UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Sede Amministrativa: Università degli Studi di Padova

Dipartimento di Diritto pubblico, internazionale e comunitario

SCUOLA DI DOTTORATO DI RICERCA IN GIURISPRUDENZA
CICLO XXIII

DIRITTO ALLA RISERVATEZZA E INDAGINI PENALI

Nuove dimensioni dell'indagine genetica e informatica

Direttore della Scuola : Chiar.mo Prof. Roberto E. Kostoris

Supervisore :Chiar.mo Prof. Roberto E. Kostoris

Dottoranda: Annaleda Galluzzo

SOMMARIO

PARTE PRIMA

CAPITOLO I

Origini ed evoluzione del diritto alla riservatezza nel quadro nazionale ed europeo

PARTE SECONDA

CAPITOLO I

La *privacy* e le indagini genetiche: bilanciamenti reciproci dopo la ratifica del Trattato di Prüm

CAPITOLO II

Tutela della riservatezza e indagini informatiche

PARTE PRIMA

INTRODUZIONE

Il diritto alla riservatezza è un diritto di seconda generazione, che si sviluppa in risposta a esigenze sorte nel contesto sociale con il progresso tecnologico, e segue un continuo processo di evoluzione parallelo alle nuove necessità di tutela connesse ai mutamenti economici, e allo sviluppo scientifico. Il contenuto del diritto alla *privacy*, dunque, si evolve di fronte alle trasformazioni tecnologiche del XX secolo.

Alla fine dell'Ottocento, infatti, le possibilità di incidere sulla sfera privata del soggetto erano limitate all'attività della stampa dei quotidiani e della fotografia. Pertanto, il dibattito teso ad affermare il diritto alla riservatezza era emerso in relazione alle aggressioni alla sfera intima operate dai mezzi di comunicazione e si era concentrato sulla divulgazione di notizie personali. Il diritto alla *privacy*, in questo contesto, assumeva un contenuto negativo e coincideva con il potere del singolo di impedire la pubblicizzazione e la conoscenza di fatti attinenti alla vita familiare e personale.

Alla fine del Novecento, tuttavia, il progresso scientifico nel campo informatico e dell'indagine genetica ha moltiplicato enormemente i rischi di violare la sfera privata individuale, poiché attualmente le scoperte tecnologiche permettono di memorizzare, gestire, conservare e far circolare una quantità enorme di dati sensibili, che possono riguardare non solamente il singolo ma un intero gruppo familiare nel caso di informazioni genetiche. Quindi, l'originario concetto di riservatezza come tutela dell'intimità

contro le aggressioni esterne, si arricchisce includendo anche il controllo sulla raccolta, elaborazione e circolazione dei dati personali.

La tutela del diritto alla riservatezza, così intesa, tuttavia, non ha carattere assoluto, dovendo essere sempre posta in bilanciamento con il contrapposto interesse collettivo all'acquisizione di elementi probatori nel procedimento penale. La vera difficoltà per il legislatore e l'interprete consiste nell'individuare un corretto punto di equilibrio tra l'esigenza di accertare i reati e la protezione della sfera privata del singolo.

In questa prospettiva, l'attenzione dovrà essere dedicata ai due settori maggiormente interessati oggi dalle istanze di riservatezza nel contesto di un processo penale informatico e genetico.

CAPITOLO I

Origini ed evoluzione del diritto alla riservatezza nel quadro nazionale ed europeo.

Sommario: 1. La genesi e il contenuto del diritto alla *privacy* - 2. La tutela della vita privata negli atti del Consiglio d'Europa e nella giurisprudenza della Corte Europea dei diritti dell'uomo - 3. Le fonti dell'Unione europea e l'opera della Corte di Giustizia: la riservatezza da garanzia strumentale alla realizzazione di un mercato comune a diritto fondamentale del cittadino dell'Unione - 4. Il riconoscimento del diritto alla riservatezza nell'ordinamento italiano e le prospettive di tutela nel processo penale.

1. La genesi e il contenuto del diritto alla *privacy*.

L'esigenza di tutelare la riservatezza individuale inizia a emergere, in dottrina, per la prima volta negli Stati Uniti alla fine del XIX secolo, in un momento storico di grandi mutamenti politici, economici e sociali.

Al fine di comprendere il motivo per cui il *right of privacy* sia stato teorizzato solo alla fine dell'Ottocento, giova ricordare che è il fenomeno dell'industrializzazione a mutare radicalmente lo stile di vita della collettività, favorendo l'urbanizzazione e stimolando la ricerca tecnologica. In tale quadro generale, il ceto borghese, che non ritiene più sufficiente tutelare la proprietà privata, comincia a sentire la necessità di proteggere anche la sfera intima. Pertanto, il diritto alla riservatezza inizialmente è teso

a proteggere interessi di natura elitaria ed è incapace di esprimere esigenze uniformemente diffuse nella massa dei cittadini[1].

La prima ricostruzione dottrinale del diritto in oggetto è pubblicata nel 1890 sulle pagine dell'*Harvard Law Review* da due giuristi, Louis Brandeis e Samuel Warren[2], i quali parlano di *privacy* come *right to be let alone* (diritto a essere lasciati soli)[3].Sebbene la tutela della *privacy* nasca come difesa di valori borghesi – in specie la rispettabilità messa in pericolo dai mezzi di stampa-, il merito di questi autori è di porre l'attenzione sull'esigenza di proteggere giuridicamente l'intimità della vita domestica di "ogni" individuo in generale (c.d. *inviolate personality*), ritenuta una delle "nuove esigenze" della società, che fino a quel momento proteggeva solo persona fisica e beni[4].

---

[1] S. NIGER, *Le nuove dimensioni della* privacy*: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006, p. 27; T. TRONCHIA, *Cenni problematici sulla tutele della vita privata nell'ordinamento giuridico italiano*, Cedam, Padova, 1990, p. 148.

[2] S. D. WARREN, L. D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, vol. IV, n.5, 1890, trad. it. S. Serra in V. FROSINI, *jus solitudinis*, Giuffrè, Milano, 1993, p. 52 e ss. In verità, il primo a parlare di diritto alla *privacy*, alla fine della diciannovesimo secolo, fu il giudice Thomas Cooley, che parlò, quasi incidentalmente, di diritto alla riservatezza nell'ambito di uno scritto trattatistico in materia di fatti illeciti. C.f.r. T. C. CLOONEY, *A Treatise on the Law of Torts or the Wrongs which Arise Indipendent of contract*, Challagan & Company, Chicago IL, 1888, p. 29.

[3] Anche se vi è chi ne propone una traduzione più estesa come diritto a essere lasciati in pace o tranquilli. N. LUGARESI, *Internet, privacy e pubblici poteri negli Stati uniti*, Giuffrè, Milano, 2000, p. 51.

[4] I due autori richiamano la nozione di proprietà applicandola, però, alla vita privata, svolta dal singolo all'interno delle mura domestiche. In altri termini, essi configurano il diritto alla riservatezza come un divieto di ingresso, uno *ius excludendi alios*, nello spazio domestico altrui, inteso come ambito che appartiene solo all'individuo. A. BALDASSARRE, Privacy *e costituzione. L'esperienza statunitense*, Roma, Bulzoni Ed., 1984, p. 16; S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, cit., p. 28. Numerosi sono le voci critiche sellevatesi nei confronti di tale ricostruzione giudicata troppo vaga. Si ricorda tra i molti E. J. BLUOSTEIN, *Privacy an as aspect of human dignity: an aswer: to Dean Prosser*, in *New York University Law Review*, 1964, vol. XXXIX, p. 970.

La tesi, tuttavia, non è immediatamente accolta a livello normativo e giurisprudenziale.

Le Corti statunitensi, infatti, solo a partire dai primi anni del novecento riconoscono alla *privacy* la valenza di diritto soggettivo autonomamente protetto[5]. In particolare, i profili di applicazione (soggettiva ed oggettiva) del diritto in esame sono stati progressivamente estesi grazie al *legal reasoning* espresso da giudici autorevoli in celebri *dissenting opinions*, utilizzate come base argomentativa fondamentale per quelle corti che, in momenti successivi si sono trovate a dover "rovesciare" (c.d. *overruling*) propri precedenti giudiziari che concepivano in senso restrittivo il diritto di cui trattasi[6].

Peraltro, questo processo di riconoscimento del diritto alla riservatezza era stato rallentato dal fatto che nella Costituzione americana non figura, nemmeno tra i suoi emendamenti, alcun riferimento esplicito a tale diritto

[5] La pronuncia che per prima accorda protezione alla riservatezza quale posizione giuridicamente rilevante «derivante dal diritto naturale» e dai valori costituzionali è pronunciata dalla Corte Suprema della Georgia nel 1905. [122 Ga. 190, 194, 50 S.E. 68, 70, 1905].

[6] Uno dei casi che sensibilizzò maggiormente il dibattito sul riconoscimento del diritto alla *privacy* fu *Olmstead vs. United States* del 1928, nel quale la Suprema Corte negò l'applicazione del IV Emendamento - che protegge ciascun individuo da perquisizioni e sequestri irragionevoli aventi a oggetto la persona, il domicilio, i documenti o i beni personali- in tema di intercettazioni telefoniche. La pronuncia in esame chiariva che per perquisizione si dovesse intendere solamente un'intrusione fisica dell'autorità pubblica in luoghi costituzionalmente protetti. Nel corso di tale processo, il giudice Braindeis pronunciò un'opinione dissenziente, in cui riprese e approfondì alcuni concetti già espressi nell'articolo scritto insieme a Warren. *Olstead vs. United States*, 277 U.S. 438, 1928. Solo nel 1967, in *Kantz vs United States*, la Suprema Corte riconosce, rovesciando la posizione espressa nella sentenza *Olmstead vs. United States* fornisce tutela alle aspettative di *privacy* di chi comunica privatamente per via telefonica, sul presupposto che il IV emendamento protegga non solo cose e luoghi, ma anche le persone.

né, vi erano leggi federali sul tema fino al 1974[7]. Fondamentale, allora, è stata l'attività ermeneutica della *Supreme Court* federale, poiché ha consentito di attribuire copertura costituzionale al diritto alla riservatezza[8] e di definirne di volta in volta il contenuto, adeguandolo ai mutamenti sociali e alle nuove coscienze scientifiche. Tale giurisprudenza si è imposta anche in virtù dell'operare del principio dello *stare decisis,* essendo tutti i giudici – federali e statali – vincolati ai principi di diritto da essa definiti.

La *privacy* si configura originariamente come esigenza di tutela della vita privata circoscritta all'interno delle mura domestiche e avvertita dal solo ceto borghese e continua a essere concepita in questo modo fino al secondo dopoguerra, quando inizia ad affermarsi il "modello della società di massa". Negli anni sessanta, infatti, si assiste a una poderosa rinascita dell'interesse alla protezione della riservatezza nonché al significato da attribuire alla medesima. Tuttavia, è l'evoluzione tecnologica, che a partire dal 1970 determina una diffusione capillare dei mezzi di informazione e un incremento esponenziale della quantità di dati personali raccolti da soggetti pubblici o privati (es. pratiche di *marketing*), a far diventare la *privacy* una istanza generalizzata, sentita dell'intera collettività[9].

La giurisprudenza statunitense, perciò, amplia le ipotesi in cui viene garantito il riserbo, riconoscendo margini di protezione anche in luoghi

[7] La prima legge federale volta a regolare il diritto alla riservatezza è il *Privacy act*, adottata nel 1974, che riconosce all'individuo il diritto di accedere, prendere visione e rettificare i propri dati personali detenuti da una *agency*.

[8] Molte pronunce ricercano la base giuridica per proteggere la sfera intima del soggetto nella Costituzione complessivamente considerata (es. *Griwold vs. Cunnecticut,* [381 U.S., 479, 1965]), mentre altre nel IV emendamento (es. *Kantz vs United States,* cit. e *Kyllo vs. United States,* [533 U.S. 27, 2001]).

[9] S. RODOTÀ, *La* privacy *tra individuo e collettività*, in *Pol. Dir.*, 1974, 3, p. 551.

diversi dal domicilio[10], giungendo nel tempo a ricostruire la riservatezza non solo come mero *ius excludendi alios*[11], ma come vero e proprio diritto di controllo dei (e sui) propri dati (c.d. *control over personal information*)[12]. Non si ritiene più che il diritto al riserbo sia circoscritto al solo potere di vietare qualsiasi circolazione di informazioni sul proprio conto, ma lo si estende anche al potere di vigilare su di essa, avendo la possibilità all'occorrenza di rettificare o cancellare i dati.

2. Le origini del percorso europeo per proteggere la riservatezza: la tutela della vita privata negli atti del Consiglio d'Europa e nella giurisprudenza della Corte Europea dei diritti dell'Uomo.

Nel continente europeo le prime fonti internazionali che riconoscono espressamente il diritto alla *privacy* sono la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950 (c.d. CEDU) e, successivamente, la Convenzione di Strasburgo n. 108 del 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati

[10] *Berber vs. Time, Incorporated, a Corporation*, 348 Mo. 1199, 159, S.W. 2d, 1942, 291, in cui la Corte Suprema del Missuri ha riconosciuto l'esistenza di un diritto alla riservatezza del paziente nella stanza d'ospedale, in precedenza negata perché area accessibile al pubblico. Estremamente significativa è anche la sentenza *Katz vs. United Stetes,* cit. in materia di intercettazioni telefoniche, nella quale la Corte Suprema federale [533, U.S. 27, 2001] ha sostenuto che la riservatezza non è circoscritta in modo spaziale ai soli luoghi di privata dimora, ma deve essere individuata anche con riferimento ai fatti che la persona ritiene privati.

[11] *United States Department of Justice vs. Reporters Comm. for freedom of the press,* [489 U.S. 749, 1989].

[12] Le teorie che definivano il diritto alla riservatezza come potere di controllo sui propri dati personali sono state recepite in parte dalla legislazione federale con il *Privacy Act* del 1974.

personali[13]; convenzione, questa, specificatamente finalizzata a fornire strumenti comuni per proteggere efficacemente i diritti inviolabili minacciati dalla invasività delle nuove tecnologie[14].

Nell'ambito della CEDU, invece, la riservatezza trova tutela generale nell'art. 8 che, al primo paragrafo, garantisce il diritto al rispetto della vita privata e familiare, mentre, al secondo, ne prevede la possibile compressione da parte della pubblica autorità unicamente per il

[13] Convenzione del Consiglio d'Europa n. 108 adottata il 20 gennaio 1981 a Strasburgo (cd. Convenzione di Strasburgo) diretta ad armonizzare le legislazioni degli Stati aderenti in tema di protezione delle persone in relazione al trattamento automatizzato dei dati a carattere personale. La ratifica della Convenzione da parte dei singoli Stati membri presupponeva l'approvazione di una normativa interna a protezione dei dati personali. L'Italia, pur avendo autorizzato la ratifica della Convenzione, non ha potuto a lungo procedervi per mancanza di una legislazione a tutela dei dati fino al 1995. Attraverso la promulgazione della legge 675/1995, in recepimento della direttiva comunitaria 95/46/CE, pertanto, il nostro Paese ha potuto adeguarsi agli *standards* di garanzia previsti della Convenzione, provvedendo alla ratifica.

[14] Nonostante la fondamentale importanza rivestita dalla CEDU, il Consiglio d'Europa, che ha rappresentato una delle sedi internazionali più attive nell'elaborazione normativa in tema di riservatezza, già alla fine degli anni '70 si interrogava, attraverso una questione posta dall'Assemblea parlamentare al Consiglio dei Ministri, sull'effettiva idoneità del solo art. 8 CEDU a proteggere gli individui da un utilizzo abusivo della tecnologia informatica in continuo sviluppo. A tal fine il Consiglio dei Ministri adottò due risoluzioni - Risoluzione n. (73)22 del 26 settembre 1973 e n. (74) 29 del 20 settembre 1974 -, che indicarono le linee guida sulla base della quali venne redatta la successiva Convenzione n. 108 del 1981. Tale accordo internazionale si concentra esclusivamente sulla tutela dei diritti in materia di trattamento automatizzato dei dati relativi alle persone fisiche e introduce alcuni principi fondamentali nel processo di creazione di un sistema normativo specifico di protezione dei dati. Alcuni principi della Convenzione saranno infatti ripresi, e spesso rafforzati e ampliati, dalla direttiva 95/46/CE e dalla legislazione italiana, come a es. il principio di esattezza con i connessi obblighi di aggiornamento e rettifica. G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, Giuffrè, Milano, 1997, p. 8 e ss.; S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 1995, p. 66.

perseguimento di rilevanti interessi pubblici quali, ad esempio, la sicurezza nazionale, l'ordine pubblico e la prevenzione dei reati[15].

La portata e il contenuto di questa previsione sono stati progressivamente definiti in via pretoria dalla Corte EDU[16] .

L'art. 8 CEDU, infatti, nel riconoscere espressamente l'interesse di ogni persona al rispetto della propria vita privata e familiare non ne definisce precisamente la nozione. Ciò ha consentito ai Giudici di Strasburgo di individuare i profili giuridicamente rilevanti del concetto di riservatezza, operando, di volta in volta, un bilanciamento con gli interessi contrapposti e tenendo conto delle nuove esigenze di tutela emerse in relazione all'evolvere delle tecnologie. Così, attraverso questa attività ermeneutica, i Giudici hanno attratto nell'ambito di applicazione dell'art. 8 CEDU anche la protezione dei dati personali e il potere di controllo sulla circolazione delle informazioni personali, fenomeni presi invece in considerazione esplicitamente dalla Convenzione 108/1981. L'elaborazione giurisprudenziale ha chiarito l'esistenza di uno stretto legame tra i due testi normativi, evidenziando come la protezione dei dati personali rappresenti un'applicazione specifica del diritto alla riservatezza[17]. Pertanto, rientra nella protezione dell'art. 8 «qualsiasi limitazione al rispetto della vita

[15] Il testo dell'art. 8 CEDU recita: «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

[16] Corte Eur., *X eY c. Paesi Bassi*, 26 marzo 1985, la quale definisce il diritto alla *privacy* quale diritto del singolo a vivere gli aspetti più intimi della propria esistenza al riparo da interferenze di terzi, avendo predisposto l'ordinamento giuridico le misure necessarie a garantirne una tutela piena ed effettiva.

