non impongano di procedere immediatamente; in questo caso il provvedimento giudiziale deve intervenire nelle quarantotto ore successive (*Rule 47*). Laddove, quindi, la limitazione dei diritti fondamentali è massima, si è ritenuto opportuno richiedere un controllo *ex ante*, a livello nazionale. Spetta, infatti, a ciascuno Stato membro individuare il giudice competente a concedere la prescritta autorizzazione (*Rule 7, § 2*)[548].

Tra le misure che il PME può disporre senza autorizzazione, rientrano l'ordine di "congelamento" – *freezing* - di *stored computer data* e *stored traffic data* per un massimo di novanta giorni (*Rule 41*)[549] e la localizzazione del cellulare (*tracking and tracing*), ma solo se limitata ad una specifica occasione; se invece il controllo è prolungato – *continued surveillance* -, occorre l'autorizzazione del giudice (*Rule 45*)[550].

---

[546] Cfr. S. ALLEGREZZA, *Le misure coercitive*, cit., p. 162 e G. DI PAOLO, *Note a margine*, cit., p. 136 ss.

[547] Il riferimento non è alla Corte di Strasburgo, ma ad un organo da individuare nel quadro istituzionale dell'UE ai sensi dell'art. 257 TFUE. Così, G. DI PAOLO, *Note a margine*, cit., p. 137.

[548] Le *Model Rules* si pongono in questo ambito in linea di continuità con il *Corpus juris* che prevedeva l'istituzione di un "*judge of freedoms*" situato a livello nazionale.

[549] Si tratta di una previsione simile a quanto stabilito dagli artt. 29 e 30 della Convenzione *Cybercrime*. Si veda, *supra*, par. 2.

[550] Sembra di ravvisare in questa disposizione, che distingue i presupposti della sorveglianza a seconda della sua durata, un'eco della giurisprudenza della Corte EDU nel caso *Uzun v. Germany*. *Supra*, capitolo III, par. 2.2.

Autorizzazione che è altresì richiesta per perquisizioni di *computer* e sistemi informatici (*Rule 48*)[551], intercettazioni di telecomunicazioni, incluse le *e-mail* (*interception of telecommunication – content data*, *Rule 51*), *real-time surveillance of telecommunications traffic data* (*Rule 52*)[552]. La terza categoria di strumenti di indagine comprende quindi prevalentemente, anche se non esclusivamente, forme di sorveglianza tecnologicamente assistita, ossia mezzi di ricerca della prova di ultima generazione[553].

Delle misure investigative utilizzabili da parte del PME si occupa anche la proposta della Commissione per l'istituzione della Procura Europea[554]. L'approccio seguito è molto più cauto di quello espresso nelle *Model Rules*; si rinuncia infatti ad una disciplina uniforme ed esaustiva [555].

Per ovviare alla disomogeneità in materia di misure investigative di nuova generazione che caratterizza gli Stati membri, la proposta di regolamento fa un elenco di strumenti d'indagine di cui può avvalersi il Procuratore Europeo (art. 26). Tale previsione obbliga gli Stati membri ad introdurre nell'ordinamento interno,

[551] Il paragrafo 2 prevede la possibilità di estendere la perquisizione ad un altro sistema informatico o parte di esso, se il PME ha ragione di ritenere che ivi si trovino i dati ricercati, a condizione che l'accesso a tali dati sia legittimo a partire dal sistema originariamente perquisito. Tale previsione è simile a quella contenuta nell'art. 19, § 2 della Convenzione *Cybercrime*; tuttavia, non contiene un'analoga restrizione ai soli sistemi informatici che si trovino nel territorio nazionale della possibilità di estendere la perquisizione. Ai sensi della *Rule 2* l'ambito di competenza del PME si estende a tutto il territorio dell'Unione; probabilmente quindi il potere di estensione riguarda solo sistemi informatici che si trovino nell'ambito dell'UE. Si pone pertanto il problema di quali regole seguire se, cosa molto probabile, i dati siano salvati su un *server* extra-europeo.

[552] A differenza dei *traffic data*, già conservati dai fornitori di servizi di telecomunicazione, acquisibili ai sensi della *Rule 41*, in questo caso i *traffic data* sono acquisiti in tempo reale.

[553] Oltre a quelle menzionate, rientrano in tale gruppo le seguenti misure investigative: le perquisizioni "classiche" (*Rule 48*), gli accertamenti corporali sull'imputato, compresi i prelievi biologici coattivi (*Rule 49*), l'ordine di produzione di documenti, dati e oggetti rilevanti per le indagini, anche se salvati in *computer* o criptati (*Rule 50*), le riprese investigative in luoghi non pubblici (*Rule 53*), il controllo in tempo reale delle transazioni finanziarie (*Rule 55*), con possibilità di blocco fino ad un massimo di cinque giorni (*Rule 56*) e le indagini sotto copertura (*Rule 57*).

[554] COM (2013) 534 def.

[555] Così S. ALLEGREZZA, *Verso una Procura europea per tutelare gli interessi finanziari dell'Unione. Idee di ieri,* chances *di oggi, prospettive di domani*, in *www.penalecontemporaneo.it*, che rileva come la proposta non contenga una «micro-codificazione settoriale di diritto processuale»; infatti, il regolamento «non mira all'autosufficienza e ribadisce la necessità dell'integrazione costante col diritto degli Stati membri, segnatamente con il diritto dello Stato in cui si svolge l'azione o l'indagine penale. […] In nome della proporzionalità e della sussidiarietà europee, si presenta al Consiglio una proposta troppo timida e timorosa». In tal senso anche A. VENEGONI, *Considerazioni sulla normativa applicabile alle misure investigative intraprese dal Pubblico Ministero Europeo nella proposta di regolamento COM (2013) 534*, in *www.penalecontemporaneo.it,* il quale segnala che, nonostante tutto, alcuni Stati membri (in numero sufficiente a raggiungere il *quorum* richiesto dall'art. 7 del Protocollo n. 2 del TFUE per il riesame del progetto) hanno espresso critiche verso la proposta della Commissione sotto il profilo della sussidiarietà.

laddove non presenti, gli strumenti di indagine specificamente individuati, al fine di renderli disponibili per il PME (art. 26, par. 2).

Seguendo l'impostazione delle *Model Rules*, l'art. 26 prevede che alcuni strumenti di indagine (elencati alle lettere da a) a j)) debbano sempre essere autorizzati dall'autorità giudiziaria dello Stato membro in cui devono essere eseguite, a prescindere da cosa preveda la disciplina nazionale[556]. Tra questi rientrano le perquisizioni informatiche, l'ordine di produzione di *stored computer data* (inclusi gli *stored traffic data*), il *data freezing*, le intercettazioni di telecomunicazioni, la sorveglianza in tempo reale delle telecomunicazioni con ordine di immediata trasmissione dei dati di traffico al fine della localizzazione dell'indagato. Per le misure indicate alle lettere da k) a u) invece l'autorizzazione giudiziale è necessaria solo se così dispone il diritto nazionale dello Stato membro in cui devono essere eseguite; tra esse si possono ricordare, a titolo esemplificativo, il sequestro, la sorveglianza dell'indagato in luoghi pubblici e l'interrogatorio di indagati e testimoni. Tali strumenti investigativi possono essere adottati solo se l'obiettivo non sia perseguibile con mezzi meno intrusivi.

La disposizione in esame è apprezzabile, non solo perché fa chiarezza su quali siano le misure di cui può avvalersi il PME, ma soprattutto in quanto favorisce una certa armonizzazione, stimolando gli Stati membri a legiferare in settori lacunosi, come quelle delle misure di *surveillance*[557]. Per quanto riguarda, invece, le modalità di espletamento delle indagini, la proposta rinuncia ad introdurre regole comuni[558]. Ai sensi dell'art. 11, par. 3, infatti, agli aspetti non disciplinati dal regolamento si applica il diritto nazionale, in particolare quello dello Stato membro in cui la misura investigativa deve essere eseguita (principio della *lex loci*, art. 11,

[556] In questo modo, tuttavia, si corre il rischio che una stessa misura sia disposta in uno Stato membro sulla base di presupposti diversi a seconda che sia utilizzata dal PME o in un procedimento nazionale, ancorché con carattere transnazionale. Così, A. VENEGONI, *Considerazioni sulla normativa applicabile alle misure investigative*, cit., p. 9.

[557] Cfr. S. ALLEGREZZA, *Verso una Procura europea*, cit., p. 7. Anche A. VENEGONI, *Considerazioni sulla normativa applicabile alle misure investigative*, cit., p. 8 valuta positivamente questo aspetto che rappresenta «un passo avanti rispetto alla situazione attuale dove l'incertezza sull'esistenza o sulla qualificazione giuridica di una misura può essere fonte di problemi nei rapporti tra autorità giudiziarie dei vari Stati membri».

[558] Cfr. S. ALLEGREZZA, *Verso una Procura europea*, cit., p. 7, che sottolinea come ciò costituisca altresì una retrocessione rispetto a quanto previsto dalla proposta di direttiva sull'Ordine Europeo di Indagine penale.

par. 3, art. 26, par. 2)[559]. Ciò significa, verosimilmente, che una stessa attività investigativa verrà condotta secondo procedure diverse a seconda del luogo in cui deve essere svolta. Infatti, l'art. 25 della proposta, ai sensi del quale «il territorio dell'Unione rappresenta un unico spazio giuridico in cui la Procura europea può esercitare la sua competenza» (principio di territorialità europea), indica l'estensione geografica dei poteri dell'organo, ma non legittima l'uso del diritto interno oltre i confini nazionali: «è il risultato probatorio a circolare, non le regole per la sua acquisizione»[560].

Per quanto riguarda infine l'ammissibilità della prova, la proposta di regolamento prevede che il giudice «ammette le prove al processo senza necessità di convalida o altra operazione giuridica analoga, anche se il diritto nazionale dello Stato membro in cui ha sede l'organo giurisdizionale prevede norme diverse per la raccolta e la presentazione delle prove»[561].

Riemergono, quindi, le preoccupazioni, già avanzate rispetto alla proposta per l'OEI, di rischio di un procedimento c.d. *patchwork*[562], di conseguente diminuzione delle garanzie per l'indagato e di *forum shopping*.

Anche in questo caso è pertanto auspicabile che le istituzioni europee orientino la loro attività verso una maggiore armonizzazione delle discipline nazionali, adottando, tramite direttiva, quelle «norme minime» previste dall'art. 82, par. 2 TFUE.

---

[559] Questo emerge dalla traduzione italiana della proposta di regolamento che, all'art. 26, par. 2, individua l'autorità giudiziaria competente a dare la prescritta autorizzazione allo svolgimento di determinate misure investigative in quella «dello Stato membro in cui la misura deve essere eseguita». Secondo quest'interpretazione, nel caso di indagini transfrontaliere, occorrerebbe ottenere tante autorizzazioni quanti sono gli Stati in cui la misura deve essere eseguita. Tuttavia, va segnalato che l'originale versione inglese lascerebbe spazio ad una diversa interpretazione. Infatti, l'art. 26, par. 2 individua l'autorità giudiziaria competente non in quella del luogo in cui la misura «*is to be executed*», ma in quella del luogo dove la misura «*is to be carried out*», concetto più ampio che potrebbe essere inteso come luogo in cui la misura deve essere intrapresa e quindi includere anche la fase della richiesta autorizzativa. In questo caso, quindi, sarebbe sufficiente ottenere l'autorizzazione dell'autorità giudiziaria davanti a cui pende il procedimento. Resta comunque fermo il fatto che la misura verrà concretamente eseguita secondo le regole vigenti nello Stato di esecuzione – e ciò anche qualora si accogliesse l'idea che l'autorizzazione del giudice di uno Stato membro acquisti una sorta di "efficacia extra-territoriale". Per questi rilievi, si veda A. VENEGONI, *Considerazioni sulla normativa applicabile alle misure investigative*, cit., p. 9 ss.

[560] Così, S. ALLEGREZZA, *Verso una Procura europea*, cit., p. 7.

[561] Il giudice del merito è tenuto a verificare che l'ammissione delle prove presentate dal PME non pregiudichi l'imparzialità del giudice, né i diritti di difesa sanciti dagli artt. 47 e 48 della Carta dei Diritti Fondamentali dell'Unione Europea (art. 30).

[562] L'inquirente europeo raccoglie infatti atti di indagine formati secondo regole nazionali diverse. Così, S. ALLEGREZZA, *Verso una Procura europea*, cit., p. 7.

4. Quale tutela per i diritti fondamentali?

Cooperazione giudiziaria, mutuo riconoscimento, accesso diretto a dati informatici costituiscono altrettanti fattori di rischio per la protezione dei dati personali. Negli ultimi anni si è assistito ad un incremento delle attività di scambio di dati e informazioni per finalità di *intelligence* e *law enforcement*, soprattutto nell'ambito del contrasto al terrorismo internazionale e alla criminalità informatica. Nel bilanciamento tra sicurezza e riservatezza, la protezione dei dati è stata spesso erroneamente considerata un ostacolo alla piena protezione della sicurezza delle persone fisiche o per lo meno una condizione inevitabile da rispettare da parte delle autorità di contrasto. Si tratta, come correttamente messo in luce dal Garante Europeo per la Protezione dei Dati Personali, di una visione riduttiva: un solido quadro di protezione dei dati può, al contrario, affinare e rafforzare la sicurezza[563].

Come si è visto nella prima parte del presente lavoro, il diritto alla protezione dei dati personali è un diritto fondamentale, riconosciuto come tale dall'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea e dall'art. 16 TFUE, nonché dall'art. 8 CEDU, come interpretato dalla Corte di Strasburgo. Esso deve quindi essere rispettato quando si utilizzano strumenti di cooperazione giudiziaria. A tal fine è opportuno dotarsi di una normativa puntuale in materia di *data protection*, che sia in grado di garantire una tutela effettiva ed uniforme, quanto meno all'interno degli Stati membri dell'Unione europea.

Infatti, la mancanza di armonizzazione nel settore della protezione dei dati personali ha conseguenze estremamente negative nell'era del *cloud computing* e dei *social networks*, in una società dell'informazione in cui le frontiere fisiche tra gli Stati diventano sempre meno rilevanti, e in cui ogni dato, anche se apparentemente "neutro", rivela in realtà aspetti della vita privata.

4.1 La protezione dei dati personali nella Regione Europa

A livello europeo la prima fonte normativa che si occupa di garantire un'adeguata protezione dei dati personali di fronte allo sviluppo tecnologico è la

[563] Parere del GEPD del 14 gennaio 2011, in *GUUE* del 22 giugno 2011, C 181/1.

Convenzione del Consiglio d'Europa per la protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale del 17 dicembre 1980[564]. La Convenzione, tuttavia, non riconosce diritti ai singoli, limitandosi ad introdurre in capo agli Stati l'obbligo di adottare le misure necessarie per rendere effettivi i principi ivi affermati. Ciononostante essa rappresenta una pietra miliare nel processo di progressivo affermarsi del diritto alla tutela dei dati personali come diritto autonomo rispetto a quello alla protezione della vita privata, garantito dall'art. 8 CEDU.

L'Unione europea è tributaria dell'elaborazione del Consiglio d'Europa per quanto riguarda la tutela dei dati personali e infatti, sia la Direttiva 95/46/CE, cosiddetta "direttiva madre" del diritto comunitario in tema di dati personali[565], che la D.Q. 2008/977/GAI sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale[566] richiamano espressamente i principi contenuti nella Convenzione del 1981, come elaborati e interpretati dalla Corte di Strasburgo[567].

Come emerge dalla datazione dei citati provvedimenti, l'Unione europea giunge con un significativo ritardo ad apprestare una compiuta ed organica disciplina della tutela dei dati personali nel settore della cooperazione giudiziaria e di polizia in materia penale. I motivi di tale ritardo sono imputabili principalmente alla ritrosia degli Stati membri a cedere sovranità in un campo così delicato come quello della protezione dei dati personali e dell'autodeterminazione informativa, oltre al fatto che tale tutela era percepita come un ostacolo alla cooperazione informativa finalizzata alla prevenzione e repressione del terrorismo internazionale.

---

[564] Convenzione n. 108 aperta alla firma il 28 gennaio 1981, in vigore dal 1985, ratificata dall'Italia con legge 21 febbraio 1989, n. 98.

[565] *GUCE* del 23 novembre 1995, L 281/31. Cfr. decimo e undicesimo *considerandum* della direttiva, ove si prevede che «le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'art. 8 della [CEDU] e dai principi generali del diritto comunitario; [...] pertanto il ravvicinamento di dette legislazioni non deve avare per effetto un indebolimento della tutela da esse assicurata, ma deve anzi mirare a garantire un elevato grado di tutela nella Comunità», e che «i principi della tutela dei diritti e delle libertà delle persone, in particolare del rispetto della vita privata, contenuti nella direttiva, precisano ed ampliano quelli enunciati dalla Convenzione del Consiglio d'Europa del 1981».

[566] *GUUE* del 30 dicembre 2008, L 350/60. Cfr. *Considerandum* n. 41 della decisione quadro.

[567] La nozione di dato personale accolta da tali strumenti è molto ampia: si considera tale «qualsiasi informazione concernente una persona fisica identificata o identificabile». Cfr. Art. 2, lett. a) Convenzione 108/1981, art. 2, lett. a) direttiva 95/45/CE, art. 2 D.Q. 2008/977/GAI.

La c.d. direttiva madre in materia di protezione dei dati personali - la direttiva 95/46/CE - adottata al preciso scopo di contemperare la libertà di circolazione di persone, beni e servizi con la tutela della vita privata, e strumentale alla realizzazione del mercato interno, non si applicava alle attività di Terzo Pilastro, e in particolare, alle materie penali [568]. In quest'ambito, la tutela dei dati personali e dell'autodeterminazione informativa è stata per lungo tempo affidata a normative di settore – in particolare quelle relative a *Eurojust*, *Europol* e al Sistema Informativo Schengen (SIS) – dando vita ad un «quadro giuridico assolutamente frammentario, talvolta persino incoerente»[569].

Muovendosi nel solco delle direttrici individuate nel Programma dell'Aia, adottato dal Consiglio europeo nel novembre del 2004, e in cui si riconosceva che la realizzazione di uno Spazio di Libertà, Sicurezza e Giustizia richiedeva non solo il rafforzamento della sicurezza, ma altresì il rafforzamento dei diritti fondamentali garantiti dalla CEDU e dalla Carta di Nizza, è stata adottata la decisione quadro 2008/977/GAI con l'obiettivo di dotare anche le attività di Terzo Pilastro di una normativa generale a tutela dei dati personali[570].

[568] Cfr. art. 3, par. 2 della Direttiva 95/46/CE: «Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali effettuati per l'esercizio di attività che non rientrino nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del Trattato sull'Unione Europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale». Tra gli strumenti a tutela dei dati personali adottati nell'ambito del Primo Pilastro va ricordata inoltre la direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, c.d. direttiva *e-privacy* (*GUCE* del 31 luglio 2007, L 201/37), come modificata dalla direttiva 2006/24/CE, c.d. direttiva *data retention*.

[569] Così, G. DI PAOLO, *La circolazione dei dati*, cit., p. 1981.

[570] Ai fini dell'attuazione del Programma dell'Aia, la Commissione nel 2005 ha infatti formulato due proposte di decisione quadro relative, l'una alla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (COM (2005) 475 def., del 4 ottobre 2005), l'altra allo scambio d'informazioni in virtù del principio di disponibilità, introdotto proprio dal Programma dell'Aia per agevolare la cooperazione informativa (COM (2005) 490 def., del 12 ottobre 2005). L'ordine temporale con cui le due proposte sono state adottate non è casuale, ma risponde ad un preciso intento, quello di garantire un adeguato livello di protezione dei dati e di armonizzazione delle legislazioni nazionali, prima di procedere ad incrementare le forme di scambio degli stessi: l'armonizzazione deve infatti costituire un presupposto della libera circolazione. Purtroppo nei fatti questo *iter* virtuoso non è stato rispettato, e si è quindi giunti ad una decisione quadro in materia di *information sharing* (D.Q. 2006/960/GAI) molto prima di adottarne una che mirasse a garantire un'uniforme protezione dei dati personali a livello europeo (D.Q. 2008/977/GAI).

Tuttavia, il testo della decisione quadro, frutto di un inevitabile compromesso[571], è ampiamente insoddisfacente. In particolare, il trattamento *purely domestic* dei dati personali, oggetto di riserva da parte di molti Stati membri, è stato espunto dal suo ambito di applicazione, e così anche le norme, contenute nel testo originario della proposta di decisione quadro (COM (2005) 475 def.), riguardanti l'obbligo di distinguere i dati raccolti in varie categorie a seconda dello *status* del titolare.

La decisione quadro 2008/977/GAI, dopo aver enunciato i principi di legalità, proporzionalità e finalità limitata del trattamento (art. 3), articola la tutela del dato personale lungo le consuete direttrici del diritto alla riservatezza e di quello all'autodeterminazione informativa, intesa sia in senso oggettivo che soggettivo.