[17] Corte Eur., *Z. c. Finlandia*, 25 febbraio 1997.

privata[18]» che avvenga in materia di trattamento dei dati personali attraverso il ricorso a tecniche di investigazione o di controllo invasive della sfera intima[19].

Nel 1987, per la prima volta, una sentenza della Corte Europea affronta il problema della raccolta, archiviazione e utilizzo di dati personali ad opera dell'autorità pubblica - nel caso di specie forze di *intelligence* - quale attività lesiva della vita privata del ricorrente[20], e fa arretrare la tutela della *privacy* al momento del semplice reperimento[21] e catalogazione delle informazioni[22], a prescindere da un loro successivo uso[23].

I giudici di Strasburgo, inoltre, hanno ritenuto anche la raccolta di dati di natura pubblica rilevante ai fini della potenziale lesione dell'art. 8 CEDU[24],

---

[18] In tal senso Corte Eur., *Khan c. Regno Unito*, 15 maggio 2005.

[19] Analizzando la giurisprudenza della Corte è possibile affermare che la protezione dei dati *ex* art. 8 CEDU si estende a tutte le operazioni che possono essere con questi compiute, *id est* raccolta, registrazione, conservazione, impiego, trasferimento, divulgazione, rettifica o cancellazione. Simile problema si pone in particolar modo con riferimento ai dati digitali raccolti nel corso delle indagini di polizia svolte in rete Intenet, come ad esempio capita con le informazioni ricavabili dai *social network*. A titolo esemplificativo *Leander c. Svezia* del 26 marzo 1987 e *Rotaru c. Romania* del 4 maggio 2000.

[20] Corte Eur., *Leander c. Svezia*, 26 marzo 1987, la quale nello specifico esaminava il caso di un *dossier* delle forze di polizia, il cui contenuto aveva determinato conseguenze negative nella vita lavorativa del ricorrente.

[21] Tali conclusioni naturalmente non assumono valore nelle ipotesi in cui ricorrano le ragioni di sicurezza e ordine pubblico individuate dall'art. 8 comma 2 CEDU, che giustificano la compressione della sfera di riserbo individuale.

[22]Corte Eur., *Leander c. Svezia*, cit., «la memorizzazione da parte di un'autorità pubblica dei dati relativi alla vita privata di un individuo costituisce una ingerenza ai sensi dell'art. 8. L'utilizzazione ulteriore delle informazioni memorizzate *importe peu*» In senso conforme si segnalano anche Corte Eur., *Kopp c. Svizzera*, 23 marzo 1998.

[23] Corte Eur., *Amman c. Svizzera*, cit., «basta constatare che i dati relativi alla vita privata sono stati raccolti da una autorità pubblica» per concludere che la loro sistemazione e la conservazione «costituiscono una ingerenza, ai sensi dell'art. 8». In senso analogo anche Corte Eur., *Rotaru c. Romania*, 4 maggio 2000.

[24] Corte Eur., *Leander c. Svezia*, cit.; Corte Eur., *Amman c. Svizzera*, cit.

qualora siano schedati e memorizzati sistematicamente in banche dati o registri tenuti da organi pubblici[25].

Quello che rileva è la archiviazione metodica o permanente[26] del dato personale o di dati anche inizialmente estranei alla sfera privata o sensibile[27], poiché informazioni di per sé neutre possono, grazie alle nuove tecnologie, soprattutto se aggregate e incrociate, originare intromissioni indebite nella vita altrui[28]. È dovere dello Stato in generale impedire la divulgazione indebita di informazioni personali nonché consentire all'interessato accesso e rettifica dei dati raccolti, che lo riguardano[29]. Infatti, la Corte spesso considera la mancata conoscenza del trattamento da parte dell'interessato, il denegato accesso, oppure la mancata possibilità di

[25] Corte Eur., *Rotaru c. Romania,* cit..

[26] Un aspetto particolarmente problematico, infatti, è la durata della conservazione dei dati personali in specie se genetici o digitali. Cfr. in tal senso Corte Eur., Bouchacourt c. Francia, *Gardel c. Francia* e *M.B. c. Francia*, 17 dicembre 2009.

[27] Corte Eur., *Perry c. Regno Unito*, 17 luglio 2003, e Corte Eur., P.G. e J.H. c. Regno Unito, 25 settembre 2001, .

[28] È dato personale «qualsiasi informazione relativa alla persona fisica determinata e determinabile» ex art 2 Conv. Strasburgo. A giudizio della Corte Europea dei diritti dell'uomo sussiste una particolare tipologia di dati il cui trattamento deve avvenire nel rispetto della massima riservatezza e sicurezza, tra i quali spiccano le informazioni concernenti lo stato di salute della persona (Corte Eur., *M sc. c. Svezia*, 27 agosto 1997). Sulla scorta di simili osservazioni con un ragionamento *a fortiori*, i Giudici di Strasburgo hanno statuito che, oltre alle impronte digitali, i campioni di materiale organico e i profili genetici del DNA, rientrano nella nozione di dato sensibile poiché contengono informazioni che consentono di giungere non solo all'identificazione del soggetto ma alla sua appartenenza a un gruppo familiare o addirittura all'individuazione di talune patologie genetiche (Corte eur., *S. e Marper c. Regno Unito*, 4 dicembre 2008).

[29] Sempre in questo quadro, peraltro, il Consiglio d'Europa ha approvato la Convenzione sulla criminalità informatica, promulgata a Budapest il 23 novembre 2001, recentemente ratificata anche dal nostro Paese con legge 18 marzo 2008, n. 48. Merita, inoltre, di essere segnalato, nell'ambito del percorso svolto dalle Nazioni europee per garantire la riservatezza, il Trattato di Prüm del 1985 (c.d. Schengen II), accordo multilaterale, negoziato e concluso da alcuni tra gli stati membri dell'Ue al di fuori dello spazio giuridico della stessa, che si è occupato della cooperazione transfrontaliera in relazione alla lotta al terrorismo, alla criminalità e alla migrazione illegale

modificare o cancellare le informazioni personali quali elementi rilevanti per accertare una violazione della riservatezza[30].

Il diritto fondamentale alla *privacy*, così come delineato nel suo contenuto, però, non è garantito in modo assoluto, poiché, come anticipato, l'art. 8, paragrafo 2, CEDU ne ammette la possibile restrizione da parte della pubblica autorità. Infatti, se in generale grava sullo stato l'obbligo di astenersi dall'interferire nella vita privata e familiare dei propri cittadini, gli unici interventi restrittivi ammessi dai giudici di Strasburgo son quelli rientranti nel c.d. margine di apprezzamento statale[31], vale a dire quegli interventi previsti dalle normative vigenti nello Stato che, però, si sostanziano in misure necessarie in una società democratica a perseguire interessi collettivi (quali la sicurezza nazionale, l'ordine pubblico, il benessere economico, la prevenzione dei reati) o individuali (la protezione di diritti e libertà altrui)[32].

Al fine di stabilire la legittimità dell'interferenza, il giudice europeo svolge un bilanciamento tra gli opposti interessi in gioco[33], valutando se la misura adottata dalla Stato aderente, oltre che provvista di una base legale, sia proporzionata e necessaria per proteggere gli interessi pubblici indicati nella clausola derogatoria (art. 8 paragrafo 2 CEDU) [34]. In base alla giurisprudenza della Corte, però, la compressione della sfera intima da parte del potere pubblico è giustificabile se accanto ai tre criteri della conformità alla legge statale di una Nazione firmataria (principio di

[30] Corte Eur., *Rotaru c. Romania*, cit.
[31] U. KILKELLY, The Right to Respect for Private and Family Life. A Guide to the Implementation of Article 8 of European Convention on Human Right, Strasburgo, 2003, p. 8 e ss..
[32] A. BLASI, *La protezione dei dati personali nella giurisprudenza della Corte Europea dei diritti dell'uomo,* in *Riv. Trim .dir. u.,* 1999, p. 543
[33] Corte Eur., *S. e Marper c. Regno Unito*, 4 dicembre 2008.
[34] Corte Eur., *Leander c. Svezia*, cit.

legalità)[35], del perseguimento di un fine legittimo (principio di legittimità)[36] e della necessità in una società democratica (principio di proporzionalità)[37] sia simultaneamente soddisfatto anche il principio della temporaneità della misura stabilito nella Convezione 108/1981[38].

In altri termini, un'azione statale invasiva della riservatezza individuale è legittima solo quando sia prevista e conforme alla legge, essendo diretta a conseguire uno scopo meritevole di tutela (quale la difesa dell'ordine pubblico) e risultando congrua a raggiungere lo scopo perseguito. Le misure restrittive applicate, tuttavia, dovranno sempre mantenere il carattere della temporaneità senza tradursi in vincoli indeterminati, eccessivamente afflittivi per i diritti individuali, in specie la *privacy*.

Tale è il contenuto del diritto di riservatezza delineato nel sistema CEDU, ma è ancora parzialmente controversa la portata e l'efficacia della Convenzione all'interno del sistema giuridico interno.

Nelle sentenze della Corte Costituzionale nn. 348 e 349 del 2007[39] si è affermato che il novellato art. 117 c. 1 Cost. posiziona le norme CEDU ad

---

[35] Corte Eur., *Malone c. Regno Unito*, 2 agosto 1984. Merita, tuttavia, di essere presa in considerazione la recente pronuncia Corte Eur., U. c. Germania, 02 settembre 2010 adottata in tema di pedinamenti tramite il sistema GPS. In essa i Giudici hanno ritenuto legittima questa metodica, all'atto di verificare se l' interferenza di simile tecnologia con la vita privata del soggetto investigato fosse ammissibile perché prevista previamente dalla legge e proporzionata. Al riguardo la Corte rileva che, pur non essendo il sistema GPS previsto a livello normativo, esso debba considerarsi meno intrusivo di altri (l'intercettazione di comunicazioni) che sono disciplinati dalla legge. Inoltre, la condizione della preventiva previsione legislativa era da ritenersi soddisfatta per il fatto che doveva ragionevolmente preventivarsi che i progressi della tecnologia avrebbero consentito questo tipo di investigazioni.

[36] Corte Eur., *L.L. c. Francia*, 10 ottobre 2006

[37] Corte Eur, *Handyside c. regno Unito,* 1976, ove si specifica che l'ingerenza appare necessaria in una società di tipo democratico quando l'interesse perseguito risulti proporzionato rispetto al diritto sacrificato.

[38] Corte Eur., *S. e Marper c. Regno Unito*, cit.

[39] C.Cost. sent. 348/2007 in *www.giurcost.org*: C. Cost. 349/2007, *ivi*; in senso conforme C. Cost. . 239/2009,*ivi*; C. Cost. 93/2010, *ivi.*

un livello gerarchico interposto tra la legge ordinaria e la Costituzione[40]. Si è escluso, per converso, che le disposizioni della stessa Convenzione possano avere diretta applicazione nell'ordinamento interno in forza dell'art. 11 Cost. e che il giudice nazionale possa disapplicare la normativa interna contrastante con essa senza sollevare questione di legittimità costituzionale. Queste conclusioni sono state messe nuovamente in discussione dalle disposizioni sui diritti fondamentali contenute nell'art. 6 Trattato sull'Unione europea, come riformato dal Trattato di Lisbona.

La dottrina e la giurisprudenza nazionali si interrogano sugli effetti dell'entrata in vigore del Trattato di Lisbona nel sistema di tutela dei diritti individuali per capire se le innovazioni introdotte da questo abbiano comportato il mutamento della collocazione delle norme della Convenzione europea nel sistema delle fonti del diritto.

Due sono le teorie che si contendono il campo. Secondo la posizione dominante, la previsione normativa di cui al paragrafo 2 dell'art. 6 TUE pone le basi per l'adesione dell'UE alla CEDU [41] e assume rilevanza sotto un duplice profilo. Per un verso, è presumibile che la futura adesione

---

[40] L'interpretazione dell'art. 117 Cost. è stata molto controversa in dottrina ed esclusivamente l'intervento chiarificatore della Consulta ha posto fine al dibattito, definendo il rapporto esistente tra Convenzione e ordinamento interno. In particolare, secondo l'opinione dominante in dottrina, la conseguenza derivante dall'inclusione nel testo costituzionale del riferimento agli «obblighi internazionali» è rappresentata dal fatto che le norme interne di adattamento non possono più ora essere modificate o abrogate dalle leggi ordinarie successive, costituendo addirittura parametro interposto per valutare la legittimità costituzionale delle leggi ordinarie posteriori. F. SORRENTINO, *Nuovi profili costituzionali dei rapporti tra diritto internale, internazionale e comunitario*, in *Dir. Pubbl. Comp. Eur*., 2002, p. 1359.

[41] Esso stabilisce che "l'Unione aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Tale adesione non modifica le competenze dell'Unione definite nei Trattati". La scelta di introdurre una simile disposizione nel testo del Trattato sull'Unione europea nasce dalla circostanza che, nel 1996, la Corte di Giustizia CE espresse parere contrario a che Comunità europea potesse aderire alla CEDU. Parere n. 2/94 del 28 marzo 1996 *sull'adesione dalla Comunità alla Convenzione europea per la salvaguardia dei diritti dell'uomo,* in *Racc.*, p. I-1758.

potenzierà il sistema di tutela giurisdizionale dei diritti individuali, riconoscendo un ruolo anche alla Corte europea dei diritti dell'uomo. Per l'atro, la Convenzione assumerà una nuova posizione nel sistema delle fonti dell'UE, in virtù della quale potrà avere diretta applicazione all'interno degli ordinamenti degli Stati membri[42]. La Consulta con la sentenza 80 del 2011[43], in cui ha negato l'avvenuta "comunitarizzazione" della Convenzione Europea, contraddicendo in modo aperto alcune decisioni giurisprudenziali e impostazioni dottrinali che avevano ritenuto i principi CEDU direttamente applicabili nel nostro ordinamento, in quanto entrati a far parte di quel sistema di valori comunitari che informano l'intera attività legislativa dell'Unione, ha aderito a questa ricostruzione[44]. La tesi avvallata dalla Consulta pare preferibile poiché la teoria volta a riconoscere diretta applicabilità alla Convenzione negli ordinamenti degli Stati membri con conseguente disapplicazione di ogni disposizione interna

[42] Infatti, la Corte di Giustizia ha affermato che le norme dei Trattati stipulati dall'Unione possono avere efficacia diretta negli ordinamenti delle Nazioni aderenti, purché si dimostri che la natura e la struttura dell'accordo permettono di riconoscere effetti diretti alle sue disposizioni e che la norma presa in considerazione e sufficientemente precisa. In ogni caso sarà il tenore dell'accordo di adesione alla CEDU a determinare entro quali limiti i singoli cittadini potranno invocare la Convenzione dinnanzi alle autorità giudiziarie nazionali o dell'Unione. L. DANIELE, *Diritto dell'Unione europea. Sistema istituzionale, ordinamento, tutela giurisdizionale, competenze*, Giuffrè, Milano, 2010, p. 220.

[43] C. Cost., 11 marzo 2011, n. 80 in *giurcost.org*

[44] Le sentenze a cui si fa riferimento sono Cons. Stato, sez. IV, 2 marzo 2010, n. 1220, in *Guida al diritto*, n.14, 2010, 88 ss. e Tar Lazio, sez. II, 18 maggio 2010, n. 11984, in *Riv. giur. edilizia*, n. 4, 2010, 1259. Esse hanno interpretato le previsioni del Trattato di Lisbona nel modo più ampio possibile, riconoscendo a pieno titolo la possibilità di applicare il diritto convenzionale "comunitarizzato" senza il preventivo vaglio di costituzionalità svolto dalla Corte Costiuzionale. Un commento, in toni peraltro critici alle sentenze è stato svolto da A. CELOTTO , Il Trattato di Lisbona ha reso la CEDU direttamente applicabile nell'ordinamento italiano? in www.giustamm.it; G. COLAVITTI, C. PAGOTTO, *Il Consiglio di Stato applica direttamente le norme CEDU grazie al Trattato di Lisbona: l'inizio di un nuovo percorso?, Guida al diritto*, n.14, 2010, 88 ss; L. D'ANGELO, *"Comunitarizzazione" dei vincoli CEDU in virtù del Trattato di Lisbona? No senza una* expressio causae, in www.forumcostituzionale.it.

contrastante, implica l'utilizzo da parte del giudice nazionale di strumenti interpretarvi molto delicati rispetto al nostro sistema costituzionale, fondato su in sindacato accentrato e non diffuso[45].

3. Le fonti dell'Unione europea e l'opera della Corte di Giustizia: la riservatezza da garanzia strumentale alla realizzazione di un mercato comune a diritto fondamentale del cittadino dell'Ue.