[571] Solo così, infatti, si è potuto approvare un testo definitivo, dopo anni di trattative e un avvicendarsi frenetico di proposte. La proposta originaria della Commissione (COM (2005) 475 def., del 4 ottobre 2005) prevedeva l'adozione di una decisione quadro il cui ambito di applicazione si estendesse a qualunque operazione, compiuta con o senza l'ausilio di processi automatizzati, relativa ai dati personali, sia nel settore della cooperazione di polizia che in quello della cooperazione giudiziaria in materia penale. Non riguardava, invece, i trattamenti dei dati personali effettuati da *Europol*, *Eurojust* e dal Sistema Informativo Schengen (SIS), in quanto già disciplinati da normative di settore contenenti esplicite previsioni in materia di tutela dei dati personali. Tale proposta inoltre mirava a disciplinare non soltanto lo scambio transfrontaliero di dati, ma anche la raccolta e il trattamento *purely domestic* da parte delle autorità giudiziarie o di polizia. Si auspicava inoltre che gli Stati rispettassero il principio di finalità limitata - ai sensi del quale i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità - e che distinguessero i dati in categorie a seconda dello *status* dei soggetti a cui si riferivano - si distingueva tra «persone sospettate di aver commesso un reato, persone condannate in sede penale e persone che danno adito a ritenere che commetteranno un reato» - e al livello di accuratezza del trattamento e di affidabilità delle rispettive fonti. Era vietato il trattamento dei dati c.d. sensibili, ossia quelli in grado di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché profili concernenti la salute o la vita sessuale. La proposta di decisione quadro era inoltre correlata da un insieme di garanzie e diritti soggettivi da riconoscere al titolare del dato trattato, quali il diritto all'informazione (sull'esistenza e la finalità del trattamento, sul responsabile del trattamento, *etc.*), il diritto di accesso e il diritto all'oblio, cioè il diritto alla cancellazione dei dati al ricorrere di determinate condizioni, quali il venir meno dell'esigenza per cui erano stati raccolti oppure l'illegittimità del trattamento. A tali garanzie soggettive si accompagnavano garanzie oggettive, in particolare i profili della sicurezza e della riservatezza del trattamento, ossia la necessità che le informazioni fossero sempre aggiornate e corrette. Infine, va precisato che la Commissione, consapevole della delicatezza del tema, aveva concepito il trattamento e la circolazione dei dati personali come *extrema ratio*. Infatti, nella proposta di decisione quadro veniva precisato che all'attività in questione si procedesse solo qualora vi fossero ragionevoli motivi per ritenere, sulla base di fatti specifici, che lo scambio di informazioni personali agevolasse o accelerasse la prevenzione, le indagini, l'accertamento o il perseguimento di un reato, purché lo stesso risultato non si potesse raggiungere con altri mezzi meno invasivi per la persona cui i dati si riferivano. La proposta di decisione quadro non è stata approvata a causa dell'impossibilità di raggiungere un accordo sul suo contenuto, in particolare con riferimento all'estensione del suo ambito di applicazione anche al trattamento *purely domestic* di dati personali e alle condizioni per la trasmissione dei dati a Paesi terzi e organizzazioni internazionali. Cfr. S. CIAMPI, *Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea*, in F. PERONI, M. GIALUZ (a cura di), *Cooperazione informativa*, cit., p. 34 ss.; G. DI PAOLO, *La circolazione dei dati*, cit., 1980 ss.

Sotto il primo aspetto, essa impone agli Stati membri l'adozione di misure volte a garantire la riservatezza e la sicurezza del trattamento, al fine, tra gli altri, di evitare che i dati vengano accidentalmente cancellati o di prevenire accessi illegittimi alle banche dati (artt. 21 e 22). Per quanto riguarda, invece, il diritto all'autodeterminazione informativa, sotto il profilo oggettivo, la decisione contiene una serie di disposizioni volte a garantire la qualità ed esattezza dei dati, quali l'obbligo di rettificare i dati qualora siano inesatti, cancellarli nel caso in cui non servano più allo scopo per il quale erano stati raccolti, e infine bloccarli, quando non sono più necessari allo scopo, ma la loro cancellazione potrebbe pregiudicare interessi legittimi dell'interessato (art. 4), nonché obblighi di registrazione e documentazione dei dati raccolti al fine di permettere la tracciabilità dello scambio (art. 10). Sotto il profilo soggettivo, alla persona interessata è riconosciuto innanzitutto il diritto ad essere informata della raccolta e trattamento di dati che la riguardano (art. 16), inoltre il diritto di accesso (art. 17) al fine di un'eventuale rettifica, cancellazione o blocco dei propri dati personali (art. 18), infine le è garantito il diritto al risarcimento del danno subito a causa di un trattamento illegale (art. 19). A completare il quadro, è prevista la designazione da parte di ciascuno Stato membro di un'autorità nazionale di controllo, indipendente e dotata di poteri investigativi e d'intervento (art. 25).

La disciplina in questione, tuttavia, è insoddisfacente. Innanzitutto, come già evidenziato, rinuncia ad estendere il suo ambito di applicazione ad attività di raccolta e scambio di dati puramente interne; inoltre, seppur solo nel caso in cui sia strettamente necessario e la legislazione nazionale preveda adeguate garanzie, essa ammette il trattamento di dati sensibili (art. 6), diversamente da quanto prevedeva la proposta originaria. Infine, lasciano perplessi le prescrizioni relative alla trasmissione dei dati a Paesi terzi o organizzazioni internazionali (art. 13). Infatti, seppur esse subordinino tale trasmissione alla sussistenza di un adeguato livello di protezione, i criteri in base ai quali valutare tale adeguatezza sono vaghi[572]. Inoltre, l'operatività di

[572] Cfr. G. TIBERI, *Protezione dei dati personali e sicurezza dopo Lisbona*, in G. GRASSO, L. PICOTTI, R. SICURELLA (a cura di), *L'evoluzione del diritto penale*, cit., p. 573. Ai sensi dell'art. 13, § 4 della decisione quadro, l'adeguatezza è valutata tenendo in considerazione «la natura dei dati, la finalità e la durata del trattamento previsto, lo Stato d'origine e lo Stato e organismo internazionale di destinazione finale dei dati, le norme di diritto, generali o settoriali, vigenti nel paese terzo o

tale presupposto è limitata ai casi in cui oggetto della trasmissione siano dati personali a loro volta «trasmessi o resi disponibili dall'autorità competente di un altro Stato membro» (art. 13, § 1), con la conseguenza che si applicheranno regimi diversi a seconda che i dati richiesti da un Paese terzo ad uno Stato membro siano di "prima o di seconda mano"[573]. A ciò va aggiunta la circostanza che la decisione fa salve disposizioni specifiche dettate da "normative di settore", quali quelle relative a *Eurojust*, *Europol*, al Sistema Informativo Schengen (SIS) o al Sistema Informativo Dogane (SID), nonché la decisione Prüm, con ciò rinunciando ad erigersi a normativa unitaria di tutela dei dati personali nel Terzo Pilastro.

In questo quadro normativo si inseriscono le modifiche apportate dal Trattato di Lisbona: l'art. 16 TFEU dopo l'affermazione, analoga a quella contenuta nell'art. 8 CDFUE, che «ogni persona ha diritto alla protezione dei dati a carattere personale che la riguardano»[574], introduce un'unica base giuridica (co-decisione Parlamento-Consiglio) per l'adozione da parte dell'Unione di norme uniformi in materia di tutela dei dati personali, anche nell'ambito della cooperazione di polizia e giudiziaria in materia penale.

La decisione quadro 2008/977/GAI, adottata nell'ambito del Terzo Pilastro, senza la co-decisione con il Parlamento europeo, non soddisfa i requisiti posti dall'art. 16 TFUE. Essa, tuttavia, in virtù del Protocollo n. 10 allegato al Trattato di Lisbona, rimarrà in vigore fino a quando non sarà sostituita da un nuovo strumento, che il legislatore europeo è obbligato ad adottare in forza dell'art. 16 TFUE. A tal fine, il 25 gennaio 2012, la Commissione ha adottato due proposte per una nuova disciplina della materia[575], consapevole che la portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso e che la tecnologia attuale consente alle autorità competenti di utilizzare dati personali, come mai in precedenza, nello

---

nell'organismo internazionale in questione, nonché le regole professionali e le misure di sicurezza che si applicano».

[573] Cfr. G. DI PAOLO, *La circolazione dei dati*, cit., p. 1985.

[574] Questa precisazione, lungi dall'essere superflua o ridondante, contribuisce ad inquadrare la questione degli strumenti europei di protezione dei dati personali nell'ambito della tutela dei diritti fondamentali. Cfr. G. TIBERI, *Protezione dei dati personali*, cit., p. 528.

[575] La Commissione ha lanciato una consultazione pubblica che è culminata nella presentazione della comunicazione "Un approccio globale alla protezione dei dati personali nell'Unione Europea" del 4 novembre 2010 (COM (2010) 609 def.). In tale comunicazione si sottolinea la necessità che la nuova normativa europea in tema di protezione dei dati personali tenga conto delle sfide derivanti dalla globalizzazione e dalle nuove tecnologie, in modo che si continui a garantire un alto livello di tutela degli individui rispetto al trattamento di dati in tutte le aree di azione dell'Unione europea.

svolgimento delle loro attività. Tale evoluzione impone quindi da un lato di agevolare la libera circolazione dei dati tra le autorità competenti all'interno dell'Unione e il trasferimento verso Paesi terzi e organizzazioni internazionali, dall'altro di garantire un elevato livello di protezione dei dati personali. Ciò richiede un quadro giuridico più solido e coerente in materia di protezione dei dati nell'Unione. La rapidità dell'evoluzione tecnologica impone, infatti, di adottare norme "tecnologicamente neutre", che siano capaci di adattarsi ai cambiamenti, senza ostacolarli, e continuando ad offrire adeguata protezione ai diritti oggetto di tutela.

Il pacchetto di riforma comprende una proposta di regolamento concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati[576], che dovrebbe sostituire la direttiva madre del '95, e una proposta di direttiva concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati[577], che dovrebbe sostituire la decisione quadro 2008/977/GAI.

Non è questa la sede per esaminare nel dettaglio il suddetto pacchetto di riforma, ciò che preme sottolineare è come, a ben vedere, esso non risolva il problema della frammentarietà del quadro giuridico dell'Unione in materia di protezione dei dati personali. Innanzitutto, viene mantenuto uno strumento diverso per l'ambito della cooperazione di polizia e giudiziaria in materia penale; in secondo luogo, appare criticabile la scelta della direttiva che, per dirla con il Garante Europeo della Protezione dei Dati personali, «fornisce un livello di protezione inadeguato, di gran lunga inferiore a quello della proposta di regolamento»[578]. Già in sede di valutazione della comunicazione della Commissione "Un approccio globale alla protezione dei dati personali nell'Unione europea" che aveva preceduto il pacchetto di riforma, il Garante Europeo aveva infatti sottolineato come lo strumento più indicato per la protezione dei dati fosse il regolamento: «uno strumento unico,

[576] Regolamento generale sulla protezione dei dati, COM (2012) 11 def.
[577] COM (2012) 10 def.
[578] Parere del 7 marzo 2012 sul pacchetto di riforma della protezione dei dati, reperibile in inglese su *http://www.edps.europa.eu.* Una sintesi in italiano del parere è pubblicata in *GUUE* del 30 giugno 2012, C 192/7.

direttamente applicabile negli Stati membri, è il mezzo più efficace per proteggere il diritto fondamentale alla protezione dei dati e creare un vero mercato interno in cui i dati personali possano circolare liberamente e in cui venga assicurato lo stesso livello di protezione indipendentemente dal Paese o dal settore in cui i dati vengono trattati»[579]. Optando per la direttiva, al contrario, si corre il rischio di consistenti differenze nell'implementazione da parte degli Stati membri con evidenti ripercussioni negative sull'esigenza di armonizzazione e prima ancora sul diritto fondamentale che si vuole garantire, come dimostra la vicenda della direttiva *data retention*[580]. Infine, la proposta di direttiva lascia inalterati diversi strumenti dell'Unione europea in materia di protezione dei dati, tra cui quelli riguardanti le istituzioni e gli organismi dell'Unione (art. 2)[581] e gli specifici strumenti adottati nel settore della cooperazione di polizia e giudiziaria in materia penale come la decisione Prüm e le norme relative a *Eurojust* e *Europol* (art. 59).

Due, invece, gli apprezzabili elementi di novità rispetto alla decisione quadro: la proposta di direttiva distingue i dati in base al soggetto cui si riferiscono (indagato, imputato, vittima, persona terza rispetto al procedimento, art. 5) e si applica anche al trattamento *purely domestic* dei dati personali. Quest'ultima previsione è senz'altro da accogliere positivamente nell'ottica dell'armonizzazione; tuttavia, finché il nuovo strumento in materia di protezione dei dati personali assume la forma della direttiva, l'effettiva armonizzazione dipenderà dalla sua implementazione da parte degli Stati membri.

[579] Parere del 14 gennaio 2011, in GUUE del 26 giugno 2011, C 181/1. Secondo il Garante Europeo «non esistono differenze fondamentali tra le autorità giudiziarie e di polizia e altre autorità di contrasto (fiscali, doganali, antifrode e competenti per l'immigrazione) soggette alla direttiva 95/46/CE» che possano giustificare l'adozione di due strumenti diversi in materia di protezione dei dati personali.

[580] Il 24 aprile 2011 la Commissione ha presentato al Consiglio e al Parlamento europeo una relazione di valutazione dell'applicazione della direttiva 2006/24/CE (COM (2011) 225 def.), da cui emerge un quadro estremamente differenziato circa l'implementazione della suddetta direttiva. Le differenze riguardano la durata della conservazione dei dati, la finalità della conservazione, le Autorità che possono accedere ai dati, nonché le disposizioni in materia di protezione e sicurezza dei dati. Inoltre, va ricordato che in quattro Stati membri, Germania, Romania, Repubblica Ceca e Bulgaria la normativa di attuazione della direttiva è stata dichiarata incostituzionale e non si è ancora provveduto a sostituirla.

[581] Continua a trovare applicazione in quest'ambito il regolamento 2001/45/CE, in *GUCE* del 12 gennaio 2001, L 8/1.

4.2 La giurisprudenza della Corte di Strasburgo come base per l'armonizzazione europea

Una cooperazione giudiziaria in materia di acquisizione probatoria che sia rispettosa dei diritti fondamentali dei soggetti coinvolti e che porti a risultati utilizzabili e ammissibili in giudizio presuppone l'esistenza di standard investigativi comuni.

Il Trattato di Lisbona introduce un'apposita base giuridica per l'adozione di «norme minime» in materia di ammissibilità delle prove, «laddove [sia] necessario per facilitare il riconoscimento reciproco delle decisioni giudiziarie e la cooperazione di polizia e giudiziaria in materia penale», con la precisazione che tali norme dovranno tenere comunque conto delle «differenze tra le diverse tradizioni giuridiche degli Stati membri, […] senza impedire a [questi ultimi] di introdurre o mantenere un livello più elevato di tutela delle persone» (art. 82 TFUE).

Come è emerso dagli studi preparatori delle *Model Rules*, il livello di armonizzazione raggiunto a livello europeo varia in ragione del tipo di mezzo di ricerca della prova. Al riguardo è possibile individuare tre distinte aree omogenee[582]. Innanzitutto, misure investigative "classiche", quali audizioni di persone informate sui fatti, perquisizioni e sequestri; in secondo luogo, tecniche d'indagine di c.d. penultima generazione, come le intercettazioni telefoniche e le indagini corporali (incluso il prelievo di materiale biologico); infine le tecnologie del controllo di ultima generazione, ossia strumenti di captazione, localizzazione, trasmissione e registrazione di dati.

La disciplina dei mezzi di ricerca della prova appartenenti al primo e al secondo gruppo presenta un buon livello di armonizzazione, grazie all'attività della Corte Europea dei Diritti dell'Uomo che con la sua giurisprudenza ne ha stimolato il progressivo riavvicinamento. Tale Corte ha, infatti, imposto a tutti gli Stati aderenti alla Convenzione il rispetto dei diritti fondamentali ivi sanciti, fissando i presupposti di una loro legittima limitazione per finalità investigative e ha così «codificato i canoni essenziali di ogni disciplina interna e lima[to] le differenze esistenti».

Per quanto riguarda invece le misure di *surveillance*, «l'unico elemento che

[582] Così S. ALLEGREZZA, *Le misure coercitive*, cit., p. 159 ss.

pare accomunare le legislazioni nazionali è l'assenza di una disciplina puntuale nelle legislazioni nazionali»[583]. In quest'ambito, come si è visto nella prima parte del presente lavoro, diversa è la sensibilità degli ordinamenti: alcuni reagisco prima, in via legislativa o giurisprudenziale, riconoscendo la peculiarità dei nuovi strumenti investigativi ed apprestando una disciplina *ad hoc*; altri ricorrono all'applicazione analogica di norme dettate per misure affini o alla categoria della prova atipica. Il fenomeno non è nuovo, ma presenta criticità nuove in un contesto in cui sempre più spesso vi sono occasioni di confronto tra sistemi giuridici diversi a causa della transnazionalità della criminalità e della natura digitale della prova.

L'Unione europea, seguendo la strada del mutuo riconoscimento, ha fino ad ora rinunciato ad adottare norme comuni e condivise in questo particolare settore. Non si esclude che nel lungo periodo tale strategia possa portare ad una «progressiva osmosi fra i diversi ordinamenti», favorendo quell'armonizzazione in via giudiziaria che si è avuta con riferimento al Mandato d'Arresto Europeo: «i giudici, chiamati a "riconoscere" l'atto esogeno, si troveranno a dirimere i punti di contrasto che il legislatore comunitario non può e non vuole risolvere»[584]. Ciò, tuttavia, finirà per favorire i sistemi processuali più flessibili e meno formali, realizzando un'armonizzazione "verso il basso", con minori garanzie per i diritti fondamentali dei soggetti coinvolti.

Con l'entrata in vigore del Trattato di Lisbona, l'Unione ha gli strumenti per dettare disposizioni comuni agli Stati membri in materia di acquisizione probatoria (art. 82 TFUE). A tal fine, riteniamo che la giurisprudenza della Corte di Strasburgo relativa in particolare all'art. 8 CEDU possa costituire una buona base di partenza[585].

---

[583] Le citazioni sono di S. ALLEGREZZA, *Le misure coercitive*, cit., p. 159 ss.

[584] Così, S. ALLEGREZZA, *L'armonizzazione della prova penale*, cit., p. 167 ss.

[585] G. DE AMICIS, *Limiti e prospettive*, cit., p. 504, riconosce la forza espansiva della giurisprudenza CEDU, che agisce come «fonte indiretta di ravvicinamento della disciplina della prova penale»; tale ruolo riceverebbe ulteriore impulso per effetto della prevista adesione dell'Unione europea alla CEDU (art. 6 TUE). Cfr. altresì A. BALSAMO, S. RECCHIONE, *La costruzione di un modello europeo di prova dichiarativa: il «nuovo corso» della giurisprudenza e le prospettive aperte dal Trattato di Lisbona*, in *Cass. pen.*, 2010, p. 3623 ss., secondo i quali la giurisprudenza interna sarebbe orientata nel senso di individuare nei principi fissati dalla Corte EDU quel comune *standard* di garanzie processuali che rende possibile la libera circolazione delle prove e dei provvedimenti giudiziari all'interno dell'Unione europea. Scettica sul ruolo che la CEDU potrebbe avere sul versante dell'armonizzazione della prova è S. GLESS, *Strategie e tecniche per l'armonizzazione della prova*, in *Prova penale e Unione Europea*, cit., p. 141 ss., in particolare p. 149, secondo la quale «la Convenzione europea non stabilisce un organico e dettagliato sistema che disciplini l'ammissibilità o la rilevanza di una prova come tale, neppure in ordine all'attendibilità o alla *fairness* della medesima». L'Autrice, tuttavia,

È vero che si tratta di *standards* minimi, ma, alla luce della riscontrata divergenza nelle discipline nazionali in particolare in materia di mezzi di ricerca della prova di ultima generazione, si ritiene più prudente individuare un minimo comun denominatore, fermo restando che gli Stati potranno poi adottare presupposti più stringenti e garantisti (secondo quanto previsto dallo stesso art. 82 TFUE)[586].

Inoltre, quest'approccio ha il pregio di consentire di impostare il discorso sui requisiti che le singole misure investigative devono rispettare, muovendo dai diritti fondamentali coinvolti. E quindi, mezzi di ricerca della prova che interferiscono con il diritto alla vita privata, nell'ampia interpretazione che ne dà la Corte Europea dei Diritti dell'Uomo, dovranno essere previste dalla legge, ossia avere una base nel diritto interno – di creazione legislativa o giurisprudenziale - ed essere conoscibili dall'interessato, il quale deve essere in grado di prevedere le conseguenze derivanti dall'applicazione della misura nei suoi confronti (*foreseeability*). La *legge* dovrà indicare la natura, lo scopo, la durata della misura e i motivi per cui può essere adottata, individuare l'autorità competente ad autorizzare, condurre, nonché supervisionare la sorveglianza, e contemplare dei rimedi per l'interessato. I presupposti saranno poi graduati in considerazione del diverso livello di intrusività della misura[587].