Come noto, i Trattati Istitutivi delle Comunità Europee e dell'Unione Europea non contenevano alcuna clausola volta a tutelare in via specifica i diritti fondamentali (quale quello alla riservatezza). Tuttavia, ciò non implicava affatto che l'ordinamento Europeo, pur incentrato sulla protezione delle libertà economiche, fosse estraneo a forme di tutela dei diritti fondamentali, in ragione, soprattutto, dell'affermazione del principio di prevalenza del diritto comunitario su quello dei singoli Stati, dell'implementazione della «tradizioni costituzionali comuni» di cui all'art. 6 del TUE approvato a Maastricht nel 1992 e, in particolare, della giurisprudenza della Corte di Giustizia. Così, si comincia ad apprestare tutela alla *privacy*, nel 1990, in modo strumentale al perseguimento delle

[45] Il problema principale dell'ammettere l'applicazione diretta delle disposizioni CEDU nell'ordinamento italiano sarebbe proprio rappresentato dal fatto di "passare da un sindacato costituzionale accentrato a uno diffuso" con conseguenze di difficile gestione. Forse la tesi dell'applicazione diretta sarebbe praticabile dopo una riforma costituzionale che attribuisca al Giudice delle Leggi la competenza a esprimersi su questioni pregiudiziali di interpretazione (come la Corte di Giustizia) e attribuendo all'individuo il potere di adire direttamente la Corte costituzionale, laddove ritenga di aver subito una lesione di un diritto fondamentale.

politiche comunitarie della libera circolazione di merci, persone e servizi[46], trovando espressione specialmente negli atti di diritto europeo derivato.

Infatti, l'adozione negli Stati membri di proprie e diversificate normative interne in tema di riservatezza, con particolare riferimento alla protezione dei dati personali, costituiva un ostacolo al raggiungimento dei menzionati obiettivi, in quanto rendeva disomogenei gli *standards* di garanzia sul territorio europeo. Il crescente interesse alla realizzazione di un mercato comune determinava l'esigenza di apprestare una disciplina uniforme a tutela dalla aumentata mole di dati personali trasmessi senza alcuna limitazione a causa dell'abbattimento delle barriere economiche, voluta dalle istituzioni europee.

Quindi, per motivi prevalentemente economici, le direttive 95/46/CE[47] e 97/66/CE [48]garantiscono la riservatezza nella dimensione di libertà di circolazione dei dati[49]. La prima fonte, pur richiamando la CEDU e la Convenzione 108/1981, ha un ambito applicativo più vasto di quest'ultima e regola qualsiasi trattamento di dati anche non automatizzato o relativo ad

[46] Cf.r. art. 23 (ex art. 9) e ss. del Trattato che istituisce la Comunità europea sottoscritto a Roma il 27 marzo 1957, come modificato dal Trattato di Unico Europeo firmato a Maastricht il 7 febbraio 1992, ratificato con l. 3 novembre 1992, in *G. U.*, 24 novembre 1992, n. 227, suppl. ord., e dal Trattato di Amsterdam sottoscritto il 2 ottobre 1997, ratificato con l. 16 giugno 1998, *ivi*, 6 luglio 1998, n. 155, suppl. ord.

[47] Il riferimento è alla Direttiva del Parlamento europeo e del Consiglio 95/46 del 23 novembre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di essi in *G.U.C.E. L 281/31*, del 23 novembre 1995. Da tale direttiva in Italia ha tratto spunto l'abrogata legge sul trattamento dei dati personali l. n. 675/1996 (oggi sostituita dal cd. Codice della *Privacy* d. lgs. 196/03).

[48] La successiva direttiva del Parlamento europeo e del Consiglio 97/66 del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni ha avuto il compito di tradurre i principi della citata direttiva in norme specifiche per il settore delle telecomunicazioni, in *G.U.C.E. 24/l*, del 30 gennaio 1998

[49] artt. 14 , 95 e 286 del Trattato CE.

archivi elettronici[50], perseguendo l'obiettivo di bilanciare la tutela della vita privata con l'esigenza di tutelare una libera circolazione delle informazioni tra le Nazioni dell'Unione, propedeutica a consentire la libera circolazione di persone, beni e servizi in un mercato comune[51]. La seconda, invece, risponde alle esigenze specifiche poste con riguardo alla tutela dei dati personali e della vita privata degli utenti dall'introduzione di nuove tecnologie avanzate in materia di telecomunicazioni, legata soprattutto alla diffusione della rete internet, che, rivoluzionando le strutture di mercato e le metodiche di comunicazione, creava nuovi pericoli per la sfera privata dei singoli.

Se attraverso l'emanazione di queste direttive il legislatore europeo tenta di armonizzare le normative degli Stati membri in materia di *privacy* nel settore delle comunicazioni elettroniche al fine si eliminare gli ostacoli nel mercato comune, questa prospettiva nel corso degli anni muta. Infatti, la protezione dei dati personali, anziché essere legata primariamente a ragioni di politica economica, risulta nel tempo sempre più connessa a motivi di pubblica sicurezza e lotta contro la criminalità organizzata. Tale è l'obiettivo sotteso all'approvazione della successiva normativa europea di diritto derivato sia in tema di gestione e conservazione delle dati personali in materia di comunicazioni elettroniche (direttiva 2002/58/CE[52],

---

[50] U. DE SIERVO, *Tutela dei dati personali,* in *Diritti, Nuove tecnologie, trasformazioni sociali. Scritti in memoria di P. Barile,* Cedam, Padova, 2003, p. 299.

[51] M. MIGLIAZZA, *Profili internazionali ed europei del diritto all'informazione e alla riservatezza,* cit., p. 36 e ss.

[52] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, in G.U.C.E., 31 luglio 2002, L201/37, *(c.d. direttiva "e-privacy")* relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, intervenuta a modificare e integrare la precedente direttiva 97/66/CE in materia di telecomunicazioni su rete pubbliche e *privacy* e modificata dalle successive direttive 2006/24/CE e 2009/136/CE. Essa nel dare applicazione ad alcune disposizioni contenute nella direttiva 46/95/CE, ha imposto agli Stati membri di

2006/24/CE[53] e 136/2009/CE[54]), sia in tema di scambio di informazioni genetiche[55].

È, però, con la Carta dei diritti dell'Unione Europea (cd. Carta di Nizza)[56], che l'Unione disciplina ampiamente e compiutamente il diritto inviolabile di ogni individuo alla riservatezza, predisponendo due distinti articoli volti a garantire la vita privata (art. 7) e la protezione dei dati personali (art. 8)[57]. Ciò, anche se i diritti fondamentali in essa enunciati, pur

---

proteggere la riservatezza delle comunicazioni su reti pubbliche e di vietare la conservazione dei dati relativi al traffico generati nel corso di esse, eccettuate le ipotesi di conservazione espressamente autorizzate . Essa ha, infatti, tra i suoi obiettivi la sicurezza dei dati raccolti intesa sia come tutela in caso di perdita, distruzione o diffusione non autorizzata sia come difesa dell'ordine pubblico e della collettività.

[53] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 13 aprile 2006 in *G.U.C.E.*, L 105 (cd. direttiva "*data retention")*, 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.

[54] Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, in *G.U.C.E.*, 31 luglio 2002, L201/37.

[55] Decisione quadro del Consiglio 2006/615/GAI in cui si precisa che l'atto contiene "disposizioni basate sulle principali disposizioni del Trattato di Prüm", accordo internazionale che svolge un ruolo fondamentale nella disciplina dello scambio di informazioni genetiche, concluso il 27 maggio 1985 con lo scopo di rafforzare la cooperazione tra gli stati nella lotta al terrorismo, alla criminalità transfrontaliera e alla migrazione illegale. Esso, nonostante sia stato concluso e negoziato al di fuori dello spazio giuridico dell'Ue solamente da alcuni Stati membri (Belgio, Germania, Francia, Spagna, Lussemburgo, Paesi Bassi e Austria), viene in quest'ultimo "trasposto" con la decisione 2008/615/GAI adottata da quindici Stati membri unitamente alla decisione 2008/616/GAI, attuativa della prima. In questo modo le disposizioni del Trattato di Prüm entrano a far parte a tutti gli effetti della legislazione dell'Ue con particolare attenzione agli scambi di informazioni relativi ai profili di DNA e al relativo obbligo di creazione e gestione di data base nazionali. A. MUSUMECI, *La ratifica del Trattato di Prüm*, in L. MARAFIOTI e L. LUPARIA, *Banca dati del DNA e accertamento penale*, Giuffrè, Milano, 2010, p. 19 e ss.

T.A. AULETTA, Riservatezza e tutela della personalità

[56] Carta dei diritti fondamentali dell'Unione europea, *G.U.C.E,* 18 dicembre 2000, C364/1.

[57] Rispetto all'art. 8 CEDU, la scelta, fatta nella Carta di Nizza, di approntare una protezione separata a situazioni diverse, in cui il singolo definisce la propria sfera personale, consente di recepire un ricchissimo patrimonio giurisprudenziale elaborato nel corso dei decenni dalla Corte Europea con le proprie decisioni, che hanno fornito una lettura "vivente" del testo elaborato nel 1950 al passo con l'evoluzione sociale,

ispirando l'azione dell'Unione, non erano formalmente vincolanti e il loro rispetto era rimesso alla discrezione delle Istituzioni e della Corte di Giustizia.

Tuttavia, è solo con il Trattato di Lisbona che, in una prospettiva di rafforzamento dei meccanismi di tutela delle libertà personali, si colloca la Carta dei diritti fondamentali al livello più alto nell'ordinamento dell'Unione, attribuendogli lo stesso valore giuridico dei Trattati Istitutivi[58]. Ne deriva un vincolo diretto non solo per il legislatore europeo, ma anche per il legislatore nazionale in sede di attuazione degli obblighi comunitari ed in questo contesto la Corte di Giustizia viene ad assumere un importante ruolo di custode dei diritti fondamentali.

La nuova collocazione attribuita alla Carta ha, peraltro, un'altra conseguenza importante, legata al fatto che essa, nel richiamare la CEDU, pone una clausola di equivalenza, secondo cui, laddove la stessa Carta contenga «diritti corrispondenti a quelli garantiti» dalla Convenzione, il significato e la portata da attribuire ad essi «sono uguali a quelli conferiti dalla suddetta Convenzione»[59]. Sicché le prescrizioni contenute nella Carta e inerenti il diritto alla *privacy* possono essere recepite tenendo conto del valore e contenuto loro conferito dal testo della Convenzione e dall'interpretazione della Corte di Strasburgo.

---

economica e culturale. F. PIZZETTI, *La* privacy *come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in P. BILANCIA, M. D'AMICO, *La nuova Europa dopo il Trattato di Lisbona*, Giuffrè Milano, 2011, p. 85

[58] L'art. 6 del Trattato sull'Unione (ex art 6 TUE) -che recepisce i principi e le libertà sancite nella Carta di Nizza e prevede l'adesione dell'UE alla CEDU - ha costituito il passaggio essenziale e finale *dell'iter* che ha portato a riconoscere la *privacy*, e in particolare la protezione dei dati personali, quale diritto fondamentale del singolo nel sistema del diritto europeo. N. PARISI, *Funzione e ruolo della Carta di diritti fondamentali nel sistema delle fonti alla luce del Trattato di Lisbona,* in *Dir. Un. Eur.*, 2008, p. 653.

[59] La Carta di Nizza contiene un espresso riferimento alla CEDU sia al citato art. 52, par. 3, sia e all'art. 53, in cui introduce una clausola di compatibilità.

Sulla scorta di queste considerazioni, non la CEDU quale atto di diritto internazionale, ma le norme in essa contenute e richiamate dalla Carta dovrebbero, da un lato, costituire parametro di legittimità del diritto derivato dell'Unione e, dall'altro, divenire direttamente efficaci nei settori dell'ordinamento interno attuativi del diritto dell'Unione. Per cui, la Convenzione non assume efficacia diretta in tutto l'ordinamento nazionale nemmeno per il tramite della Carta di Nizza, restandone fuori sia nei settori di esclusiva competenza nazionale sia in quelli di competenza concorrente in cui non sono intervenuti atti normativi dell'Unione.

La Corte di Giustizia avrà presumibilmente un ruolo determinante nel processo espansivo della sfera di pertinenza dell'Unione come già aveva fatto anteriormente all'adozione della Carta di Nizza e all'approvazione del Trattato di Lisbona, recependo alcuni principi affermati dalla Corte di Strasburgo[60] e ponendo le basi per la "costruzione", all'interno dell'UE, della *privacy* quale diritto fondamentale autonomo.

In tal senso i Giudici di Lussemburgo hanno dato un apporto determinante al processo di emersione del diritto alla riservatezza grazie all'adozione di interpretazioni estensive del diritto europeo, che riconoscevano tutela alla riservatezza, richiamando l'art. 8 CEDU non solamente in casi in cui sussisteva un collegamento con il diritto dell'Unione. In alcune decisioni, infatti, tale rinvio serviva alla Corte di giustizia come supporto per operare una lettura estensiva della normativa

[60] Autorevole dottrina, all'indomani della proclamazione della Carta di Nizza osserva come l'Europa da tempo abbia «(se non una «Carta dei diritti») un proprio «catalogo dei diritti», la cui la costruzione è iniziata nel 1969 con la sentenza C-29/69 della Corte di giustizia» e continuata nel corso di un trentennio. Tale catalogo era richiamato dall'art. 6, comma 2, del Trattato dell'Unione , prima introdotto a Maastricht e poi confermato ad Amsterdam A. BARBERA, cit., p. 241. Più recentemente in tal senso sul ruolo della Carta di Nizza anche M. CARTABIA, *Il Trattato di Lisbona,* in *Giornale dir. amm.*, 2010, fasc. 3, p. 221

dell'Ue[61]. Nella causa *Bodil Lindquist c. Aklagarkammaren i Jönköping*, con riferimento alla direttiva 95/46, i Giudici di Lussemburgo affermano che la portata della disciplina nazionale può essere ampliata a settori che non risultano compresi nell'ambito applicativo della direttiva stessa, nel caso di specie al trasferimento telematico di dati, purché ciò non entri in contrasto con altre norme europee[62].

4 . Il riconoscimento del diritto alla riservatezza nell'ordinamento italiano e le prospettive di tutela nel processo penale.

In Italia, le prime costruzioni dottrinali sul diritto alla *privacy* si sono avute solo cinquant'anni dopo il celebre studio di Warren e Braindeis, poiché lo sviluppo industriale nel nostro Paese è avvenuto in un'epoca successiva rispetto a quello americano[63].

Esattamente come l'ordinamento statunitense, anche quello nazionale non tutelava esplicitamente il diritto alla *privacy* né in Costituzione né a livello

[61] H. LABAYLE, *Le droit des étrangers au regroupement familial, regards croisés du droit interneet du droit européen*, in *Revue Française de Droit Administratif*, 2007, fasc. 1, p 110. Tale autore, nel commentare la sentenza della Corte di Giustizia del 27 giugno 2006, C-540/03, precisa che la Carta di Nizza assume un ruolo meramente confermativo e ricognitivo dei principi elaborati dai Giudici di Strasburgo, poiché essa non è la fonte normativa diretta del diritto alla riservatezza. Tale fonte resta, invece, la CEDU, seppur attraverso il filtro della categoria dei principi generali. La Corte, infatti, ricostruisce il principio generale del diritto in base alla Convenzione europea, come interpretata dalla Corte dei diritti dell'uomo, per poi trasporlo tale e quale nell'ordinamento Ue.

[62] Cort. Giust. Sent. e novembre 2003, *Bodil Lindquist c. Aklagarkammaren i Jönköping* causa C-101/01, 6, in *Foro. It.*, IV, 2004, cc. 57-77. Conformi Corte. Giust., sent. 20 maggio 2003, cause riunite, C-465/00, C-138/01 e C-139/01, *Rechnungshof c. Osterreichischer Rundfunk* e altri; Corte di Giustizia sent. 27 giugno 2006, C-540/03.

[63] T.A. AULETTA, *Riservatezza e tutela della personalità*, in *Pol. Dir*., 1974, p.54; A. RAVÀ, *Istituzioni di diritto privato*, Cedam, Padova, 1938, p. 157; S. RODOTÀ, *op. loc. cit.*, 1974, p. 545.

di legislazione ordinaria. La mancanza di una disciplina espressa ha portato la dottrina di metà novecento a proporre diverse definizioni alla riservatezza, influenzate dall'esperienza americana e accomunate dal fatto di concepire l'interesse al riserbo come potere del singolo di vietare la conoscenza a soggetti terzi di fatti attinenti alla propria sfera privata. In questa fase, infatti, gli studi volti ad affermare l'esistenza del diritto alla riservatezza riprendono le osservazioni svolte da Warren e Braindeis e definiscono l'interesse al riserbo come diritto a essere lasciati soli (c.d. *right to be let alone)* [64], trovando inizialmente riscontro nella giurisprudenza di merito[65]. Solo successivamente, a partire dagli anni settanta, si è assistito ad una svolta, sia nel pensiero dottrinale, sia nell'elaborazione giurisprudenziale. Infatti, la diffusione progressiva dei *computer* e l'influenza dell'esperienza americana stimolano alcuni autori a cambiare il modo di concepire la riservatezza, ampliandone il concetto[66]. In particolare, essi cominciano ora a considerare l'interesse al riserbo, come non limitato semplicemente al diritto ad essere lasciati soli (*right to be let alone*), ma esteso anche al potere di controllare e gestire le informazioni

[64] A. DE CUPIS, *I diritti della personalità*, in *Trattato di diritto civile e commerciale*, CICU, MESSINEO (a cura di), Giuffrè, Milano, I, 1982, p. 326; A. RAVÀ, *op. loc. cit.*. Per ricostruire il dibattito sul diritto alla riservatezza nel nostro ordinamento cfr. F. CARNELUTTI, *Il diritto alla vita privata, in Riv. Trim. dir. Pubbl*., 1955, p. 3; G. GIAMPICCOLO, *La tutela giuridica della persona umana e il cd diritto alla riservatezza*, in *Riv. Trim. dir. Proc. Civ.*, 1958, p. 461.