---

riconosce il grande impatto che la CEDU ha avuto sulle procedure penali degli Stati europei sul versante delle regole di acquisizione probatoria; ciò che critica è il ruolo della CEDU in materia di ammissibilità della prova, in quanto essa «lascia senza risposta l'interrogativo se un elemento di prova – raccolto legalmente o illegalmente in un paese – sia ammissibile davanti al giudice di un altro paese».

[586] Cfr. S. MARCOLINI, *La circolazione della prova nello spazio giudiziario europeo tra vecchi e nuovi modelli: la difficile convivenza tra efficienza e tutela*, in G. GRASSO, L. PICOTTI, R. SICURELLA (a cura di), *L'evoluzione del diritto penale*, cit., p. 535 ss., il quale, molto opportunamente precisa che «se si interviene mediante la fonte della direttiva, questa dovrebbe essere quanto più precisa, dettagliata e «*self executing*» possibile, proprio per garantire la massima uniformità applicativa».

[587] A tal proposito si veda altresì la bozza di risoluzione del III Colloquio preparatorio al XIX Congresso Internazionale di Diritto Penale, "Società dell'informazione e diritto penale", che prevede che «i mezzi di indagine con *ICT* debbono essere consentiti solo nei casi specificati dalla legge quando le informazioni desiderate non possono essere raccolte con strumenti meno intrusivi. La legge deve definire l'ambito dei poteri di indagine, la durata massima di ogni atto di indagine e i requisiti per l'archiviazione e/o distruzione dei dati ottenuti. I mezzi di indagine con *ICT* che si intromettono gravemente nel diritto alla *privacy*, come quelli che accedono al contenuto di comunicazioni o implicano l'intercettazione o la raccolta di dati in tempo reale, dovrebbero, di regola, essere permessi solo dietro autorizzazione del giudice, nei casi in cui ci sia un ragionevole sospetto di commissione di uno dei delitti di una categoria di delitti gravi, e che il bersaglio sia legato alla commissione di tale delitto». Si è scelto di non includere una lista di strumenti investigativi che sfruttano le *Information and Communication Technology*. Il testo della bozza, assieme a tutti i materiali disponibili dei colloqui preparatori, è reperibile all'indirizzo *www.aidpitalia.org*.

Infine, se, come autorevolmente ricordato, «in epoca anteriore alle codificazioni è stato il diritto delle prove elaborato dalla pratica medievale, sia pure con l'affermazione di valori e prassi ora ripudiati, a cementare l'unità del processo», l'armonizzazione della *law of evidence* potrebbe proprio costituire il punto di partenza per l'armonizzazione del diritto processuale penale europeo. Nel fare ciò, occorre tuttavia che siano rispettate le diversità dei sistemi giuridici nazionali, in modo da evitare che l'individuazione di regole comuni si trasformi «in una forzata omologazione suscettibile di comportare arretramenti sul piano delle garanzie»[588].

[588] Le citazioni sono di E. AMODIO, *Giusto processo,* procès èquitable *e* fair trial*: la riscoperta del giusnaturalismo processuale in Europa*, in *Riv. it. dir. proc. pen.*, 2003, p. 93 ss., in particolare p. 106, 107.

BIBLIOGRAFIA

ADDIS M. P., *Diritto all'autodeterminazione informativa e processo penale in Germania*, in D. NEGRI (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 87 ss.;

ALESSI G., *Il processo penale. Profilo storico*, Roma-Bari, 2001;

ALLEGREZZA S., *Verso una Procura europea per tutelare gli interessi finanziari dell'Unione. Idee di ieri,* chances *di oggi, prospettive di domani*, in *www.penalecontemporaneo.it*;

ALLEGREZZA S., *Le misure coercitive nelle* «Model Rules for the Procedure of the European Public Prosecutor's Office», in F. RUGGIERI, T. RAFARACI, G. DI PAOLO, S. MARCOLINI, R. BELFIORE (a cura di), *Processo penale, lingua e Unione Europea*, Padova, 2013, p. 151 ss.;

ALLEGREZZA S., *L'armonizzazione della prova penale alla luce del Trattato di Lisbona,* in *Prova penale e Unione Europea*, in G. ILLUMINATI (a cura di), Bologna, 2009, p. 161 ss.;

ALLEGREZZA S., *Giustizia penale e diritto all'autodeterminazione dei dati personali nella regione Europa*, in D. NEGRI (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 59 ss.;

ALLEGREZZA S., *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. 700 ss.;

ALLENA G., *Riflessioni sul concetto di incostituzionalità della prova nel processo penale*, in *Riv. it. dir. e proc. pen*., 1989, p. 506 ss.;

AMATO G., *Art. 13*, in A. BRANCA (a cura di), *Commentario alla costituzione*, *Rapporti civili*, Bologna, 1975, p. 1 ss.;

AMATO G., *Art. 14*, in A. BRANCA (a cura di), *Commentario alla costituzione*, *Rapporti civili*, Bologna, 1975, p. 54 ss.;

AMATO G., *Art. 16*, in A. BRANCA (a cura di), *Commentario alla costituzione*, *Rapporti civili*, Bologna, 1975, p. 114 ss.;

AMODIO E., *Giusto processo,* procès èquitable *e* fair trial*: la riscoperta del giusnaturalismo processuale in Europa*, in *Riv. it. dir. proc. pen.*, 2003, p. 93 ss.;
AMORTH A., *La Costituzione italiana*, Milano, 1948;

APRILE E., *Sequestro del computer di un giornalista, clonazione della relativa memoria e tutela del segreto professionale*, in *Dir. Internet* 2007, p. 585 ss.;

APRILE E., *Le indagini tecnico-scientifiche: problematiche giuridiche sulla formazione della prova penale*, in *Cass. pen.*, 2003, p. 4034;

ATERNO S., *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, p. 955 ss.;

ATERNO S. - CISTERNA A., *Il legislatore interviene ancora sul* data retention*, ma non è finita*, in *Dir. pen. proc.* 2009, p. 282 ss.;

AULETTA T. A., *Riservatezza e tutela della personalità*, Milano, 1978;

BÄR W., *Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen*, in *MMR*, 2008, p. 215 ss.;

BALDASSARRE A., *Diritti della persona e valori costituzionali*, Torino, 1997;

BALSAMO A., TAMIETTI A., *Le intercettazioni, tra garanzie formali e sostanziali*, in A. BALSAMO, R. E. KOSTORIS (a cura di), *Giurisprudenza europea e processo penale italiano*, Torino, 2008, p. 425 ss.;

BALSAMO A., RECCHIONE S., *La costruzione di un modello europeo di prova dichiarativa: il «nuovo corso» della giurisprudenza e le prospettive aperte dal Trattato di Lisbona*, in *Cass. pen.*, 2010, p. 3623 ss.;

BARBERA A., *Le tre Corti e la tutela multilivello dei diritti*, in P. BILANCIA, E. DE MARCO (a cura di), *La tutela multilivello dei diritti. Punti di crisi, problemi aperti, momenti di stabilizzazione*, Milano, 2004, p. 89 ss.;

BARBERA A., *Art. 2 Cost.*, in G. Branca (a cura di), *Commentario della Costituzione. Principi fondamentali*, Bologna,1975;

BARBERA A., *I principi costituzionali della libertà personale*, Milano, 1967;

BARBIERI A., *Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici* in: *La ratifica della Convenzione del Consiglio d'Europa sul* cybercrime*: profili processuali*, in *Dir. Internet* 2008, p. 516 ss.;

BARILE P., *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984;

BARILE P., CHELI E., voce *Corrispondenza (libertà di), Enc. dir.*, vol. X, Milano, 1962, p. 741 ss.;

BARILE P., CHELI E., voce *Domicilio (libertà di), Enc. dir.*, vol. XIII, Milano, 1964, p. 859 ss.;

BARTOLE S., DE SENA P., ZAGREBELSKY V. (a cura di), *Art. 8. Commentario breve alla Convenzione Europea dei Diritti dell'Uomo*, Padova, 2012;

BEHAR D. C*., An Exception to an Exception: Officer Inadvertence as a Requirement to Plain View Seizures in the Computer Context,* in *66 U. Miami L. Rev. 471 (2012)*;

BENDICH A. M., *Privacy, Poverty and the Constitution*, *Report for the Conference on the Law of the Poor*, *University of California at Berkeley*, p. 7 ss.;

BORRELLI G., *Riprese filmate nel bagno di un pubblico esercizio e garanzie costituzionali*, in *Cass. pen.*, 2001, p. 2453 ss.;

BRAGHÒ G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, p. 181 ss.;

BRENNER S. W., *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, in 81 *Miss. L. J.*, 1 (2011);

BRENNER S. W. - FREDERIKSEN B. A., *Computer Searches and Seizures: Some Unresolved Issues,* in 8 *Mich. Telecomm. Tech. L. Rev.,* 39 (2001/2002);

BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. e proc. pen.*, 1967, p. 1079 ss.;

BRODOWSKI D., *Strafprozessuale Zugriff auf E-Mail-Kommunikation*, in *JR*, 2009, p. 402 ss.;

BRUEGGEMANN WARD K., *The Plain (or not so Plain) View Doctrine: Applying the Plain View Doctrine to Digital Seizures,* in 79 *U. Cin. L. Rev.,* 1163 (2011);

BRUSCO C., *La valutazione della prova scientifica*, in *Dir. pen. proc.*, 2008, suppl. al n. 6, p. 27 ss.;

BULL P. H., *Informationelle Selbstbestimmung – Vision oder Illusion?,* Tübingen, 2. Auflage, 2011;

BUONOMO G., *Metodologia e disciplina delle indagini informatiche*, in R. BORRUSO, R. BUONOMO, G. CORASANTI, G. D'AIETTI (a cura di), *Profili penali dell'informatica*, Milano, 1994, p. 148 ss.;

CAJANI F., Internet Protocol. *Questioni operative in tema di investigazioni penali e riservatezza*, in *Dir. Internet* 2008, p. 545 ss.;

CAMON A., *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento ed alcuni dubbi nuovi*, in *Riv. it. dir. e proc. pen.* 2006, p. 1550 ss.;

CAMON A., *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. e proc. pen.*, 2005, p. 594 ss.;

CAMON A., *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen.*, 1999, p. 1188 ss.;

CAMON A., *Le intercettazioni nel processo penale*, Milano, 1996;

CANTONE R., *Sulla riesaminabilità del decreto di sequestro probatorio di cose già restituite*, in *Cass. pen.* 2005, p. 915 ss.;

CAPRIOLI F., *Nuovamente al vaglio della Corte costituzionale l'uso degli strumenti investigativi di ripresa visiva*, in *Giur. cost.*, 2008, p. 1832 ss.;

CAPRIOLI F., *Riprese visive nel domicilio e intercettazioni «per immagini»*, in *Giur. cost.*, 2002, p. 1062 ss.;

CAPRIOLI F., *Colloqui riservati e prova penale*, Torino, 2000;

CARNELUTTI F., *Principi del processo penale*, Napoli, 1960;

CARNEVALE S., *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. proc.* 2009, p. 481 ss.;

CARNEVALE S., *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in D. NEGRI (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 3 ss.;

CARTABIA M., *La convenzione europea dei diritti dell'uomo e l'ordinamento italiano*, in A. BALSAMO, R. E. KOSTORIS (a cura di), *Giurisprudenza europea e processo penale italiano*, Torino, 2008, p. 33 ss.;

CARTABIA M., *Le sentenze "gemelle": diritti fondamentali, fonti, giudici*. *Giur. cost.*, 2007, p. 3535 ss.;

CASEY E., *What does "forensically sound" really mean?*, *Digital investigation*, 2007, f. 4, p. 49 ss.;

CASEY E., *Digital Evidence and Computer Crime. Forensic science, computers and the Internet*, *Second Edition*, Elsevier, 2004;

CASSIBBA F., *L'ampliamento delle attribuzioni del pubblico ministero distrettuale*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, p. 113 ss.;

CERQUA F., *Le Sezioni Unite fissano i criteri per stabilire quando gli atti investigativi non sono ripetibili*, in *Dir. pen. proc.*, 2007, p. 1576 ss.;

CERRI A., *Libertà negativa di manifestazione del pensiero e di comunicazione - Diritto alla riservatezza: fondamento e limiti*, in *Giur. cost.*, 1974, p. 610 ss.;

CESARI C., *L'irripetibilità sopravvenuta degli atti di indagine*, Milano, 1999;

CHELO MANCHÌA A., *Sequestro probatorio di* computers*: un provvedimento superato dalla tecnologia?*, in *Cass. pen.* 2005, p. 1634 ss.;

CIAMPI S., *Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea*, in F. PERONI, M. GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009, p. 34 ss.;

CISTERNA A., *Perquisizioni in caso di fondato motivo*, in *Guida dir.*, 2008, n. 16, p. 66 ss.;

COLOMBO E., *La sentenza del caso di Garlasco e la* computer forensics, in *Cyberspazio e diritto*, 2010, p. 454 ss.;

CONFORTI B., *Sulle recenti modifiche della Costituzione italiana in tema di rispetto degli obblighi internazionali comunitari*, in *Foro it.*, 2002, V, c. 229 ss.;

CONSO G., GREVI V., BARGIS, M., *Compendio di procedura penale*, VI Ed., Padova, 2012;

CONTI C., *Incostituzionale la richiesta coatta di archiviazione: la consulta tra principio di incidentalità e di preclusione*, in *Dir. pen. proc.*, 2009, p. 1367 ss.;

CORDERO F., *Procedura penale*, Milano, 2012;

CORDERO F., *Codice di procedura penale commentato*, II Ed., Torino, 1992;

CORDERO F., *Prove illecite,* in *Tre studi sulle prove penali*, Milano, 1963;

COSTABILE G., ATTANASIO A., IISFA Membergroup *2012.* Digital Forensics*. Condivisione della conoscenza tra i membri dell'*IISFA ITALIAN CHAPTER, *Experta Edizioni*, 2012;

CRISAFULLI V., *Libertà personale, costituzione e passaporti*, in *Arch. pen.*, 1955, II, p. 117 ss.;

DANIELE M., *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, p. 440 ss.;

DANIELE M., *Caratteristiche della prova digitale*, in F. RUGGIERI, L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, p. 203 ss.;

DANIELE M., *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 283 ss.;

DE AMICIS G., *Limiti e prospettive del mandato europeo di ricerca della prova*, in G. GRASSO – L. PICOTTI – R. SICURELLA (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, p.475 ss.;

DE CUPIS A., *I diritti della personalità*, Padova, 1942;

DELMAS-MARTY M., VERVAELE J. A. E., (a cura di), *The implementation of Corpus iuris*, Antwerpen-Groenigen-Oxford, 2000;

DE SIERVO U., voce *Soggiorno, circolazione, emigrazione (Libertà di)*, in *Novissimo digesto italiano*, vol. XVII, Torino, 1970, p. 822 ss.;

DE VIRES K., BELLANOVA R., DE HERT P., *Proportionality overrides Unlimited Surveillance. The German Constitutional Court Judgment on data retention*, in *CEPS*, 2010, p. 1 ss.

DI BITONTO M. L., *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. Internet*, 2008, p. 503 ss.;

DI BITONTO M. L., *Le riprese video domiciliari al vaglio delle Sezioni Unite*, in *Cass. pen.* 2006, p. 3937 ss.;

DI FILIPPO, *Dati esteriori delle comunicazioni e garanzie costituzionali*, in *Giur. it.* 1995, I, c. 117 ss.;

DI PAOLO G., *Note a margine della recente proposta di istituzione di una Procura europea contenuta nelle* Model Rules for the Procedure of the European Public Prosecutor's Office, in F. RUGGIERI, T. RAFARACI, G. DI PAOLO, S. MARCOLINI, R. BELFIORE (a cura di), *Processo penale, lingua e Unione Europea*, Padova, 2013, p. 129 ss.;

DI PAOLO G., (voce) *Prova informatica (diritto processuale penale)*, in *Enc. dir.*, Annali VI, Milano, 2013, p. 736 ss.;

DI PAOLO G., *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in *Cass. pen.*, 2010, p. 1969 ss.;

DI PAOLO G., *Judicial investigations and gathering of evidence in a digital online context*, in *IRPL*, 2009, p. 201 ss.;

DI PAOLO G., *"Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Padova, 2008;

DRALLÉ L., *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, *Lorenz-von-Stein-Institut*, 2010;

ECKHARDT J – SCHUTZE M., *Vorratsdatenspeicherung nach BverfG: "Nach dem Gesetz ist vor dem Gestetz..."*, in *CR* 2010, p. 225 ss.;

FANCHIOTTI V., U.S. v. Jones*: Una soluzione tradizionalista per il futuro della* privacy*?*, in *Dir. pen. proc.*, 2012, p. 381 ss.;

FASOLIN S., *La copia di dati informatici nel quadro delle categorie processuali*, in *Dir. pen. proc.*, 2012, p. 372 ss.;

FERRUA P., *La regola d'oro del processo accusatorio: l'irrilevanza probatoria delle contestazioni*, in R. E. KOSTORIS (a cura di), *Il giusto processo, tra contraddittorio e diritto al silenzio*, Torino, 2002, p. 11 ss.;

FICHERA M., *The implementation of the European Arrest Warrant in the European Union: law, policy and practice*, Antwerpen-Oxford, 2011;

FILIPPI L., *Il GPS è una prova incostituzionale? Domanda provocatoria, ma non troppo, dopo la sentenza Jones della Corte Suprema U.S.A.*, in *Arch. pen.*, 2012, p. 1 ss.;

FILIPPI L., *L'intercettazione di comunicazioni*, Milano, 1997;

FLOR R., *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, in *www.penalecontemporaneo.it*;

FLOR R., *Verso una rivalutazione dell'art. 615* ter *c.p.?*, in *Dir. pen. cont.*, 2012, n. 2, p. 126 ss.;

FLOR R., Data retention *e limiti al potere coercitivo dello Stato in materia penale: le sentenze del* Bundesverfassungsgericht *e della* Curtea Constituţională, in *Cass. pen.*, 2011, p. 1952;

FLOR R., *La tutela dei diritti fondamentali della persona nell'epoca di Internet. Le sentenze del* Bundesverfassungsgericht *e della* Curtea Constituţională *su investigazioni ad alto contenuto tecnologico e* data retention, in F. RUGGIERI, L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, p. 32 ss.;

FLOR R., *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, p. 359 ss.;

FLOR R., *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* Online Durchsuchung*. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona. Aspetti di diritto penale sostanziale*, in *Riv. trim. dir. pen. ec.*, 2009, p. 697 ss.;

FLOR R., Phishing, identity theft *e* identity abuse. *Le prospettive applicative del diritto penale vigente*, *Riv. it. dir. proc. pen.*, 2007, p. 899 ss.;

FLOR R., *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di "domicilio informatico" e lo jus excludendi alios*, in *Dir. pen. proc.*, 2005, p. 81 ss.;

GAETA, *Per utilizzare registrazioni fra presenti fatte dalla Pg è sufficiente un decreto del pubblico ministero*, in *Guida dir.*, 2010, p. 75 ss.;

GALANTINI N., *sub art. 12, Le intercettazioni*, in A. CADOPPI (a cura di), *Commentario delle norme contro la violenza sessuale e della legge contro la pedofilia*, Padova, 2002, p. 774 ss.;

GALANTINI N., *L'inutilizzabilità della prova nel processo penale*, Padova, 1992;

GALEOTTI S., *La libertà personale*, Milano, 1953;

GALETTA D. U., *Principio di proporzionalità e sindacato giurisdizionale nel diritto amministrativo*, Milano, 1998;

GALIZIA M., *La libertà di circolazione e soggiorno (dall'Unificazione alla Costituzione repubblicana)*, in P. BARILE (a cura di), *La pubblica sicurezza*, Vicenza, 1967, p. 545 ss.;

GENTILE D., *Tracking satellitare mediante GPS: attività atipica di indagine o intercettazione di dati?*, in *Dir. pen. proc.*, 2010, p. 1472 ss.;

GERCKE M., *Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit*, in *CR*, 2007, p. 245 ss.;

GHIRARDINI A., FACCIOLI G., *Computer forensics*, Milano, 2010;

GIAMPICCOLO G., *Scritti giuridici in memoria di P. Calamandrei*, V, Padova, 1958, p. 440 ss.;

GIUNCHEDI F., *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, Torino, 2009;

GLANCY D. J., *Privacy on the Open Road*, in 30 *Ohio N. U. L. Rev.*, 295 (2004);

GLESS S., *Strategie e tecniche per l'armonizzazione della prova*, in G. ILLUMINATI (a cura di), *Prova penale e Unione Europea*, Bologna, 2009, p. 141 ss.;

GLESS S., *Mutual Recognition, Judicial Inquiries, Due Process and Fundamental Rights*, in J. A. E. VERVAELE (a cura di), *European Evidence Warrant. Transnational Judicial Inquiries in the EU*, Antwerpen-Oxford, 2005, p. 121 ss.;

GRASSO G., SICURELLA R., *Il Corpus juris 2000: un modello di tutela penale dei beni giuridici comunitari*, Milano, 2003;

GREVI V., *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.* 1973, p. 341ss.;

GREVI V., *Libertà personale dell'imputato e costituzione*, Torino, 1976;

GRILLO A., MOSCATO U. E., *Riflessioni sulla prova informatica*, in *Cass. pen.*, 2010, p. 375 ss.;

GUSY C., *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, in *DuD*, 2009, p. 33 ss.;