[65] Il percorso seguito in dottrina per giustificare la tutela alla riservatezza ha trovato eco nelle sentenze dei giudici di merito , che già intorno alla metà degli anni cinquanta affermavano l'esistenza nel nostro ordinamento del diritto alla *privacy*, mentre la giurisprudenza di legittimità inizia a parlare espressamente di interesse al riserbo solo dieci anni più tardi. In particolare si ricordano: Trib. Roma, 14 ottobre 1953, in Foro it., 1954, I, c. 115; Trib. Roma, 23 febbraio 1955, in *Foro it*., 1955, I, c. 918 e, tra tutte, Cass. Civ., 22 dicembre 1956, 4487, in *ivi*, 1957, I, cc. 4 e ss..

[66] G. B. FERRI, Privacy *e libertà informatica*, in ALPA,BESSONE (a cura di), *Banche dati telematiche e diritti della persona*, Cedam, Padova, 1984, p. 47; S. RODOTÀ, *op. loc.cit.*, p. 545.

personali[67]. È stato appunto osservato che il diritto in esame rappresenta una delle istanze di tutela più significative emerse nella società contemporanea[68], poiché risulta minacciato dal constante sviluppo di tecnologie altamente invasive della sfera giuridica individuale.

Per trovare un fondamento costituzionale al diritto alla riservatezza, data l'assenza di un esplicito richiamo nella Carta Costituzionale, la dottrina ha invocato variamente l'art. 2 Cost.. Tale disposizione, infatti, è al centro della nota *querelle*, che vede contrapporsi le tesi di chi configura la norma in parola come una fattispecie (o clausola) chiusa, in quanto la considera meramente riassuntiva e riepilogativa delle libertà e dei diritti espressamente previsti dal Testo costituzionale, e di chi concepisce detto articolo, invece, come una fattispecie (o clausola) aperta all'introduzione di interessi non esplicitamente menzionati dalla Costituzione (cd. nuovi diritti)[69].

I sostenitori dell'interpretazione estensiva riconoscono copertura costituzionale ai diritti nuovi (cioè non formalmente previsti nella Carta Costituzionale), come la riservatezza, considerando implicitamente l'art. 2 una norma di produzione giuridica[70]. A tale lettura aperta si contrappone[71]

---

[67] S. RODOTÀ, *La* privacy *tra individuo e collettività*, cit., p. 547.

[68] A. BARBERA, FUSARO, *Corso di diritto pubblico*, Il Mulino, Bologna, 2008

[69] Sul punto cfr. A. PACE, *Problematiche sulle libertà fondamentali*, Cedam, Padova,III ed., 2003; A. BARBERA, *Commento all' art. 2 della Costituizione. Principi fonamentali*, in G. BRANCA (a cura di) , *Commentario della Costituzione italiana*, Zanichelli –Foro Italiano, Bologna-Roma, 1975, p. 60 e s.

[70] Nell'ambito di tale orientamento, tuttavia, si ritrovano diverse posizioni che affrontano in modo diverso soprattutto l'aspetto del fondamento dei diritti non scritti in Costituzione (in questo senso nuovi) . In effetti, con riferimento alla fonte dei diritti nuovi o c.d. inediti, questo orientamento si divide tra coloro che risentono degli influssi giusnaturalistici e, di conseguenza, sottolineano il rinvio al diritto naturale [S. GALEOTTI, *La libertà personale*, Giuffrè, Milano, 1953, p. 29; Vassalli, 1960, 1640], e coloro che ricercano comunque un fondamento positivo [P. BARILE, E. CHELI, P. GRASSI, *Istituzioni di diritto pubblico*, Cedam, Padova, 2009, p. 391] o, in termini più lati, richiamano l'opera delle forze socio-politico e culturali che, in dato momento

l'orientamento che reputa l'art. 2 Cost. una clausola chiusa, ossia di mero rinvio ai diritti espressamente codificati dalla Carta costituzionale[72]. Il diritto alla *privacy* viene tutelato, allora, dando una lettura aggiornata ed estensiva delle disposizioni costituzionali previste agli artt. 13[73], 14[74] e

---

storico, determinano la costituzione materiale [A. BARBERA, *Commento all'art. 2 della Costituzione,* in G. BRANCA (a cura di), *Commentario della Costituzione italiana,* cit., p. 84-85; C. MORTATI, *Isituzioni di diritto pubblico,* Cedam, Padova, 1991, p. 158] o ancora rinviano al diritto sovranazionale [B. CONFORTI, *Diritto internazionale,* 1992, Ed. Scientifica, Napoli, p.294; A. LA PERGOLA, *Costituzione e adattamento dell'ordinamento interno al diritto internazionale,* Giuffrè, Milano, 1961, p. 267 e s.]

[71] In via generale, i sostenitori dell'interpretazione restrittiva criticano quella estensiva per le conseguenze che da essa deriverebbero. Infatti, secondo questi studiosi, non vi sarebbe alcuna utilità giuridica nel fare emergere nuovi diritti da una norma generale (l'art. 2 Cost. appunto), che si limita a riconoscerli e a garantirli, ma non li delinea nel contenuto né ne precisa la disciplina. In sostanza, si darebbe luogo a una operazione creativa di diritti, peraltro, inutile, perché i cd. "nuovi diritti" sarebbero già codificati (o "estraibili") dalle altre disposizioni costituzionali esistenti [A. PACE, *Problematica delle libertà costituzionali,* Cedam, Padova, 1990, p. 4 e s.]. Ma, ancor di più, si sottolinea il pericolo insito nel soggettivismo dei giudici, poiché, se si legittimasse la produzione del diritto in base a procedimenti interpretativi si rimarrebbe esposti alla loro discrezionalità [G. DE VERGOTTINI, *Oltre il dialogo tra le Corti. Giudici, diritto straniero e comparazione,* Il Mulino, Bologna, 2010, p. 149].

[72] Peraltro, anche all'interno di questo orientamento dottrinale non si riscontra uniformità di pensiero. Possono, infatti, individuarsi diverse posizioni che vanno da quella più rigorosa, che ammette l'ampliamento del catalogo costituzionale dei diritti solo per il tramite del procedimento di revisione costituzionale [P. GROSSI, *Introduzione a uno studio sui diritti inviolabili nella Costituzione italiana,* Cedam, Padova, 1972, 172], a quella meno rigida che attribuisce una certa capacità estensiva alle norme e, quindi, alle libertà in esse garantite [P. BARILE, *Diritti dell'uomo e delle libertà fondamentali,* Il Mulino, Bologna, 1984, p. 55 e s.].

[73] Tradizionalmente la libertà personale si è affermata, sia in dottrina che nella giurisprudenza costituzionale, come esigenza di garantire la libertà (e l'integrità) fisica, vale a dire come "libertà dagli arresti", poiché affonda le proprie radici nel *wirt of habeas corpus* del diritto anglosassone. [Cfr. A. PACE, *Libertà personale* (dir. cost.), in Enciclopedia del diritto, XXIV, Giuffrè, Milano, 1974, p. 287 e ss. e, a es., C. Cost., sent. 2/1956, in *www.consultaonline.org*]. Pertanto, rientrano nell'ambito di tutela della disposizione in esame esclusivamente le coercizioni fisiche che infliggono un patimento alla persona che le subisce.

Occorre, però, sottolineare che, accanto a tale costruzione, parte dominante della dottrina e della giurisprudenza costituzionale hanno sostenuto una concezione più ampia, tesa a includere nell'articolo in discorso anche la protezione della libertà morale, da intendersi come pretesa dei singoli all'integrità della propria coscienza e

15[75] Cost e ai diritti ivi contemplati della libertà personale, di domicilio, nonché libertà e segretezza di ogni forma di comunicazione.

A questa conclusione giunge anche la Corte Costituzionale, poco dopo gli anni settanta. Essa, infatti, afferma l'esistenza del diritto alla riservatezza ancorandolo all'art 2 Cost., inteso come clausola di chiusura del sistema, leggendolo in combinato disposto con gli artt. 13, 14 e 15 Cost. [76]. L'adesione a tale ricostruzione implica che la limitazione del diritto alla

---

autodeterminazione [Cfr. T. MARTINES, *Diritto Costituzionale,* Giuffrè, Milano, 2005; P. BARILE, *cit.*, 1984, p. 111 *e* la sent. C. Cost. 30/1962, in *www.consultaonline.org*]. Sulla scorta di questa definizione, l'art. 13 Cost. proteggerebbe il singolo, oltre cha da ogni indebita coercizione fisica (temporanea o non), da qualsiasi misura, anche obbligatoria, idonea a ledere la sua libertà morale. In questa prospettiva, il progresso tecnico e gli strumenti della scienza moderna hanno mostrato come la libertà morale, ancor più di quella fisica, possa essere vulnerata (basti pensare, a es., alle schedature informatiche).

[74] Il regime costituzionale della libertà di domicilio ricalca in larga misura quello sancito dalla libertà personale. Esso, infatti, tradizionalmente è ritenuto essere la proiezione spaziale della persona [T. MARTINES, *Diritto Costituzionale,* cit., p. 652-653]. Per quanto attiene al suo contenuto, la libertà di domicilio consiste nel diritto dell'uomo ad avere una propria sfera privata, delimitata nello spazio e isolata dall'ambiente esterno, in cui svolgere ogni tipo di attività lecita, impedendo qualsiasi interferenza altrui e potendo altresì scegliere il luogo in cui stabilire il proprio domicilio. Una definizione così ampia del diritto in esame è idonea a tutelare il diritto alla riservatezza [T. MARTINES, *Op. loc. ult. cit.]*.Si ritiene che la nozione costituzionale di domicilio sia più ampia di quella contenuta nel codice civile (art. 43 cc), avvicinandosi a quella prevista nel codice penale (artt. 614 e 615 c.p.). Quest'ultimo nel tempo, arricchitosi di nuove fattispecie incriminatrici (artt. 615 *ter, quater e quinquies* c.p.), rispondenti alle esigenze di tutela imposte dall'evoluzione informatica e delle comunicazioni telematiche, ha introdotto nell'ordinamento giuridico il concetto di domicilio informatico, come si vedrà più diffusamente nel cap. II, parte II. Cfr. C. PECORELLA, *Il diritto penale dell'informatica,* Giuffrè, Milano, 1994, p. 326 e ss

[75]La formulazione di ampio respiro scelta dal Legislatore costituente («ogni altra forma di comunicazione sono inviolabili…») consente di includere nel novero di tutela della disposizione ogni tipo di comunicazione resa possibile dalla nuove tecnologie (es. comunicazioni elettroniche o telecomunicazioni es. e-mail).

[76] C. Cost. sent. 34/1973 e C. Cost. sent. 135/2002 reperibili sul sito www.*consultaonline.org,* nelle quali il Giudice delle Leggi si è espresso rispettivamente sulla legittimità costituzionale dell'intercettazione telefonica e delle videoriprese. Nella pronuncia più recente, in particolare, la Consulta ha definito la libertà di domicilio, al pari della libertà di comunicazione, una espressione del più ampio diritto alla riservatezza della persona.

riservatezza operata nel coso delle indagini sia legittima ove ricorrano i due requisiti del rispetto della legge e dell'esistenza di un atto motivato da parte dell'autorità giudiziaria che ne autorizzi la compressione.

Diversamente, la tesi che riconduce il diritto alla *privacy* alla tutela apprestata dall'art. 2 Cost., come sostenuto dalla Corte di Cassazione a Sezioni unite[77], richiederebbe la sola adozione di un atto motivato da parte dell'autorità giudiziaria, non essendo prevista nel testo normativo alcuna riserva di legge. Ne consegue, secondo i Giudici di Legittimità, la possibilità di svolgere atti di indagine atipici, anche sfruttando mezzi di ricerca della prova tecnologicamente nuovi, riconducibili analogicamente alla disciplina dell'art. 189 cpp[78] essendo sufficiente operare un contraddittorio differito sugli atti investigativi già eseguiti.

Una impostazione questa che, tuttavia, ha incontrato alcune critiche dovute al tenore letterale della norma[79]. La formulazione dell'articolo, infatti, non solo si riferisce esclusivamente ai mezzi di prova non disciplinati dalla legge, ma richiede anche un contraddittorio preventivo tra

---

[77] Cass, sez. un., 28 marzo 2006, n. 26759, in *Cass. pen.*, p. 3937, in tema di videoriprese.

[78] A. CAMON , *Le riprese visive come mezzo di indagine: spunti per una rioflessione sulle prove incostituzionali*, in *Cass. pen*., 1999, p. 1195 A. LARONGA, *Le prove atipiche nel processo penale*, Cedam, Padova, 2002, p. 18 e ss.

[79] Il problema delle investigazioni atipiche, introdotte dalle nuove scienze (genetica e informatica) risulta grandemente ridimensionato, nell'ordinamento giuridico italiano, dall'entrata in vigore della legge30 giugno 2009 n. 85 di recepimento del trattato di Prüm e della legge 18 marzo 2008 n. 48 di conversione della Convenzione di Budapest (c.d. Convenzione sul *cybercrime*), che hanno disciplinato le indagini genetiche e informatiche, oggi divenute tipiche. Il problema si propone ancora soprattutto con riferimento alle indagini informatiche atipiche (quali il tracciamento satellitare tramite gps cfr. D. GENTILE, Tracking *satellitare mediante gps: attività atipica di indagine o intercettazione di dati*, in *Dir. pen. e proc*., 2010, p. 1464 e s.), in relazione alle quali discussa è l'applicabilità della disciplina prevista dall'art. 189 c.p.p.

le parti sulla prova da assumere, cosicché il suo ambito applicativo sarebbe addirittura circoscritto alle prove costituende[80].

Le ripercussioni pratiche dell'adesione all'una delle due teorie, tuttavia, attualmente possono ritenersi superate dal ruolo svolto nell'ordinamento giuridico italiano dalla Convenzione Europea, che all'art. 8 richiede per legittimare un atto di investigativo restrittivo del diritto alla riservatezza una previsione legislativa, ossia introduce una riserva di legge[81].

[80] N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Cedam, Padova, 1992, p. 213; L. FILIPPI, *L'home –watching: documento, prova atipica o prova incostituzionale?*, in, *Dir. pen. e proc.,* 2001, 1, p. 92.
[81] Sul valore delle disposizioni della CEDU cfr. par. 2 e 3

PARTE SECONDA

INTRODUZIONE

L'applicazione alle indagini penali sia delle tecniche di analisi genetica sia di quelle informatiche ha avuto un impatto rivoluzionario nell'ambito del processo penale, tanto che la ricostruzione del fatto storico è, oggi, sempre più di frequente affidata ai risultati della prova scientifica. Attualmente, gli accertamenti genetici, infatti, possono essere svolti, con esiti straordinariamente attendibili in punto di identificazione, pur avendo a disposizione ridottissime quantità di reperti biologici, e le investigazione informatiche consentono di ricercare, captare, archiviare, elaborare e incrociare quantità di dati enormi di gran lunga sovrabbondanti rispetto agli obiettivi investigativi.

L'uso di questi strumenti è stato incentivato, anche a livello di normazione internazionale (da politiche spesso di natura emergenziale), nel quadro della lotta al terrorismo e al crimine organizzato, che ha indotto molte Nazioni a varare ampie riforme processuali all'insegna della sicurezza. Tali novelle hanno mutato le finalità del processo penale, trasformandolo sempre più in uno strumento di controllo sociale in cui trovano ampio spazio le forze di polizia e gli organi di *intelligence* nonché l'impiego di nuovi mezzi investigativi di inedita invasività soprattutto per quanto riguarda i diritti alla riservatezza[82]. In questa prospettiva acquista rilievo la protezione della *privacy*, intesa come diritto di controllare la

[82] Per un approfondimento sull'impatto che le politiche emergenziali di contrasto al terrorismo hanno avuto sui sistemi processuali statali, che spesso hanno introdotto strumenti di indagine aventi carattere preventivo, e sui diritti fondamentali individuali quali la *privacy* cfr. R. E. KOSTORIS, *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella risoluzione del XVIII Congresso internazionale del diritto penale,* in *Riv. dir. proc.*, 2010, p. 330.

correttezza, l'uso e la rivelazione di dati, informazioni e notizie attinenti alla sfera individuale[83].

Rebus sic stantibus, è stato inevitabile che il legislatore intervenisse a disciplinare in modo organico le indagini genetiche e informatiche, cercando di contemperare il diritto alla riservatezza con l'esigenza di accertare i reati; cosa che si è verificata con la legge 30 giugno 2009 n. 85 di ratifica al trattato di Prüm e la legge 18 marzo 2008 n. 48 di conversione della Convenzione di Budapest (c.d. Convenzione sul *cybercrime*).

Nei successivi due capitoli si cercherà, quindi, di analizzare in modo critico il difficile bilanciamento realizzato nell'ordinamento giuridico italiano tre le esigenze del procedere penale e la tutela della vita privata del singolo.

[83] P. FELICIONI, *Accertamenti sulla persona e processo penale. il prelievo del materiale biologico*, Giuffré, Milano 2007, p. 3.

CAPITOLO I

La *privacy* e le indagini genetiche: bilanciamenti reciproci dopo la ratifica del Trattato di Prüm

Sommario: 1. La riservatezza in ambito genetico. - 2. L'analisi del campione o reperto biologico e le esigenze di tutela - 3. Il bilanciamento tra protezione della riservatezza ed efficienza investigativa nella gestione, conservazione, cancellazione o distruzione di dati e campioni biologici. - 4. Segue: L'attività della banca dati nazionale del DNA: tutela della *privacy* e raffronto dei profili a fini investigativi. - 5. La protezione della *privacy* e la "cooperazione informativa" di dati genetici dopo la legge di ratifica del Trattato di Prüm.

1- La riservatezza in ambito genetico.