HEARD C., MANSELL D., *The European Investigation Order: Changing the Face of Evidence–gathering in EU Cross-border Cases*, in *EuCLR*, 2011, p. 353 ss.;

HERRERA-FLANIGAN J.R., *Cybercrime and Jurisdiction in the United States*, in B.J. KOOPS – S.W. BRENNER (a cura di), *Cybercrime and Jurisdiction. A Global Survey*, TMC Asser Press, The Hague, 2006, p. 313 ss.;

HOFMANN M., *Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmaßnahme?*, in *NStZ,* 2005, p. 121 ss.;

HOLZNER S., *Die Online-Durchsuchung: Entwicklung eines neuen Grundrechts*, Freiburg im Breisgau, 2009;

HOOD N.*, No Requirement Left Behind: The Inadvertent Discovery Requirement. Protecting Citizens One File at a Time,* in *45 Val. U. L. Rev. 1529 (2011)*;

HORNUNG G., *Die Festplatte als "Wohnung"?*, in *JZ*, 2007, p. 828 ss.;

HUBMANN H., *Das Persönlichkeitsrecht*, Münster-Köln-Böhlau, 1953, p. 17 ss.;

IACOBACCI D., *Sulla necessità di riformare la disciplina delle intercettazioni prendendo le mosse dalle esitazioni applicative già note*, in *Giust. pen.*, III, 2011, c. 365 ss.;

ICHINO G., *Gli atti irripetibili e la loro utilizzazione dibattimentale*, in G. UBERTIS (a cura di), *La conoscenza del fatto nel processo penale*, Milano, 1992, p. 114 ss.;

ILLUMINATI G., *L'armonizzazione della prova penale nell'Unione Europea,* in G. ILLUMINATI (a cura di), *Prova penale e Unione Europea*, Bologna, 2009, p. 9 ss.;

ILLUMINATI G., *La disciplina processuale delle intercettazioni*, Milano, 1983;

IOVENE F., *Perquisizione e sequestro di computer: un'analisi comparatistica*, in *Riv. dir. proc.*, 2012, p. 1607 ss.;

IOVENE F., *Pedinamento satellitare e diritti fondamentali della persona*, in *Cass. pen.*, 2012, p. 3556 ss.;

JAHN M. - KUDLICH H., *Die strafprozessuale Zulässigkeit der Online-Durchsuchung*, in *JR*, 2007, p. 57 ss.;

KEMPER M., *Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten*, in *ZRP*, 2007, p. 105 ss.;

KERR O. S., *Digital Evidence and the New Criminal Procedure*, in *105 Colum. L. Rev.*, 2005, p. 290 ss.;

KERR O. S., *The Fourth Amendment and New technologies: Constitutional Myths and the Case for Caution*, in 102 *Mich. L. Rev.*, 801 (2004);

KERR O. S., *Searches and Seizures in a Digital World*, in 119 *Harv. L. Rev.*, 511 (2005);

KLEIN O., *Offen und (deshalb) einfach-Zur Sicherstellungund Beschlagnahme von E-Mails beim Provider*, in *NJW*, 2009, p. 2996 ss.;

KLESCZEWSKI D., *Strafprozessrecht, Carl Heymanns Verlag* 2007;

KLIP A., *European Criminal Law*, Antwerpen-Oxford, 2009;

KOHLMANN D., *Online-Durchsuchungen und andere Maßnahmen mit Technikeinsatz*, Baden-Baden, 2012;

KOSTORIS R. E., *I consulenti tecnici nel processo penale*, Milano, 1993;

KOSTORIS R. E., *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in F. RUGGIERI, L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, p. 179 ss.;

KRÜGER S., MAUCHER S. A., *Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit großen Auswirkungen auf die Praxis*, in *MMR*, 2011, p. 433 ss.;

LARONGA A., *L'utilizzabilità probatoria del controllo a distanza eseguito con sistema satellitare* g.p.s., in *Cass. pen.*, 2002, p. 3050 ss.;

LIGETI K. (ed.), *Toward a Prosecutor for the European Union. Draft Rules of procedure, Volume 2*, Oxford, 2013 (in corso di pubblicazione);

LIGETI K. (*ed.*), *Toward a Prosecutor for the European Union. A comparative analysis*, *Volume 1*, Oxford, 2012;

LIGETI K., *The European Public Prosecutor's Office: How Should the Rules Applicable to its Procedure be Determined?*, in *EuCLR*, 2011, p. 123 ss.;

LIGETI K., SIMONATO M., *The European Public Prosecutor's Office: Towards a Truly European Prosecution Service?*, in *NJECL*, Vol. 4, Issue 1-2, 2013, p. 7 ss.,

LOGLI A., *Sequestro probatorio di un personal computer. Misure* ad explorandum *e tutela della corrispondenza elettronica*, in *Cass. pen.*, 2008, p. 2952 ss.;

LORENZETTO E., *Le attività urgenti di investigazione informatica e telematica*, in L. LUPÀRIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, p. 135;

LUPÀRIA L., Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, diretto da G. SPANGHER, vol. VII, *Modelli differenziati di accertamento*, G. GARUTI (a cura di), tomo I, Torino, 2011, p. 388 ss.;

LUPÀRIA L. (a cura di), *Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48)*, Milano, 2009;

LUPÀRIA L., *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale - I profili processuali*, in *Dir. Internet*, 2006, p. 153 ss;

LUPÀRIA L., *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc.* 2008, p. 717 ss.;

LUPÀRIA L. - ZICCARDI G., *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali,* Milano, 2007;

MACRILLÒ A., *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatica* in *La ratifica della Convenzione del Consiglio d'Europa sul* cybercrime*: profili processuali*, in *Dir. Internet* 2008, p. 511 ss.;

MACRILLÒ A., *Sequestro ex art. 200 c.p.p. e sequestro del* computer *in uso al giornalista*, in *Dir. pen. proc.* 2008, p. 1416 ss.;

MAIOLI C., *Introduzione all'informatica forense*, in P. POZZI (a cura di), *La sicurezza preventiva dell'informazione e della comunicazione*, Torino, 2004;

MARAFIOTI L., Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4509 ss.;

MARCOLINI S., *La circolazione della prova nello spazio giudiziario europeo tra vecchi e nuovi modelli: la difficile convivenza tra efficienza e tutela*, in G. GRASSO, L. PICOTTI, R. SICURELLA (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, p. 535 ss.;

MARCOLINI S., *Le cosiddette perquisizioni* online *(o perquisizioni elettroniche)*, in *Cass. pen.*, 2010, p. 2855 ss.;

MARINELLI C., *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007;

MARIOTTI S. - TACCONI S., *Riflessioni sulle problematiche investigative e di sicurezza connesse alle comunicazioni VoIP*, in *Dir. Internet* 2008, p. 558 ss.;

MASON S., *Electronic Evidence: Disclosure, Discovery and Admissibility*, Londra, 2007;

MASSA M., *La "sostanza" della giurisprudenza europea sulle leggi retroattive*, in *Giur. cost.*, 2009, p. 4657 ss.;

MEYERDIERKS P., *Sind IP-Adressen personenbezogene Daten?*, in *MMR*, 2009, p. 8 ss.;

MOLINARI F. M., *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, p. 1259 ss.;

MONATERI P. G., *Diritti senza tempo né spazio*, Sole24ore, 23 dicembre 2012, p. 33 ss.;

MONTI A., *No ai sequestri indiscriminati di computer*, in *Dir. Internet* 2007, p. 264 ss.;

MONTI A., *La nuova disciplina del sequestro informatico*, in L. Luparia (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, p. 197;

MONTONE S., *Sequestro penale* (voce), in *Dig. disc. pen.,* XIII, Torino 1997, p. 260 ss.;

MORELLI F. B., *La giurisprudenza costituzionale italiana tra diritto alla riservatezza e potere di controllo sulle informazioni personali*, in D. NEGRI (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 27 ss.

MORI P., *Convenzione europea dei diritti dell'uomo, Patto delle Nazioni unite e Costituzione italiana*, in *Riv. dir. int.*, 1983, p. 306 ss.;

MOSHIRNIA A. V., *Separating Hard Fact From Hard Drive: A Solution for Plain View Doctrine in Digital Domain,* 23 *Harv. J. Law & Tec.*, *609* (2010);

MOTZO G., *Contenuto ed estensione della libertà domiciliare*, in *Rass. dir. pubbl.*, 1954, II, p. 507 ss. ;

NEGRI D. (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007;

NICOSIA G., CACCAVELLA D. E., *Indagini della difesa e alibi informatico: utilizzo di nuove metodiche investigative, problemi applicativi ed introduzione nel giudizio*, in *Dir. Internet*, 2007, p. 525 ss.;

NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006;

NOBILI M., *Divieti probatori e sanzioni*, in *Giust. pen.*, 1991, III, c. 641 ss.;

NOBILI M., Sub *art. 189 c.p.p.*, in AA.VV., *Commento al nuovo codice di procedura penale*, coordinato da M. CHIAVARIO, tomo II, Torino, 1990, p. 387 ss.;

OHLER C., KLESCZEWSKI D., *Anmerkung BVerfG 2.3.2010*, in *JZ*, 2010, p. 25 ss.;

ORLANDI R., *Strafverfolgende oder vorbeugende Überwachung des Fernmeldeverkehrs und die Privatsphäre, Einsatz technischer Mittel, online Durchsuchung und das Recht auf informelle Selbstbestimmung*, *Congress on the Criminal Law Reforms in the World and in Turkey, atti del convegno internazionale svoltosi a Istanbul-Ankara dal 26 maggio al 4 giugno 2010, Istanbul 2010*, p. 23 ss.;

ORLANDI R., *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc*., 2009, p. 129 ss.;

ORLANDI R., *Note critiche, a prima lettura, in tema di giudizio immediato "custodiale" (art. 453 1° co. bis c.p.p.)*, in *Osservatorio del processo penale*, 2008, n. 3, p. 10 ss.;

ORLANDI R., *Lodo "Maccanico": attuazione dell'art. 68 Cost. e sospensione dei processi per le alte cariche. Profili di diritto processuale*, in *Dir. pen. proc.*, 2003, p. 1214 ss.;

ORLANDI R., *Garanzie individuali ed esigenze repressive (ragionando intorno al diritto di difesa nei procedimenti di criminalità organizzata)*, in AA. VV., *Studi in ricordo di Giandomenico Pisapia, Vol. II*, Milano, 2000, p. 545 ss.;

ORLANDI R*., Qualche rilievo intorno alla vagheggiata figura di un pubblico ministero europeo*, in L. PICOTTI (a cura di), *Possibilità e limiti di un diritto penale europeo*, Milano, 1999, p. 209 ss.;

PACE A., *Diritti «fondamentali» al di là della Costituzione*, in *Pol. dir.*, 1993, p. 3 ss.;

PACE A., *Problematica delle libertà costituzionali, Lezioni, Parte Speciale II*, Padova, 1985;

PACE A., *Art. 15*, in A. BRANCA (a cura di), *Commentario alla costituzione*, *Rapporti civili*, Bologna, 1975, p. 80 ss.;

PANZAVOLTA M., *Intercettazioni e spazio di libertà, sicurezza e giustizia*, in F. RUGGIERI, L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, p. 67 ss.;

PARODI C., *VoIP, Skype e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?*, in *Dir. pen. proc.* 2008, p. 1309 ss.;

PARODI C., *Le intercettazioni: profili operativi e giurisprudenziali*, Torino, 2002;

PAULESU P. P., *Notizia di reato e scenari investigativi complessi: contrasto alla criminalità organizzata, operazioni "sotto copertura", captazione di dati digitali*, *Riv. dir. proc*., 2010, p. 801 ss.;

PERETOLI P., *Controllo satellitare con GPS: pedinamento o intercettazione?*, in *Dir pen. proc.*, 2002, p. 93 ss.;

PERONI F. – GIALUZ M. (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009;

PICOTTI L., *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giur. merito*, 2012, p. 2522 ss.;

PICOTTI L., *Ratifica della Convenzione* Cybercrime *e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Dir. Internet* 2008, p. 437 ss.;

PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. Internet*, 2005, p. 189 ss.;

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, p. 21 ss.;

PICOTTI L., (voce) *Reati informatici*, in *Enc. giur. Treccani*, agg. VIII, Roma, 2000;

PINELLI C., *Sul trattamento giurisdizionale della CEDU e delle leggi con essa confliggenti*, in *Giur. cost.*, 2007, p. 3475 ss.;

PUGLIESE G., *Il diritto alla "riservatezza" nel quadro dei diritti della personalità*, in *Riv. dir. civ.*, 1963, p. 605 ss.;

PULITO L., *La circolazione della prova penale in Europa dopo il Trattato di Lisbona*, in *Giust. pen.*, 2010, p. 378 ss.;

QUADRI R., *Diritto internazionale pubblico*, Napoli, 1968;

REMAIN J. H., *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, in *11 Santa Clara Computer & High Tech. L. J. 27 (1995)*;

RICCI A. E., Digital evidence *e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc.*, 2010, p. 337 ss.;

RIEPL F., *Informationelle Selbstbestimmung im Strafverfahren*, Tübingen, 1998;

RODOTÀ S., *Il diritto di avere diritti*, Roma, 2012;

RODOTÀ S., *Libertà personale. Vecchi e nuovi nemici*, in M. BOVERO (a cura di), *Quale libertà. Dizionario minimo contro i falsi liberali*, Roma-Bari, 2004, p. 52 ss.;

RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995;

ROGGAN F., *Online-Durchsuchung – Rechtliche und tatsächcliche Konsequenzen des BVerfG – Urteils vom 27. Februar 2008, Berliner Wissenschaftsverlag, Juli* 2008;

ROXIN C., SCHÜNEMANN B., *Strafverfahrensrecht*, *26. Auflage*, München, 2009;

RUGGIERI F., *Profili processuali nelle investigazioni informatiche*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica*, Padova, 2004, p. 157 ss.;

RUGGIERI F., *Riprese visive e inammissibilità della prova*, in *Cass. pen.*, 2006, p. 3945 ss.;

RUGGIERI F., *Divieti probatori e inutilizzabilità della disciplina delle intercettazioni telefoniche*, Milano, 2001;

RUX J., *Ausforschung privater Rechner durch die Polizei – und Sicherheitsbehörden – Rechtsfragen der "Online-Durchsuchung"*, in *JR*, 2007, p. 285 ss.;

SALAZAR L., *La nuova convenzione sull'assistenza giudiziaria in materia penale*, in *Dir. pen. proc.*, 2000, p. 1664 ss.;

SARZANA DI S. IPPOLITO C., *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in *Dir. pen. proc.* 2008, p. 1562 ss.;

SCAGLIONE A., *Attività atipica di polizia giudiziaria e controllo satellitare*, in *Foro it.*, 2002, III, p. 635 ss.;

SCHANTZ P., *Verfassungsrechtliche Probleme von "*Online-*Durchsuchungen"*, in *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft* 2007, p. 343 ss.;

SCHRÖDER B. - SCHRÖDER C., *Die* Online-*Durchsuchungen. Rechtliche Grundlagen, Technik, Medienecho,* Telepolis 2008;

SEGER A., *The Budapest Convention 10 Years On: Lessons Learnt*, in S. MANACORDA (a cura di) *Cybercriminality: Finding a Balance Between Freedom and Security*, *ISPAC*, 2012, p. 167 ss.;

SIEBER U., *Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag*, München, 2012;

SIGNORATO S., *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. e proc. pen.*, 2012, p. 580 ss;

SLOBOGIN C., *Public Privacy: Camera Surveillance of Public Places and the Right to Anonimity*, in *72 Miss. L. J.*, 213 (2002-2003);

SOTIS C., *Convenzione europea dei diritti dell'uomo e diritto comunitario*, in V. MANES, V. ZAGREBELSKY, *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Milano, 2011 p. 110 ss.;

SPAFFORD E. H., in B. D. CARRIER, E. H. SPAFFORD, *Categories of digital investigation analysis techniques based on the computer history model*, *Digital Investigation*, 3, 2006, p. 121 ss.;

SPENCER J. R., *The problems of Trans-border Evidence and European Initiatives to Resolve Them*, in G. GRASSO, R. SICURELLA (a cura di), *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, Milano, 2008, p. 471 ss.;

STRAMAGLIA M., *Il pedinamento satellitare: ricerca ed uso di una prova "atipica"*, in *Dir. pen. proc.*, 2011, p. 213 ss.;

TEGA D., *L'ordinamento costituzionale italiano e il "sistema" Cedu: accordi e disaccordi*, in V. MANES, V. ZAGREBELSKY, *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Milano, 2011, p. 193 ss.

TESORIERO S., *Uno strano ordine di esibizione della corrispondenza sospeso tra sequestro ed intercettazione,* in *Cass. pen.* 2008, p. 673 ss.;

TESTA F., Cybercrime*, intercettazioni telematiche e cooperazione giudiziaria in materia di attacchi ai sistemi informatici*, 2005, p. 22, reperibile su sito *Persona e danno*, diretto da P. CENDON, *http://www.personaedanno.it/*;

TIBERI G., *Il diritto alla protezione dei dati personali nelle carte e nelle corti sovranazionali (in attesa del Trattato di Lisbona) (I parte)*, in *Cass. pen*., 2009, p. 4467 ss.;

TIBERI G., *Protezione dei dati personali e sicurezza dopo il Trattato di Lisbona*, in G. GRASSO – L. PICOTTI – R. SICURELLA (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, p. 515 ss.;

TONINI P., *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, p. 401 ss.;

TRANCHINA G., *Sequestro* (voce), in *Enc. giur. Treccani*, XXVIII, Roma, 1992, p. 6 ss.;

TROISI P., *Sequestro probatorio del computer e segreto giornalistico*, in *Dir. pen. proc.* 2008, p. 763 ss.;

TURCO E., *Legittimazione ed interesse ad impugnare in tema di sequestro preventivo: dualismo teorico?*, in *Cass. pen.*, 2003, p. 2382 ss.;

UBERTIS G., *Sistema multilivello dei diritti fondamentali e prospettiva abolizionista del processo contumaciale,* in *Giur. cost*., 2009, p. 4747 ss.;

VACIAGO G., Digital Evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, 2012;

VACIAGO G., *La disciplina normativa sulla* data retention *e il ruolo degli* Internet Service Provider, in L. LUPARIA (a cura di), Internet provider *e giustizia penale*, Milano, 2012, p. 141 ss.;

VALENTINI E., *La poliedrica identità del nuovo giudizio immediato*, in O. MAZZA, F. VIGANÒ (a cura di), *Misure urgenti in materia di sicurezza pubblica: (d.l. 23 maggio 2008, n. 92 conv. in legge 24 luglio 2008, n. 125)*, Torino, 2008, p. 281 ss.;

VASSALLI G., *La libertà personale nel sistema delle libertà costituzionali*, in *Scritti giuridici in memoria di P. Calamandrei*, V, Padova, 1958, p. 355 ss.;

VELANI L. G., *Nuove tecnologie e prova penale: il sistema di individuazione satellitare* g.p.s., in *Giur. it.*, 2003, p. 2375 ss.;

VENEGONI A., *Considerazioni sulla normativa applicabile alle misure investigative intraprese dal Pubblico Ministero Europeo nella proposta di regolamento COM (2013) 534*, in *www.penalecontemporaneo.it*;

VENTURINI S., *Sequestro probatorio e fornitori di servizi telematici*, in L. LUPARIA (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, p. 107;

VERVAELE J. A. E., *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.;

VITALE A., *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico* in *La ratifica della Convenzione del Consiglio d'Europa sul* cybercrime*: profili processuali*, in *Dir. Internet* 2008, p. 506 ss.;

WARREN S. D., BRANDEIS L. D., *The Right to Privacy*, in *Harv. L. Rev.*, 4 (1890), p. 193 ss.;

WILLIAMS C., *Overview of the Commission's proposal for a Framework Decision on the European evidence warrant*, in J. A. E. VERVAELE (a cura di), *European Evidence Warrant. Transnational Judicial Inquiries in the EU*, Antwerpen-Oxford, 2005, p. 69 ss.;

WINICK R.*, Searches and Seizures of Computers and Computer Data,* 8 *Harv. J. L. & Tec.* 75 (1994);

ZACCHÉ F., *La prova documentale,* Milano, 2012;

ZENO ZENCOVIC V., sub *Art. 8*, in S. BARTOLE, B. CONFORTI, G. RAIMONDI (a cura di), *Commentario alla Convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2011, p. 309 ss.;

ZICCARDI G., *L'ingresso della* computer forensics *nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, p.165 ss.;

ZICCARDI G., *Manuale breve di informatica giuridica*, Milano, 2006;

ZIEMMERMANN F., GLASER S., MOTZ A., *Mutual Recognition and its Implication for the Gathering of Evidence in Criminal Proceedings: a Critical Analysis of the Initiative for a European Investigation Order*, in *EuCLR*, 2011, p. 56 ss.;

ZÖLLER M. A., *Die Vorratsspeicherung von Telekommunikationsdaten – (Deutschen) Wege und Irrwege*, *Congress on the Criminal Law Reforms in the World and in Turkey, atti del convegno internazionale svoltosi a Istanbul-Ankara dal 26 maggio al 4 giugno 2010, Istanbul 2010*, p. 33.