Le indagini fondate sull'accertamento del DNA costituiscono probabilmente la "prova scientifica" che negli ultimi decenni ha avuto la più ampia applicazione nelle aule di giustizia[84]. Tanto che l'ingresso di

[84] In argomento: A. GARGANI, *I rischi e le possibilità dell'applicazione dell'analisi del DNA nel settore giudiziario, in Riv. It. Dir. e Proc*. Pen., 1993, p. 1307; P. TONINI, *Prova scientifica e contraddittorio*, in *Dir. pen. proc*., 2003, p. 1459 e ss.. Sulla decisività del *test* del DNA e all'utilità delle banche dati genetiche per identificare l'autore del reato anche a distanza di tempo cfr. M. CASTELLANETA, *Uno scambio di informazioni tra gli Stati per rafforzare la lotta al crimine organizzato*, in *Guida al diritto*, 30, 2009, p. 63.

questo nuovo tipo di investigazione nel processo penale ha creato il rischio concreto di uno svilimento dell'attività investigativa "tradizionale" in base a una sorta di mitizzazione della precisione ed efficacia del *test* genetico[85].

È in tale conteso che si inserisce il problema di garantire la riservatezza dell'imputato, la quale rappresenta un limite al procedere penale[86] e, specificamente, a determinate attività di indagine fra cui spiccano gli accertamenti corporali, poiché il dato genetico per le sue cantieristiche intrinseche coinvolge vari aspetti anche della vita associata, a cominciare dalle relazioni familiari[87].

Il genoma di ogni persona è notoriamente capace di fornire un numero elevatissimo di informazioni, che non si limitano al sesso o alle condizioni di salute personale, come accade comunemente per i dati di tipo sanitario, ma riguarda le relazioni familiari, le caratteristiche somatiche, le malattie e la predisposizione a future patologie.

Gli aspetti critici si manifestano non solo per quanto riguarda le modalità di raccolta delle informazioni personali, ma anche e specialmente con riferimento all'esigenza di garantire un controllo su raccolta, elaborazione, conservazione e circolazione dei dati a protezione della *privacy*.

La tutela dei dati genetici quali risultato del prelievo di materiale biologico presenta, quindi, aspetti molto delicati, che vanno oltre la compressione della libertà individuale del soggetto passivo, funzionale

---

[85] P. TONINI, *Accertamento del fatto e informazioni genetiche: un difficile bilanciamento,* in *Dir. pen. e proc*, 2009, 2, *Gli speciali*, p. 5; G. UBERTIS, *Attività investigativa e prelievo dei campioni biologici,* in *Cass. Pen*, 2008, p. 6 e ss..

[86] In questi termini già M. PISANI, *La tutela penale della riservatezza": aspetti processuali*, in *Riv. it. dir. proc. pen.*, 1967, p. 787.

[87] Più ampiamente cfr. E. STEFANINI, *Dati genetici e diritti fondamentali,* Cedam, Padova, 2008, p. 8 e ss.; L. PICOTTI, *Trattamento dei dati genetici, violazioni della* privacy *e tutela dei diritti fondamentali nel processo penale,* in D. DE. LEO, S. TURRINA, M. ORRICO (a cura di), *Lo stato dell'arte nella genetica forense,* Giuffrè, Milano, 2003, p. 134 e in Dir. dell'informazione e dell'inf, 2003, p.689 e s.

all'acquisizione del materiale biologico necessario per estrarre il profilo genetico[88]. È ciò in ragione del fatto che l'esame del DNA, esperito per finalità identificative e di accertamento forense, può fornire informazioni che si estendono a interi nuclei familiari, sollevando questioni sino a poco tempo fa ignorate a livello legislativo e scarsamente considerate dalla dottrina processualistica[89]. Infatti, ciascuna persona detiene un proprio patrimonio genetico, ma nel contempo appartiene anche ad una linea genetica: questo crea uno scollamento tra diritto interno, che è concepito sul singolo, e sapere scientifico che fonda gli studi genetici sui caratteri che l'individuo condivide con altri.

Sulla scorta di tali considerazioni, si può concludere che la *privacy* riferita alle informazioni genetiche assume una dimensione e connotazione peculiare, in quanto rappresenta un interesse riferibile ai componenti di un intero nucleo familiare, che condividono le informazioni genetiche. I più evidenti punti di contrasto tra esigenze investigative e tutela del diritto alla riservatezza si hanno, infatti, con riferimento alla tecnica della ricerca del DNA familiare (*familial DNA searching*).

Questo problema emerge soprattutto nel caso di prelevi di massa di materiale genetico (cd. *screening di massa*) nonché in relazione alla creazione e archiviazione in banche dati del materiale biologico.

La riforma attuata con la legge 85/2009 di ratifica del Trattato di Prüm istituisce nel nostro Paese la banca dati nazionale del DNA e il laboratorio centrale con finalità identificativa e di collaborazione internazionale fra le

[88] Il prelievo di materiale biologico ormai avviene abitualmente con un tampone salivare, la cui attitudine intrusiva è veramente minima assimilabile alla coazione necessaria per il rilievo delle impronte digitali.

[89] È con la legge 30 giugno 2009 n. 85 di ratifica al trattato di Prüm che si specificano per la prima volta le finalità e le modalità per il trattamento delle informazioni genetiche.

forze investigative. Le sue disposizioni cercano un bilanciamento tra esigenze di indagine e riservatezza individuale in relazione all'analisi di materiale biologico, oltre che in relazione all'archiviazione e conservazione nella banca dati nazionale di profili genetici estratti dal laboratorio centrale[90].

Il contemperamento normativo tra queste opposte esigenze, operato dalla legge 85/2009, tuttavia, deve essere ancora completato attraverso l'emanazione da parte del Governo di specifici regolamenti attuativi aventi contenuto tecnico, alla luce dei quali dovrà essere valutato[91].

[90] G. GENNARI, *La istituzione della banca dati nazionale del DNA ad uso forense: dalla privacy alla sicurezza*, in A. SCARCELLA (a cura di), *Adesione al Trattato di Prüm e cooperazione transfrontaliera per il contrasto alla criminalità. Prelievo del DNA e banca dati nazionale*, Cedam, Padova, 2009, p. 50 ss; A. MUSUMECI, *La ratifica del Trattato di Prüm*, in L. MARAFIOTI e L. LUPARIA, *Banca dati del DNA e accertamento penale. Commento alla legge di ratifica del trattato di Prüm istitutiva del database* genetico *nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85)*, Giuffrè, Milano, 2009, p. 14 e ss.

[91] Tale operazione passa soprattutto attraverso la considerazione delle principali problematiche connesse alla creazione e alla gestione di una banca dati del DNA. Si tratta dei seguenti profili: l'individuazione dei soggetti dai quali prelevare il materiale biologico per archiviarne i profili genetici, la raccolta di dati biologici limitata a determinati segmenti del genoma umano, l'uso giudiziario dei risultati degli accertamenti genetici, i metodi per la trasmissione dei dati dall'archivio all'autorità procedente, i tempi di conservazione di profili e campioni genetici e, infine, la conservazione di una porzione di materiale biologico per consentire eventuali indagini difensive. P. FELICIONI, *L'Italia aderisce al Trattato di Prüm: disciplinata l'acquisizione e l'utilizzazione probatoria dei profili genetici* , in *Dir. pen. proc.*, 2009, 11 - Allegato 2 , p. 18; R. E. KOSTORIS, R. ORLANDI, *Prelievi biologici coattivi*, in R. E. KOSTORIS (a cura di), *Contrato al terrorismo interno e internazionale*, Giappichelli, Torino, 2006, p. 343 – 344.

2 L'analisi del campione e del reperto biologico e le esigenze di tutela.

La disciplina relativa all'analisi dei campioni e dei reperti biologici e alle "impronte genetiche" da essi ricavate ha numerose implicazioni sulla libertà di autodeterminazione concernente i dati personali. Essa, in particolare, assume rilievo in relazione alla costituzione e al funzionamento della banca dati nazionale del DNA, la quale è destinata a raccogliere e conservare i profili genetici estratti da campioni e reperti.

Il DNA (acido desossiribonucleico) è la molecola, contenuta in ogni nucleo cellulare, portatrice dell'informazione genetica, che si trasmette per via ereditaria. Tale molecola si struttura in due catene (i cromosomi) formate da nucleotidi posti in sequenza lineare (art. 6 l. 89/2009)[92].

Il segmento del DNA che racchiude l'informazione ereditaria, chiamato gene, contiene le informazioni per la "costruzione" –attraverso un processo cd. di trascrizione- dei componenti essenziali delle cellule (proteine) e, quindi, dell'intero organismo (DNA codificante)[93].

I geni contengono sia zone codificanti sia zone non codificanti e costituiscono una porzione minima -meno del 2%- dell'intero DNA

[92] I nucleotidi sono gli "anelli" della catena cromosomica e sono formati da due basi azotate complementari. Le basi azotate sono di quattro tipi (adenina, citosina, guanina, timina) e si accoppiano tra loro sempre allo stesso modo. L'informazione genetica consiste nella sequenza di basi. R. DOMENICI, *Prova del DNA*, in *Dig. disc. pen.*, Torino, UTET, 1997, p. 373; P. GAROFANO, *Genetica identificativa e biobanche: aspetti tecnici e problematiche connesse*, in *Dir.pen.proc.*, *dossier*, 2008, 6, p. 44-50.

[93] Una serie di meccanismi all'interno della cellula consente la trascrizione di parti specifiche del cromosoma che vengono usate come "istruzioni" per assemblare, attraverso il processo di trascrizione, altre molecole complesse (proteine), che costituiscono i componenti essenziali della cellula. All'interno di un gene sono presenti zone codificanti le proteine e zone non codificanti; entrambe vengono trascritte. A. COCITO, *Parametri internazionali e affidabilità*, in L. MARAFIOTI e L. LUPARIA, *Banca dati del DNA e accertamento penale*, cit., p. 99.

umano, il quale nelle altre parti svolge funzioni ancora quasi del tutto sconosciute.

In natura esistono per ogni gene più forme alternative (alleli)[94], che possono essere riscontrate nei diversi individui; in ragione di ciò, il patrimonio genetico di ogni persona varia ed è unico. Analizzando tali variazioni genetiche è possibile ricavare il profilo genetico (o impronta genetica) personale, che consente di identificare un essere umano con un alto grado di affidamento e fornisce un importante strumento per le indagini penali.

Il profilo genetico, estratto in laboratorio attraverso una serie di operazioni chiamate tipizzazione, è costituito da una «sequenza alfanumerica ricavata dal DNA», «caratterizzante ogni singolo individuo» (art. 6 l. 89/2009).

In passato, uno dei problemi maggiori nelle indagini era rappresentato dalla minima quantità di materiale biologico a disposizione degli investigatori, spesso insufficiente a ottenere l'impronta genetica. Il progresso tecnico-scientifico, attualmente, ha permesso di superare questo ostacolo e di tipizzare il profilo genetico del singolo anche da quantità molto ridotte di materiale biologico, come le tracce lasciate sul luogo di un delitto (capelli, sangue, cellule della pelle, etc.)[95].

---

[94] Gli alleli determinano delle varianti strutturali della molecola proteica prodotta. La presenza di varianti alleliche per un dato gene si chiama polimorfismo. In ogni cromosoma vi sono numerosissimi punti detti polimorfismi, in cui gli individui possono presentare frequenze alleliche diverse; si tratta di zone della catena cromosomica particolarmente soggette a differenze strutturali.

[95] Quando una cellula si divide, tutto il DNA si duplica, cosicché ogni cellula "figlia" è identica alla cellula madre (cd. duplicazione del DNA). Questo processo è alla base del concetto di ereditarietà di un carattere e spiega il motivo per cui ogni cellula di uno stesso individuo contiene il medesimo DNA, chiarendo perché è possibile, ai fini identificativi, comparare il profilo genetico ricavato da tessuti diversi come una traccia

A tale proposito, la legge di riforma 85/2009 ha fornito alcune indicazioni utili e ha operato una distinzione, basata sulla provenienza del materiale genetico da analizzare, tra campione e reperto biologico. Con il primo termine si intende la quantità di sostanza genetica prelevata da persona sottoposta a tipizzazione, la cui identità dunque è nota, mentre con il secondo termine si indica il materiale biologico trovato sulla scena di un delitto o comunque su cose pertinenti al reato (art. 6 l. 85/2009).

Il campione e il reperto genetico devono essere considerati una particolare categoria di dato personale, poiché da essi è possibile ricavare informazioni di gran lunga superiori a quelle identificative: essi sono infatti idonei a svelare lo stato di salute, l'origine etnica o razziale della persona e ancora i caratteri ereditari.

Nella disciplina dell'analisi dei campioni o reperti biologici, uno dei principali aspetti di contrasto con la *privacy* emerge in riferimento alla possibilità di individuare la presenza di particolari malattie genetiche di cui il soggetto sia affetto. In questa prospettiva, all'art. 11, comma 3, l. 85/2009 risolve il problema e stabilisce che per estrarre il profilo genetico debbano essere analizzati solamente i tratti di DNA che non consentono di scoprire eventuali patologie del soggetto esaminato e impone, conseguentemente, di adottare tecniche di analisi capaci di selezionare sequenze alleliche[96] che non forniscono alcuna informazione in tal senso. Vietando solo l'identificazione degli stati patologici, però, il legislatore italiano compie una scelta meno garantista di quella fatta dal Consiglio dell'Unione Europea nella Decisione quadro 2008/616/GAI[97], che

---

di saliva e il sangue del sospettato. A. COCITO, *L'ambito definitorio,* in L. MARAFIOTI, L. LUPARIA *Banca dati del DNA e accertamento penale,* cit., p. 44

[96] Si tratta di polimorfismi cfr. nota 94.

[97] Cfr. parte I, cap. I, nota 55

prevedeva la possibilità di estrarre soltanto i profili non codificanti del DNA, e cioè, i segmenti che non forniscono alcuna proprietà funzionale di un organismo[98]. Il profilo tipizzato da porzioni di DNA che presentano variazioni localizzate fuori delle sequenze codificanti, infatti, non fornirebbe nessuna informazione sull'individuo da cui è ricavato, consentendone esclusivamente l'identificazione e garantendo maggiormente il diritto alla *privacy*.

Al contrario, l'art. 11 l. 85/2009 si limita a stabilire che vengano sottoposte a esame le sequenze genetiche che, in base alle conoscenze attuali, non forniscono indicazioni sullo stato di salute individuale[99].

Tale norma, inoltre, chiarisce che l'analisi del campione o del reperto biologico deve essere eseguita rispettando i parametri internazionali indicati nell'*European Network of Forensic Science Institute* (ENFSI) e che i profili di DNA devono essere tipizzati in laboratori certificati a norma ISO/IEC[100]. Indubbiamente il ricorso a *best practices* internazionali è il presupposto fondamentale per l'uniformazione degli *standars* procedurali e consente di garantire il rispetto della riservatezza del soggetto, nei cui confronti sono utilizzate tecniche d'esame idonee a estrarre solo determinate sequenze alleliche.

---

[98] P. TONINI, *Informazioni genetiche e processo penale a un anno dalla legge*, in *Dir. pen e proc.*, 2010, 7, p. 833

[99] In questo senso, assumono un rilievo essenziale i criteri con cui vengono selezionati i marcatori (cioè una sequenza di DNA conosciuta che identifica univocamente una regione del cromosoma) utilizzati per tipizzare il profilo del DNA, al fine di ridurre al minimo il rischio di ricavare, grazie all'evoluzione scientifica, informazioni da sezioni di cromosoma non ancora completamente conosciute. Questo pericolo aumenta esponenzialmente quanto a più lungo il campione biologico da cui estrarre il profilo genetico rimane a disposizione dell'autorità giudiziaria .

[100] A. COCITO, *Parametri internazionali e affidabilità dei laboratori nell'analisi dei reperti e dei campioni*, in L. MARAFIOTI, L. LUPARIA (a cura di), *Banca dati del DNA e accertamento penale*, *cit.*, p. 93 e ss.

Sulla scorta di quanto detto, superato il problema della sequenza genetica da tipizzare e degli *standards* da usare per rispettare il diritto alla riservatezza, rimane da esaminare l'aspetto critico del coinvolgimento di terzi estranei nel prelievo biologico (coattivo o consensuale), a cui inevitabilmente si collega la possibilità di *screening* di massa e di ricerche familiari.

Sul punto è utile ricordare che la legge 85/2009 ha modificato il codice di rito (artt. 244 –*bis*, 359–*bis* c.p.p, 392 c.p.p.) e le disposizioni di attuazione (72 disp. att. c.p.p.) con l'introduzione di una disciplina specifica del prelievo coattivo di campioni biologici per scopi identificativi e ricostruttivi del fatto criminoso[101]. Essa, nello specifico, introduce, all'art.

[101] L'intervento legislativo mira a risolvere *l'impasse* provocato della nota pronuncia n. 238/96 della Corte Costituzionale in materia di prelievi biologici coattivi [cfr. R. E. KOSTORIS, *Alt ai prelievi di sangue coattivi*, in *Dir. pen. e proc.*, 1996, p.1091e ss.], non superato nemmeno dalla legge 31 luglio 2005 n. 155. Tale normativa, infatti, ha costituito un intervento settoriale, maturato in un contesto "emergenziale" di contrasto al terrorismo internazionale, non animato dalla volontà di colmare, su di un piano più generale, la lacuna determinatasi a seguito della ricordata declaratoria di incostituzionalità [R. E. KOSTORIS, *Prelievi biologici coattivi*, in R. E. KOSTORIS, R. ORLANDI (a cura di), *op.loc.cit]*. Mancando una disciplina generale dei prelievi coattivi per l'esperimento di perizie e consulenze tecniche, il nucleo della riforma attuata con la legge 85/2009 è rappresentato proprio dall'introduzione nel *corpus* codicistico dei nuovi articoli 224–*bis* e 359–*bis* c.p.p., che disciplinano l'ipotesi di prelievi biologici e accertamenti medici coattivi, rispettivamente in sede di perizia in dibattimento (o in sede di incidente probatorio) e nella fase delle indagini preliminari. Tali disposizioni regolano l'ipotesi di svolgimento coattivo del prelievo da persona vivente e non ristretta nella libertà personale. Alla polizia giudiziaria, invece, stante l'abrogazione dell'ultima parte dell'art. 354, comma 3, c.p.p. rimane la facoltà di effettuare, a fini identificativi, il prelievo coattivo di capelli o saliva, previa autorizzazione del pm (349 comma *2bis* c.p.p.). La legge, tuttavia, prevede anche alcune ipotesi extracodicistiche di acquisizione dei campioni biologici di indagati, imputati o condannati ristretti nella libertà personale (art. 9) ovvero di cadaveri o resti cadaverici non identificati o di consanguinei o di persone scomparse.
A completare il complesso quadro si aggiungono, in fine, l'acquisizione del materiale biologico reperito sulla scena del delitto o comunque su cose pertinenti al reato (cd. reperto biologico), attività questa riconducibile all'istituto dei rilievi e accertamenti urgenti di polizia giudiziaria, a cui seguirà la tipizzazione del profilo genetico tramite consulenza tecnica o perizia. La novella in esame attribuisce centralità al giudice,

359-*bis* c.p.p., la possibilità per il pubblico ministero di disporre accertamenti tecnici incidenti sulla libertà personale di ogni «persona interessata», ponendo quali unici condizioni di ammissibilità[102] la gravità del reato e l'assoluta indispensabilità del mezzo investigativo per la prova dei fatti[103].

I limiti alla compressione della *privacy* individuale dipendono dall'interpretazione attribuita alla formula che indica il soggetto passivo del prelievo nonché all'espressione «assolutamente indispensabile per la prova dei fatti».

Sotto il primo profilo, la genericità della locuzione utilizzata porta a ritenere che questo mezzo di ricerca della prova sia esperibile nei confronti di qualunque persona, anche non indagata, ivi inclusi la vittima del reato, gli incapaci o gli interdetti perché mentalmente infermi[104].

Sotto il secondo aspetto, invece, la legge richiama una valutazione discrezionale dell'autorità giudiziaria, che rischia di legittimare lo strumento della ricerca di massa e per familiarità genetiche, palesemente

---

riconosce un potere di impulso al pubblico ministero (salvo i casi di urgenza) e sottrae alla polizia giudiziaria la legittimazione a eseguire il prelievo coattivo a fini investigativi. R. ADORNO, *Il prelievo coattivo a fini investigativi,* in *Giur. It.,* 2010, 5, II, c. 1232 M. STRAMAGLIA, *Prelievi coattivi e garanzie processuali*, in L. MARAFIOTI, L. LUPARIA (a cura di), *Banca dati del DNA e accertamento penale* cit., p. 253 e ss. F. CASASOLE, *Prelievi e accertamenti tecnici coattivi, ivi,* p. 243 e ss.

[102] L'art. 359-*bis* rinvia all'art. 224 -*bis* c.p.p.

[103] Analoghe osservazioni possono essere svolte con riferimento ai prelievi coattivi disposti, anche d'ufficio, dal giudice nel corso della perizia ex art. 224-bis, in cui il legislatore estende l'esecuzione coattiva su chiunque, purché siano commessi taluni reati gravi e il mezzo di prova appaia assolutamente indispensabile alla prova dei fatti. La questione si gioca, quindi, sull'interpretazione dell'espressione assolutamente. F. CASASOLE, *Prelievi e accertamenti tecnici coattivi,* in L. MARAFIOTI, L. LUPARIA (a cura di), *Banca dati del DNA e accertamento penale* cit., p. 243 e ss.; C. GABRIELLI, *Accertamenti medici dai confini troppo incerti*, in *Guida dir.*, 2009, 30, p. 71 e ss.

[104] Ciò emerge dalla lettura sistematica dell'art. 359 –bis (e 244-bis) c.p.p. con l'art. 72 bis disp. att. c.p.p.

contrastante con la tutela della riservatezza individuale. Perciò, sarebbe stato più garantista esplicitare i criteri in base a cui l'esame genetico risulti essere assolutamente imprescindibile per provare i fatti.

Per comprendere in concreto la portata e le implicazioni di tali scelte legislative giova esemplificare alcune ipotesi in cui è utile ai fini investigativi raccogliere il profilo genetico di individui che non presentano dirette relazioni con il fatto.

Da un lato, la tipizzazione del profilo genetico di soggetti non sospettati può servire per individuare, attraverso un processo di esclusione, il DNA del colpevole: ciò accade quando la *scena criminis* è inquinata da tracce biologiche appartenenti a terzi, come la stessa vittima (es. in caso di violenza sessuale).

Dall'altro, il prelievo coattivo, esperito su chi appare estraneo al delitto, può avere una finalità esplorativa o di riduzione dei sospettati: cosa che si verifica quando le indagini "giungono a un punto morto" o non vi è nemmeno un indagato. In tal modo, però, si rischia di legittimare il ricorso alla tecnica della *mass screening* per ricerche cd. casuali svolte su una cerchia di persone anche molto vasta, che, sebbene risulti valida nell'individuazione del colpevole, stride con la tutela della *privacy*[105].

Infatti, le ricerche massive possono condurre a scoprire l'autore di un reato laddove si trovino delle corrispondenze anche solo parziali tra il DNA rilevato sul *locu delicti* e quello di uno dei soggetti sottoposti al prelievo[106].

---

[105] P. FELICIONI, *L'Italia aderisce al Trattato di Prüm: disciplinata l'acquisizione e l'utilizzazione probatoria dei profili genetici* , cit. , p. 18. L 'autrice sottolinea l'utilità investigativa della *mass screening*, soprattutto se rapportata al minino sacrificio alla libertà personale causato dal prelievo di peli o capelli.

[106] Anche in Italia si è assistito a una esperienza investigativa ove si è fatto ricorso alla tecnica dello *screening* genetico di massa in relazione a un omicidio avvenuto, nel 2002, nell'area del comune di Dobbiaco. In quel caso, la Procura della Repubblica aveva chiesto l'aiuto degli abitanti del piccolo paese, ottenendo spontaneamente una serie di

In questo caso, il donatore che abbia vincoli di parentela con il responsabile permette di indirizzare le indagini su un determinato nucleo familiare o biologico[107], delle cui caratteristiche genetiche partecipa[108]. Così, si sfrutta la familiarità genetica ai fini investigativi violando il diritto alla riservatezza individuale, come recentemente rilevato anche dalla Corte europea dei diritti dell'uomo[109].

---

campioni biologici tra cui quello, rivelatosi poi decisivo, del padre dell'assassino. Il caso è stato deciso, in primo grado, dal Trib. Bolzano, 28 marzo 2003, n. 264, inedita cfr. G. GENNARI, *Identità genetica e diritti della persona,* in *Riv. crit. dir. priv.*, 2005, p. 624 e ss.

[107] G. GENNARI, A. SANTOSUOSSO, *Il prelievo coattivo di campioni biologici*, in *Dir. pen proc.* 2007, p.398

[108] La questione della familiarità delle caratteristiche genetiche individuali viene per la prima volta affrontata dal Consiglio d'Europa nelle Raccomandazione sukka protezione dei dati personali del 13 febbraio 1997, R(97) 5. Nell'*Explanatory Memorandum* della Raccomandazione 97(9), poi, si posizionano gli appartenenti alla stessa linea genetica in una sorta di "stato intermedio", a metà strada tra l'individuo direttamente interessato e il "terzo estraneo", auspicando per essi una protezione legale ibrida. Dice testualmente il punto 58: «Queste parti terze possono essere costituite dai membri della linea genetica del soggetto dei dati o da parenti collaterali o da membri della sua famiglia sociale. Gli estensori [della Raccomandazione] convengono di accordare uno stato intermedio ai membri appartenenti alla linea genetica del soggetto dei dati, in modo tale da distinguerli dalle parti terze, nel senso stretto del termine, e di garantire loro una protezione legale ibrida». Sulla questione è tornato, successivamente, in sede europea, il Gruppo di lavoro per la tutela dei dati personali, istituito ai sensi della direttiva 95/46/CE, con un Documento di lavoro sui dati genetici (adottato il 17 marzo 2004) che recita: «Si può quindi affermare che è emerso un nuovo gruppo sociale, giuridicamente rilevante, ossia il gruppo biologico, il gruppo di consanguinei, opposto, in termini tecnici, a quello della famiglia. Questo gruppo non comprende infatti familiari come il coniuge o i figli adottivi, ma altri soggetti che non fanno parte della cerchia familiare, in termini giuridici o di fatto, come i donatori di gameti o la donna che non ha riconosciuto il figlio al momento della nascita e ha chiesto di non rivelare la sua identità, un diritto riconosciuto in alcuni ordinamenti giuridici».

[109] Corte eur., *S. e Marper c. Regno Unito*, 4 dicembre 2008. In essa si che il concetto di vita privata impiegato nell'art. 8 CEDU non può venire definito in modo esaustivo ed abbraccia molteplici aspetti dell'identità personale e sociale di una persona. Quanto ai campioni biologici, la Corte osserva che, data la natura e la quantità di informazioni personali in essi contenute, la loro conservazione interferisce di per sé con il diritto al rispetto della vita privata. Ma anche il profilo del DNA presente nella banca dati costituisce un dato personale protetto dall'art. 8 CEDU., in quanto contiene «una quantità notevole di dati personali unici» e il loro trattamento automatizzato consente alle autorità «di andare ben al di là di una identificazione neutrale», fornendo in specie

Dubbia è, quindi, la legittimità di praticare il *cd. mass screening* e, correlativamente, l'utilizzabilità dei dati appartenenti a un familiare che non si è volontariamente sottoposto al prelievo del DNA. Il donatore, infatti, grazie al suo profilo genetico, potrebbe coinvolgere nelle indagini preliminari un soggetto, a lui geneticamente legato,[110] senza averne la consapevolezza o la possibilità di opporre un rifiuto[111].

In questo quadro, può venire in soccorso l'esperienza giuridica di altri Paesi in cui è diffuso l'utilizzo dello *screening* di massa (es. Gran Bretagna e Usa)[112], la quale si caratterizza per la cooperazione del soggetto estraneo alle indagini, a cui viene richiesta la cessione consensuale di un campione biologico[113]. Pertanto, questo tipo di prelievo non può essere oggetto di un provvedimento coattivo da parte della autorità giudiziaria e la persona non coinvolta nelle investigazioni delle forze di polizia può legittimamente opporre un rifiuto[114].

---

un mezzo per individuare relazioni genetiche fra le persone (*familial searching*). Questa conclusione - sottolinea la Corte - non è intaccata dal fatto che, «essendo l'informazione espressa in forma codificata, è comprensibile solo con l'uso di tecnologia informatica e può essere interpretata soltanto da un numero limitato di persone».

[110] Si tratta del cd. terzo non estraneo

[111] Cfr. parte II, cap. I, nota 115.

[112] C. FANUELE, *Dati genetici e procedimento penale*, Giuffré, Milano, 2009, p. 178.

[113] P. FELICIONI, *L'Italia aderisce al Trattato di Prüm: disciplinata l'acquisizione e l'utilizzazione probatoria dei profili genetici* , cit., p. 18; G. GENNARI, *Identità genetica e diritti della persona*, cit., p. 629-630

[114] In Gran Bretagna, il *Criminal Justice and Police Act*, emendato nel 2001 (e ulteriormente riformato in chiave estensiva nel 2004), autorizza la polizia ad effettuare il tampone salivare a chiunque venga arrestato per una violazione della legge penale. Diversamente, il prelievo di campioni biologici da soggetti non sospettati, e non sottoposti a misura restrittiva della libertà personale, presuppone il consenso esplicito del donante. Inoltre, si disciplina espressamente i diritti del cittadino in caso di ricerche di massa, imponendo agli investigatori di acquisire in forma scritta ed informata il consenso della persona alla quale si chiede di fornire materiale biologico.
Per quel che concerne gli Stati Uniti, il prelievo biologico è assimilato agli atti di perquisizione e sequestro (*search and seizure*), coperti dalle garanzie fissate dal IV Emendamento della Costituzione. Quindi, fatte salve ipotesi particolari (es. persona condannata e reclusa) anche per ottenere un tampone salivare serve un ordine del

Simile garanzia dovrebbe essere assicurata anche nell'ordinamento italiano, accompagnata dalla consapevolezza in capo al donante del possibile interessamento dei propri familiari o appratenti al gruppo biologico[115].

3 Il bilanciamento tra protezione della riservatezza ed efficienza investigativa nella gestione, conservazione , cancellazione o distruzione di dati e campioni biologici.

La legge 85/2009 tenta di delineare i rapporti di equilibrio tra diritto alla *privacy* e attività investigativa genetica. In questa prospettiva, essa prevede l'istituzione di due organismi aventi differenti funzioni: la banca dati nazionale del DNA presso il Ministero dell'interno[116] e il laboratorio centrale per la banca dati nazionale del DNA presso il Ministero della giustizia[117] (art. 5).

La scelta legislativa di separare a livello logistico-gestionale le due strutture è connessa alla diversità di funzioni svolte e si spiega in una logica garantista. Più precisamente, la banca dati nazionale adempie alla funzione di raccogliere i profili genetici raffrontandoli a fini identificativi (art. 7). Questa dovrà contenere, a fini di comparazione, tre tipologie di profili

---

giudice fondato sul requisito della *probable cause*, e cioè della sussistenza di ragionevoli sospetti di colpevolezza a carico dell'interessato. G. GENNARI, A. SANTOSUOSSO, *Il prelievo coattivo di campioni biologici*, cit.

[115] Del resto, per giustificare questa conclusione, si può invocare anche un parallellismo tra la disciplina delle indagini genetiche e il *favor pietatis* riconosciuto dell'ordinamento in seno all'art. 199, comma 3, c.p.p., nel quel si attribuisce ai prossimi congiunti la facoltà di astenersi dal testimoniare nel processo

[116] Dipartimento della pubblica sicurezza.

[117] Dipartimento dell'amministrazione penitenziaria.

genetici: quelli attribuiti a persone identificate come soggetti arrestati o fermati, indagati, imputati o condannati sottoposti a misura restrittiva della libertà personale (*ex* art. 9 commi 1 e 2), quelli appartenenti a persone scomparse o loro consanguinei, di cadaveri e resti cadaverici non identificati e, infine, quelli tipizzati da reperti biologici acquisiti nel corso di procedimenti penali (*ex* art. 10), anche se non ancora attribuiti a persone identificate.

All'interno della banca dati, però, possono essere inserti i profili genetici di soggetti che non sono coinvolti neppure indirettamente nelle indagini in base a prelievi coattivi disposti *ex* art. 359-bis c.p.p.[118]. Analogo problema, peraltro, si pone con riferimento ai profili genetici tipizzati dai reperti biologici acquisiti nel corso del procedimento penale da luoghi od oggetti su iniziativa della polizia giudiziaria durante il sopralluogo oppure nel corso di ispezioni e perquisizioni. All'esito di tali operazioni può, anche in tal caso, aversi la presenza non consensuale nella banca dati di un profilo genetico appartenente a un soggetto terzo rispetto al reato.

Ciò comprime in modo sproporzionato il diritto alla *privacy* di un individuo non sospettato o collegato direttamente al delitto. Sarebbe opportuno, quindi, introdurre a garanzia della *privacy* un divieto espresso di trasmettere alla banca dati nazionale del DNA profili appartenenti a soggetti identificati diversi dalla persona indagata/imputata.

Il laboratorio centrale, invece, svolge il delicato compito di tipizzare i profili del DNA dei soli soggetti ristretti nella libertà personale individuati dall'art. 9 per poi inviarli con un *file* alla banca dati: i relativi campioni biologici, invece, saranno conservati dal medesimo laboratorio (art. 8). Da

[118] G. GENNARI, *La istituzione della banca dati nazionale del DNA ad uso forense: dalla privacy alla sicurezza*, in A. SCARCELLA (a cura di), *Banca dati del DNA e accertamento penale*, cit., p. 50.

questo punto di vista, esso costituisce la principale fonte di approvvigionamento della banca dati. Di conseguenza, alla banca dati nazionale i profili genetici differenti da questi ultimi pervengono, al fine di essere archiviati, da altri laboratori specializzati.

A questo punto si comprende la *ratio* della separazione strutturale e funzionale del laboratorio e della banca dati, la quale dipende dalla differenza qualitativa tra i dati conservati nell'una e nell'altro[119], o, meglio, dalla differente capacità informativa del campione biologico rispetto al profilo del DNA[120]. Infatti, il profilo identificativo inserito nella banca dati contiene le sole informazioni ottenibili dalla analisi dei marcatori utilizzati (*ex* art. 11, comma 3°), mentre il campione di materiale biologico prelevato è una fonte potenzialmente infinita di informazioni personali[121].

Per garantire la riservatezza delle persone a cui i profili genetici si riferiscono, la legge 85/2009 prevede un sistema di controlli sia interni che esterni esercitato sull'attività di questi due organismi.

Per quanto concerne il controllo esterno, esso viene effettuato in via diretta[122] dal Garante per la protezione dei dati personali, che vigila sulla banca dati del DNA, e dal Comitato nazionale per la biosicurezza, le

---

[119] G. GENNARI, *La istituzione della banca dati nazionale del DNA ad uso forense: dalla privacy alla sicurezza,* in A. SCARCELLA (a cura di), cit., p. 60.

[120] G. LAGO, *Il trattamento dei dati e dei campioni biologici: la banca dati nazionale del DNA e il bilanciamento tra le ragioni di giustizia e la tutela della* privacy, in A. CARCELLA (a cura di), cit, p. 128.

[121] G. GENNARI, *op. loc. ult. cit.*

[122] A tale controllo esterno diretto si aggiunge una forma di controllo esteriore indiretto, cioè l'obbligo di informazione al Parlamento da parte dei Ministri dell'interno e della giustizia, con cadenza annuale, relativamente sia alle attività svolte nel periodo di riferimento da banca dati nazionale del DNA e laboratorio centrale, sia allo stato di attuazione delle norme previste dal capo II, riguardante proprio l'istituzione della banca dati e del laboratorio, per le parti di rispettiva competenza (art. 19).

biotecnologie e le scienze della vita (CNBBSV) che controlla il laboratorio centrale (art. 15)[123].

Al contrario, il controllo interno si esplica, in via mediata, attraverso le disposizioni relative al metodo di analisi dei reperti e campioni biologici (art. 11), nonché alle modalità di trattamento, accesso ai dati e tracciabilità dei campioni (art. 12). In questo senso, è necessario considerare che i profili del DNA, conservati nella banca dati, e i relativi campioni, custoditi nel laboratorio centrale, non contengono le informazioni che consentono l'identificazione diretta del soggetto cui si riferiscono. In altri termini, il trattamento è obbligatoriamente effettuato con dati anonimi e l'identificazione dell'interessato avviene esclusivamente se necessaria. Si è configurato, conseguentemente, una sorta di accesso "di secondo livello": l'autorità giudiziaria e la polizia giudiziaria dovranno prima richiedere di esperire il confronto tra il profilo genetico tipizzato e i dati archiviati e, in caso di esito positivo, potranno essere autorizzati a conoscere il nominativo del soggetto cui appartiene il profilo genetico preso in considerazione.

Sempre con l'intento di garantire il diritto alla riservatezza, viene posto il principio della tracciabilità in fase di trattamento del dato e in sede di accesso al *database* o biobanca, in base al quale risultano legittimati all'ingresso alla banca dati solo polizia giudiziaria e autorità giudiziaria. Tali soggetti possono accedere ai dati archiviati nella banca del DNA o a quelli conservati dal laboratorio centrale esclusivamente per fini di

[123] Nello specifico, il Comitato ha un duplice compito: garantire l'osservanza dei criteri e delle norme di sicurezza per il funzionamento del laboratorio centrale; eseguire, sentito il Garante della *privacy*, verifiche presso lo stesso laboratorio ed i laboratori che lo alimentano, formulando suggerimenti circa i compiti svolti, le procedure adottate, i criteri di sicurezza e le garanzie previste, nonché ogni altro aspetto ritenuto utile per il miglioramento del servizio. Cfr. C. COLAIACOVO, *Competenza del Garante per la protezione dei dati personali sull'applicazione del Trattato di Prüm*, in Aa. Vv., *Prelievo del DNA e banca dati nazionale*, cit., 173

identificazione personale, oltre che per scopi di collaborazione internazionale di polizia. Per rendere trasparente il trattamento e l'accesso in questione, gli operatori dovranno essere espressamente autorizzati e seguire modalità tali da assicurare la propria identificazione e la registrazione di ogni attività svolta.

L'introduzione della tracciabilità di dati e campioni costituisce un elemento positivo per la tutela della *privacy*, ma la sua efficacia è attenuata dal fatto che il numero dei soggetti potenzialmente abilitato all'ingresso è molto elevato (si tratta del personale e dei collaboratori internazionali delle forze di polizia) e la loro specifica individuazione è rimessa a singoli provvedimenti autorizzativi.

Con riferimento all'accesso nel *database*, inoltre, occorrerebbe consentire alla difesa dell'indagato, direttamente interessato dal prelievo, di conoscere i risultati delle analisi.

In definitiva, dovrebbero essere indicate in modo puntuale le persone abilitate ad utilizzare la banca dati nazionale, tenendo conto dei poteri investigativi attribuiti ai vari soggetti del procedimento[124].

Le criticità maggiori della riforma in esame, tuttavia, emergono in tema di custodia, cancellazione o distruzione di profili genetici e campioni biologici (art. 13). È sufficiente evidenziare che attualmente non risulta essere regolata la sorte del materiale biologico e dei profili genetici riferibili alla persona vivente. Infatti, non è normativamente prevista la "sede" della conservazione, né appare disciplinato completamente l'aspetto della cancellazione/distruzione.

[124] C. FANUELE, *Dati genetici e procedimento penale*, cit., 81; A. MONTI, *Catena di custodia e "doppio binario" per campioni e reperti*, in L. MARAFIOTI e L. LUPARIA, *Banca dati del DNA e accertamento penale*, cit., p. 102 e ss.

L'art. 72 quater delle disp. attt. c.p.p. , introdotto dalla novella, prevede solo la distruzione (salva diversa valutazione del giudice) dei campioni biologici acquisiti *ex* 224 c.p.p. immediatamente dopo la perizia con cui si sono estratti i profili genetici; l'attività è svolta dal perito già incaricato dal giudice e viene documentata tramite la redazione di un verbale[125]. Al contrario, la disposizione non prevede la cancellazione delle impronte genetiche tipizzate, che potrebbero essere trasmesse alla banca dati del DNA[126]. Parimenti non è disciplinata né la sorte dei profili genetici estratti da prelievo consensuale né quella del materiale biologico (e dei relativi profili genetici da esso tipizzati) prelevato dalla polizia giudiziaria, secondo quanto previsto dall'art. 349 comma 2-bis c.p.p[127].

In ogni caso, l'art. 72 quater disp. att. c.p.p. individua nel provvedimento conclusivo del procedimento un termine indefettibile per l'eliminazione dei soli campioni[128], mentre la legge 85/2009 chiarisce che alle sentenze

---

[125] Sui rischi di una circolazione, per scopi diversi da quelli processuali, dei dati genetici confluiti nel verbale attestante le operazioni di prelievi e accertamenti coattivi cfr. S .QUATTROCOLO, *I risvolti attuativi della novella in tema di prelievi coattivi: raccolta di campioni su incapaci; verbalizzazione delle operazioni; distruzione dei campioni*, in L. MARAFIOTI, L. LUPARIA, *Banca dati del DNA e accertamento penale*, cit., p. 336.

[126] La scelta di non inserire alcun riferimento all'art. 359-*bis* c.p.p. è dovuta alla volontà di garantire che sullo stesso campione biologico analizzato dal consulente tecnico sia esperibile anche la perizia, tutelando altresì la libertà personale del soggetto sottoposto al prelievo. Tuttavia, trattandosi di accertamenti tecnici ripetibili e considerato il scarsa invasività del prelievo (es. tampone salivare), sarebbe stato probabilmente più garantista stabilire la distruzione immediata anche di questo materiale biologico.

[127] Si crea una situazione del tutto sproporzionata per i prelievi genetici volontari, in quanto per essi, non solo, non è previsto alcun limite in ordine alla gravità del reato (in ipotesi potrebbero avvenire anche per una contravvenzione) o alla necessità investigativa, ma non è prevista neppure la cancellazione del profilo genetico –anche di terzo- o la distruzione del campione biologico. Sicché non sussiste per questi alcun limite temporale di conservazione legislativamente imposto.

[128] L'archiviazione è immediata nel caso di provvedimento di archiviazione, mentre, nell'ipotesi in cui si svolga il processo, il termine coincide con il memento della pronuncia della sentenza definitiva, sia essa di condanna o assoluzione.

definitive di assoluzione consegua d'ufficio la distruzione sia delle impronte genetiche che dei campioni (art. 13).

Fuori da questi casi, i dati indentificativi del DNA e, addirittura, i campioni biologici da cui gli stessi vengono estratti saranno conservati per tempi molto lunghi.

La legge 89/2009 si è limitata a fissare i termini massimi di conservazione senza prevedere una differenziazione in relazione alle persone a cui si riferiscono i dati genetici come, invece, sarebbe stato auspicabile in base al principio di proporzionalità[129]. Si è, infatti, stabilito che i campioni biologici possano essere conservati nel laboratorio fino al termine massimo di 20 anni. Limite che si eleva fino a 40 anni per i profili genetici contenuti nella banca dati nazionale.

Inoltre, vi è l'ulteriore problema rappresentato dall'individuazione del momento a partire dal quale decorrono i termini di conservazione, vale a dire «l'ultima circostanza che ha determinato» l'inserimento nella banca dati del profilo o il prelievo per la conservazione in laboratorio. Il rischio di simile previsione è che i termini per la conservazione siano fatti decorrere nuovamente nel caso in cui si verifichino nuove "non precisate" circostanze con il risultato che il periodo di conservazione potrebbe superare addirittura

[129] Il principio di proporzionalità tra tempo di conservazione dei dati genetici e finalità che ne giustificano la raccolta trae il proprio fondamento nella tutela del diritto alla riservatezza individuale di coloro che si sottopongono al prelievo. Ciò emerge, in modo particolare dalla giurisprudenza della Corte di Strasburgo che, nella sentenza S. e *Marper c. Regno Unito* considera la detenzione di materiale biologico e di profili di DNA come un'ingerenza dell'autorità pubblica nella vita privata del singolo, legittima solo entro i limiti posti dall'art. 8 par. 2 CEDU. Pertanto, la legge nazionale può contemplare la custodia e conservazione di questi dati sensibili solamente se essa è una misura necessari e proporzionata a garantire la sicurezza pubblica e la prevenzione dei reati. Diversamente, secondo il Giudice Europeo, sussiste un vero e proprio diritto alla distruzione facente capo al titolare delle informazioni genetiche. I. ABRUSCI, *Cancellazione dei profili e distruzione dei campioni,* in L. MARAFIOTI, L. LUPARIA (a cura di), *Banca dati del DNA e accertamento penale,* cit. p. 112 e ss.

il termine massimo dei 20 o 40 anni[130]. Tutto ciò senza che sia riconosciuta all'interessato la facoltà di domandare la cancellazione dei propri dati genetici, una volta trascorso il periodo di conservazione.

4 Segue: L'attività della banca dati nazionale del DNA: tutela della *privacy* e raffronto dei profili a fini investigativi.

Per espressa previsione della l. 85/2009, la funzione esplicata dalla banca dati nazionale del DNA consiste nella raccolta sistematica di profili genetici e nel raffronto tra essi a fini identificativi.

Le banche dati genetiche vengono solitamente consultate per ottenere un confronto tra le informazioni ivi conservate e le fonti di prove raccolte dalle forze di polizia. Il risultato a cui può condurre questa operazione è l'ottenimento di una corrispondenza (*match*) tra questi dati, che verrà impiegata per lo sviluppo delle indagini[131].

Più nello specifico, potrebbe verificarsi un riscontro tra un profilo proveniente dalla scena *criminis* e un profilo individuale già inserito nel *database*, o, viceversa, tra un nuovo profilo[132] e le tracce genetiche relative a un "vecchio" caso di reato irrisolto (c.d. *cold case*), oppure,

[130] I. ABRUSCI, *op. loc. ult. cit.*; G. BUSIA, Privacy *a rischio per la durata della conservazione*, in *Guida dir.*,2009, 30, p. 77-78.

[131] P. GAROFANO, *Genetica identificativa e biobanche: aspetti tecnici e problematiche connesse,* in *Dir.pen.proc., dossier*, 2008, 6, p. 44-50; V. BARBATO, F. CORRADI, G. LAGO, *L' identificazione personale tramite Dna*, in *Dir. pen. e proc.*, 1999, p. 215 e ss.

[132] Il profilo può essere raccolto o meno sul *locu commissi delicti*.

ancora, tra due profili personali inseriti in momenti diversi, anche sotto diverso nome (*alias*)[133].

Tale convergenza di informazioni si verifica spesso quando si compiono delle attività di ricerca nella banca dati volte a individuare un *full match*, ossia una perfetta corrispondenza tra tutti i segmenti di DNA che compongono il profilo genetico individuato nel corso delle indagini e quello archiviato in precedenza[134].

Può accadere, però, non vigendo alcun divieto legislativo in merito, che si effettuino delle ricerche di sovrapponibilità solo parziale in grado di far emergere una eventuale parentela tra l'autore del reato e coloro che si trovano archiviati nella banca dati (*familial searching*), comprimendo il diritto alla riservatezza dei membri del nucleo familiare[135].

Per operare tale attività di comparazione identificativa la banca dati nazionale del DNA deve contenere, oltre ai profili tipizzati ex artt. 9, 10, 24 e 25 l. 85/2009, i profili ricavati dai reperti acquisiti nel corso di procedimenti penali antecedenti alla legge 85/2009 senza alcuna forma di controllo o coordinamento in pregiudizio alla tutela della *privacy*.

I reparti speciali della polizia giudiziaria scientifica, infatti, praticavano già prima dell'istituzione del *database* nazionale i raffronti tra le informazioni genetiche a disposizione a scopo ricognitivo. A tal proposito,

---

[133] G. GENNARI, *op. cit.*, p. 63.

[134] Tecnica di ricerca basata sul fatto che ogni persona ha un patrimonio genetico formato dalla combinazione di metà del patrimonio genetico della madre e di metà di quello del padre. Anziché ricercare la piena corrispondenza tra il profilo proveniente dalla scena del crimine e quello di un soggetto inserito nella banca dati, si cercano corrispondenze parziali, che possono fare emergere un possibile vincolo di parentela tra l'autore del fatto e colui o coloro il cui profilo si trova nella banca dati. G. GENNARI, *op.loc.ult.cit*.

[135] Cfr. parte II cap. I par. 3.

la crescente importanza, attribuita a simili operazioni ha portato le forze di investigazione scientifica a creare archivi genetici non autorizzati[136].

In questa prospettiva, emerge un aspetto problematico legato al temporaneo operare delle banche dati ufficiose anche dopo l'istituzione del *database* nazionale del DNA e del laboratorio centrale, nei quali le prime avrebbero dovuto confluire entro un anno dalla entrata in vigore della riforma.

Questo ritardo nell'attuare la legge 85/2009 ha permesso che, di fatto, questi archivi rimanessero in attività, senza prevedere alcun incremento degli *standards* di sicurezza o una intensificazione dei controlli. La conseguenza è che esistono ed operano tuttora banche dati delle quali non si ha contezza, in quanto non sono mai state monitorate dai ministeri della Giustizia e degli Interni.

Al momento si conoscono gli archivi informatico-genetici istituiti ad opera del R.IS, i quali contengono non solo i profili genetici ma anche i relativi campioni biologici, acquisiti da tutti i soggetti coinvolti in un dato procedimento penale (reo, vittima o parente che fosse) e repertati senza alcuna forma di controllo.

Tali banche dati, realizzate in assenza di una normativa di riferimento, suscitano dubbi di legittimità poiché, oltre ad operare in segretezza, non forniscono garanzie in termini di tutela della riservatezza, affidabilità

[136] Il materiale biologico ivi contenuto, non essendo possibile effettuare i prelievi coattivi, era raccolto ricorrendo a "stratagemmi" quali raccogliere oggetti abbandonati spontaneamente (es. mozziconi di sigarette) o effettuare sequestri di cose pertinenti al reato (es. indumenti intimi o pettine). L'utilizzo dei campioni volontariamente abbandonati è stato ammesso dalla sentenza Ass. Torino, ord. 21 aprile 2004, in *Dir. pen. proc*, 2005, p. 347 con nota di M. SPRIANO, *Acquisizione del DNA dall'imputato e dai suoi parenti*.

della procedura di tipizzazione[137], sicurezza e conservazione del materiale biologico[138].

Tale situazione in più occasioni è stata censurata dal Garante per la protezione dei dati che è intervenuto al fine di controllare il rispetto delle disposizioni di cui al d.lgs. n. 196 del 2003[139] .

In definitiva, dato il perdurante del silenzio legislativo sulla sorte degli archivi genetici e delle banche dati attivi presso le forze di polizia o i laboratori specializzati incaricati dalla magistratura, si avverte l'esigenza imprescindibile che vengano promulgati al più presto i regolamenti attuativi.

---

[137] Ai sensi dei requisiti tecnici richiesti dall'art. 11 l. 85/2009.

[138] Sul piano giurisprudenziale, tuttavia, la suprema Corte ha di fatto legittimato la procedura adottata da alcuni reparti scientifici della polizia giudiziaria nel senso che non è inutilizzabile, in mancanza della violazione di un divieto di legge, l'accertamento sull'identità dell'indagato compiuto mediante ricorso ai dati relativi al DNA contenuti in un archivio informatico che la polizia giudiziaria abbia istituito prescindendo dalle cautele previste dal codice della *privacy* (nella specie la Corte ha ritenuto corretta l'individuazione dell'autore del furto realizzata attraverso il confronto del DNA estratto da capelli rinvenuti nell'abitacolo dell'autovettura rubata con il codice genetico dell'imputato, conservato negli archivi informatici della p.g.). Cass., sez. V, 5 febbraio 2007, in *Ced* , n. 235969.

[139] Nelle banche dati in questione devono essere adottate le misure di sicurezza minime che sono previste dalla legge sulla *privacy* e che lo stesso Garante ha citato e imposto in relazione al Ris di Parma. Le misure prescritte dal Garante e adottate dalle Forze di polizia scientifica per la messa in sicurezza dei dati sono particolarmente rigorose. Tra le principali figurano l'obbligo di conservare traccia di ogni accesso al database e delle operazioni effettuate dal personale autorizzato che ha accesso ai campioni; l'adozione di sistemi di autenticazione per il personale che accede al database nonché sistemi elettronici (almeno con riconoscimento biometrico) per controllare l'ingresso ai locali dove sono conservati i campioni biologici; l'individuazione preventiva del personale autorizzato alla loro consultazione; l'adozione di soluzioni tali da non rendere i campioni conservati direttamente riconducibili a persone identificate. Al Ris è stato infine prescritto che l'eventuale ulteriore uso dei profili e dei campioni biologici, compresa l'attività di comparazione tra i profili genetici, deve essere effettuato attenendosi alle disposizioni delle competenti autorità giudiziarie. Il Comando generale dell'Arma dei Carabinieri ha comunicato, infine al Garante, che le stesse misure sono state applicate, oltre che al Reparto di Parma, anche agli altri Ris di Roma, Messina e Cagliari. Roma, 25 maggio 2009. V. Comunicato stampa, in *www.garanteprivacy.it*.

In questa prospettiva, la regolamentazione delle banche dati già esistenti dovrebbe prevedere indicazioni precise sul trasferimento di tutti i profili del DNA tipizzati e dei reperti biologici ivi contenuti e sulla distruzione dei campioni acquisiti con modalità non conformi alla nuova disciplina.[140] Certo, la soluzione più garantista per la riservatezza, e, in generale, per la tutela dei diritti fondamentali sarebbe conservare solo la sequenza alfanumerica che individua il campione, anziché quest'ultimo nella sua integralità. Tale operazione eviterebbe ulteriori indebite conservazioni, duplicazioni dei profili o di parte dei campioni biologici presso singole banche dati gestite dalle forze di polizia[141].

5 La protezione della *privacy* e la "cooperazione informativa" di dati genetici dopo la legge di ratifica del Trattato di Prüm.

Per affrontare il tema dello scambio reciproco di informazioni successivamente alla ratifica del Trattato di Prüm è utile fare una breve premessa sulla circolazione dei dati personali nello spazio giudiziario europeo, nonché sui meccanismi volti a consentire alle autorità

[140] G. SCROLLO, *Il regime transitorio,* in L. MARAFIOTI e L. LUPARIA, *Banca dati del DNA e accertamento penale,* cit., p. 167.

[141] Ciò perché il maggiore pericolo per la *privacy* potrebbe derivare proprio dall'uso del DNA archiviato. Mentre il profilo genetico non permette, di per sé, di risalire ad altre informazioni personali, al contrario, il campione biologico, permette di ricavare cognizioni suscettibili d'impiego per finalità diverse da quelle penali. Ad esempio, in Australia, dove esiste da tempo una banca dati del genere di cui qui si tratta, è stata aperta - per la prima volta al mondo - un'inchiesta circa ipotetiche discriminazioni genetiche, che sarebbero intervenute, da parte di talune compagnie assicurative, nella stipula di polizze sulla vita. C. FANUELE, *Dati genetici e procedimento penale,* cit., 8

giurisdizionali e di polizia dei diversi Stati membri la condivisione delle notizie in possesso delle autorità straniere (cd. *information sharing*)[142].

In materia di "cooperazione informativa", fondamentale è ricordare il Programma dell'Aja, adottato dal Consiglio Europeo il 4 novembre 2004[143], con il quale è stato introdotto il principio di disponibilità delle informazioni, che comporta la libera circolazione delle stesse nel territorio dell'Unione in un'ottica di rafforzamento della giustizia e sicurezza[144]. Tale

[142] L'obiettivo di garantire un elevato livello di protezione ai cittadini europei nello spazio di libertà, sicurezza e giustizia era posto dall'art. 29 del TUE nell'ambito del c.d. terzo pilastro. Le linee guida per la sua realizzazione, dettate dall'art. 29 comma 2 TUE, erano la progressiva armonizzazione degli ordinamenti statuali interni in materia penale e il rafforzamento della cooperazione tra le forze di polizia e le autorità giudiziarie degli Stati membri. Questi due profili, pur essendo distinti, si pongono in rapporto di complementarità. Cfr. E. BERNARDI, *Strategie per l'armonizzazione dei sistemi penali europei*, in *Riv. Trim. dir. pen. ec*., 2002, p. 789.Per quanto riguarda gli atti normativi adottati al fine di realizzare lo spazio comune di libertà sicurezza e giustizia sancito dai Trattati di Amsterdam e di Nizza nonché riaffermato nelle conclusioni prese in seno al Consiglio europeo di Tampere del 1999, cfr. M. CHIAVARIO, *Cooperazione giudiziaria e di polizia in materia penale a livello europeo,* in *Riv. it. dir. proc. pen.*, 2005, p. 974; L. SALAZAR, *La costruzione di uno spazio di libertà, sicurezza e giustizia dopo il consiglio europeo di Tampere,* in *Cass. pen.,* 2000, p.1114; ID, *La lotta alla criminalità nell'unione: passi avanti verso uno spazio giudiziario comune prima e dopo la costituzione per l'Europa ed il programma dell'Aia, ivi,* 2004, p. 3510. Invece, per un esame delle iniziative volte a superare la struttura dell'U.E. fondata su tre pilastri (Comunità europea, PESC, cioè politica estera e sicurezza comune, e GAI, cioè giustizia e affari interni) cfr. M. BARGIS, *Costituzione per l'Europa e cooperazione giudiziaria in materia penale*, in *Riv. it. dir. proc.pen.*, 2005, p. 144; G. De Amicis - G. Uzzolino, *Lo spazio di libertà, sicurezza e giustizia nelle disposizioni penali del Trattato che istituisce una Costituzione per l'Europa*, in *Cass. pen.*, 2004, p. 3067.

[143] Programma dell'Aia, in *GUUE*, c-53, 3 marzo 2005, p. 1 e il relativo Piano di attuazione del 2-3 giugno 2005 in *GUUE*, C 198, 12 agosto 2005, p. 1.

[144] Invero, già il Consiglio europeo di Tampere del 1999 aveva definito il primo quadro politico pluriennale per la cooperazione di polizia, indicando la fiducia e il riconoscimento reciproco quali nuove basi di azione [Conclusioni del consiglio di Tampere pubblicate in *Cass. pen.*, 2000, p. 302]. Le linee di questa azione sono state, poi, indicate dal Programma dell'Aia in cui si fissavano alcuni obiettivi strategici per l'Ue tra cui la lotta alla criminalità organizzata e transfrontaliera e il terrorismo. Il programma per facilitare lo scambio di informazioni tra le forze di polizia appartenenti ai diversi Stati prevedeva il ricorso alle banche dati nazionali e stabiliva che la circolazione dei dati avvenisse, a far data dal 2008, in base al canone della disponibilità.

principio mira a realizzare lo scambio reciproco dei dati in possesso di una singola Nazione con gli organismi di polizia degli altri Stati e implica la predisposizione di norme comuni in materia di accesso alle informazioni personali[145], alla conservazione delle stesse e alla tutela della riservatezza individuale[146]. In altri termini, in base ad esso, l'accesso e la condivisione di dati tra gli Stati membri dell'Ue deve avvenire in modo tale da consentire a una forza di contrasto di un Paese membro, che necessiti di talune informazioni per prevenire o reprimere determinati reati, di ottenerle

[145] La necessità di garantire una protezione efficace dei dati personali trattati ai fini di cooperazione giudiziaria e di polizia in ambito penale emerge parallelamente al rafforzamento del terzo pilastro con il Trattato di Amsterdam del 1997. Si è iniziato, infatti, a discutere l'opportunità di armonizzare le norme sulla protezione dei dati per migliorare la cooperazione giudiziaria e di polizia già nel piano di azione di Vienna del Consiglio e delle Commissione sul modo attuare al meglio le norme del Trattato Amsterdam in *GUUE*, C 19, 23 novembre 1999, p. 1. La vera svolta, però, si è avuta con il Programma dell'Aia e con il successivo paino di azione. In questi documenti programmatici, il Consiglio europeo ha affermato che la realizzazione di uno spazio di libertà, sicurezza e giustizia presuppone sia il consolidamento della sicurezza che il rafforzamento dei diritti fondamentali riconosciuti nella CEDU e nella Carta di Nizza, *in primis* la tutela della vita privata e dei dati personali. Per cui, tra le priorità fissate per il quinquennio (2005-2009) vi era la necessità di trovare un equilibrio tra lo scambio di informazioni esistente tra forze dell'ordine (o autorità giudiziarie) al fine di garantire la sicurezza e la tutela della riservatezza. Cfr. Comunicazione della Commissione al Consiglio e al Parlamento europeo, del 10 maggio 2005, *Il programma dell'Aia: dieci priorità per i prossimi cinque anni. Partenariato per rinnovare l'Europa nel campo della libertà, sicurezza e giustizia*, COM(2005), 184 definitivo, p. 6, in *www. eur-lex.europa.ue.it.*

[146] Parte della dottrina sottolinea che nel Programma dell'Aia è individuabile un principio di disponibilità in senso lato, a cui si collegherebbero i tre corollari del principio di conservazione delle informazioni rilevanti ai fini di prevenzione e repressione della criminalità, il principio di disponibilità in senso stretto e quello di accessibilità M. GIALUZ, *La cooperazione informativa quale motore del sistema europeo di sicurezza,* in F. PERONI, M. GIALUZ (a cura di),*Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009, p. 18 e ss. Più ampiamente sul principio di disponibilità nel Programma dell'Aia cfr. anche S. CIAMPI, *Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea,* in F. PERONI, M. GIALUZ, cit., p. 34.

direttamente da un altro Stato membro, alle stesse condizioni previste per le autorità interne[147].

L'enunciazione di questo principio costituisce una novità per la cooperazione nell'area europea, ove tradizionalmente operano strumenti basati sul presupposto dell'appartenenza esclusiva delle informazioni alle autorità degli Stati che le detengono, i quali possono stabilire limiti e condizioni di accesso alle proprie banche dati [148].

Superando tale impostazione e ispirandosi al principio di disponibilità, il Trattato di Prüm, il cui contenuto è stato sostanzialmente recepito dalla decisione 2008/615/GAI (cd. Decisione Prüm)[149], vuole rafforzare la cooperazione tra gli organi di pubblica sicurezza nei settori della lotta contro il terrorismo, della criminalità transnazionale e dell'immigrazione

[147] Probabilmente si è di fronte a un'ulteriore applicazione ai principi della libera circolazione e del mutuo riconoscimento, nati originariamente per le merci e i prodotti e, successivamente, estesi a capitali, servizi, decisioni giudiziarie e, infine, ai beni immateriali come i dati in possesso di privati o degli organi pubblici. In tal senso si è espresso il Garante europeo della protezione dei dati personali (GEPD), *Terzo parere sulla proposta di decisione quadro sulla protezione dei dati personali trattati nell'ambito del terzo pilastro,* in *GUUE*, c 139, 23 giugno 2007, p.1.

[148] Basta pensare al SIS (Sistema Informativo Schengen), E-TECS di Europol, EPOC-III di Eurojust.

[149] Decisioni quadro 2008/615/GAI in *GUUE*, L 210, 6 agosto 2008, p. 1 e decisione quadro attuativa della prima 2008/616/GAI, *ivi*, p.12, sul punto cfr. cap. 1 parte I nota 54. Il Consiglio dell'Unione europea fa proprie le disposizioni del Trattato attraverso la decisione 2008/615/GAI, in cui ricalca e recepisce sostanzialmente i contenuti normativi dell'atto internazionale, così inserendo quelle disposizioni all'interno della legislazione europea. Invero, misure volte ad agevolare lo scambio di informazioni investigative erano già state adottate nell'ambito della normativa europea. Tra queste, vi è la decisione 2005/671/GAI del 20 settembre 2005 sullo scambio di informazioni e la cooperazione in materia di reati terroristici e la decisione 2006/960/GAI del 18 dicembre 2006 concernente lo scambio di informazioni e di *intelligence* tra le autorità degli Stati membri dell'Ue incaricate dell'applicazione della legge, in base a un meccanismo di reciproco scambio ispirato al canone della disponibilità, nonché recentemente la decisione 2009/426/GAI relativa al rafforzamento di Eurojust, rispettivamente in *GUUE*, L 252, 27 settembre 2005, p. 22, *ivi*, L 386, 29 dicembre 2006, p. 89 e *ivi*, L 138, 4 giugno 2009, p. 14.

clandestina mediante lo scambio diretto delle informazioni in possesso dei singoli Stati[150].

Più precisamente, le Nazioni aderenti al Trattato si impegnano a istituire tre banche dati nazionali accessibili *on-line* e contenenti profili genetici, dati in materia di impronte digitali (*fingerprints*) e dati relativi ai veicoli iscritti nei pubblici registri.

Certamente la semplificazione e velocizzazione della circolazione di dati sensibili, in specie quelli genetici, pone inevitabilmente problemi di tutela del diritto alla *privacy* individuale. Per quanto riguarda la cooperazione informativa tra gli Stati, il Trattato e la decisione n. 615 hanno affrontato la questione introducendo una disciplina dettagliata dei meccanismi di scambio di dati, che garantisce l'efficienza delle indagini e contemporaneamente tutela la *privacy*. In ossequio a ciò la legge italiana 85/2009 di recepimento dell'accordo di Prüm rinvia espressamente alle norme più significative del Trattato in tema di cooperazione (art 20).

Nello specifico, queste disposizioni affidano la gestione degli scambi di dati tra le diverse autorità statali ai punti di contatto nazionali autorizzati in via esclusiva ad accedere e consultare i dati archiviati, potendo procedere a una comparazione automatizzata dei profili di DNA.

I meccanismi di accesso alla informazioni sono differenziati in base alla tipologia di dato richiesto, sicché esistono due diversi "livelli di tutela" del diritto alla riservatezza a seconda della natura più o meno sensibile dell'informazione da trattare. Per quanto riguarda i dati meno sensibili, ossia quelli attinenti ai veicoli, si prevede un accesso diretto *on-line* a tutte le notizie in possesso dello Stato richiesto. Al contrario, per i dati personali

[150] La decisione statuisce, come peraltro il Trattato (art. 37), che per gli Stati membri le disposizioni della stessa prevalgano sulle corrispondenti norme del Trattato.

più sensibili, *id est* quelli genetici (e dattiloscopici), non si consente una immediata identificazione della persona interessata, ma si stabilisce un procedimento di consultazione diviso in due fasi (cd. doppio binario).

In primis, si consente l'accesso automatizzato (via *internet* e in tempo reale) agli indici di consultazione contenuti all'interno delle banche dati (cd. sistema *hit/no hit*). Pertanto, mediante questa procedura l'autorità richiedente può visionare direttamente e unicamente i profili di DNA (o i dati dattiloscopici) anonimi, a cui è abbinato un numero di riferimento (*reference index*) al fine di verificare la presenza del dato nell'archivio. Tale procedura di accesso, a seconda del tipo di informazione in possesso della parte procedente, può avvenire in due modalità: la consultazione o la comparazione. Nel primo caso, l'autorità richiedente dispone di un profilo DNA riferibile a un soggetto identificato e, pertanto, può avviare una procedura di consultazione automatizzata per verificare se il dato in suo possesso trovi una concordanza tra le informazioni registrate nella banca dati straniera. Lo scopo della consultazione è, pertanto, quello di accertare se la banca dati contenga un profilo corrispondente a quello trasmesso. Nella seconda ipotesi, invece, la parte richiedente ha raccolto un profilo DNA non attribuibile a una persona determinata (*cd. open record*), sicché può attivare un procedimento automatico di comparazione. Questa procedura è avviata mediante la trasmissione alla banca dati del profilo anonimo al fine di controllarne la corrispondenza con tutti i dati ivi contenuti, siano o meno riferibili a un individuo identificato. Le due forme di accesso alla banca dati, quindi, si distinguono principalmente per il tipo di dato biologico a disposizione dello Stato richiedente, costituito, nel primo caso, da un profilo identificato, e, nel secondo caso, da una "traccia

anonima" (o cd. traccia aperta), mentre la procedura di ricerca è automatizzata e segue modalità analoghe.

Vi è, poi, una seconda fase diretta ad acquisire le informazioni non disponibili *on line* e si svolge solo se si verifica una corrispondenza tra i dati archiviati e quelli in possesso dell'organo nazionale procedente. Per cui gli indici consentono solo di verificare se le informazioni richieste sono presenti nella banca dati senza che sia possibile l'identificazione personale.

L'esito positivo o negativo dell'accesso telematico per svolgere la consultazione o la comparazione è comunicato automaticamente all'autorità che ha domandato le notizie. Solamente quando tale ricerca abbia dato un risultato positivo, riscontrando una corrispondenza tra dati immessi e dati archiviati nel *database*, si apre la seconda fase del procedimento che riguarda la trasmissione allo Stato richiedente delle informazioni che consentono l'identificazione dell'interessato. L'inoltro di simili dati, però, non avviene in forma automatizzata ed è a cura dell'autorità a cui è rivolta l'istanza[151].

A fronte di una disciplina così attenta alla tutela della riservatezza individuale sul piano dello scambio reciproco di informazioni tra Nazioni, tuttavia, non corrisponde una pari attenzione per la gestione nazionale dei dati raccolti e trasmessi dalle singoli Paesi. Né il Trattato di Prüm né la decisione 2008/615/GAI dettano, infatti, specifiche regole comuni per garantire uno *standard* minimo di tutela alla *privacy* durante il trattamento nazionale delle informazioni. La mancanza di una disciplina normativa generale del diritto alla protezione di particolari dati personali come le informazioni genetiche nell'ambito dell'attività di polizia svolta all'interno

[151] E CALVANESE, *Adesione al Trattato di Prüm e cooperazione transfrontaliera*, in A. SCARCELLA (a cura di), cit., p. 11; F.GANDINI, *Trattato di Prüm: modello di cooperazione transfrontaliera*, in *D. & G.*, 2006, 37, p. 56 e ss.

dei singoli Stati rappresenta un pericolo per la protezione della vita privata individuale e allo stesso tempo potrebbe diventare un freno alla libera circolazione degli stessi[152].

Il Trattato di Prüm, a cui la legge 85/2009 rinvia, e la decisione n. 615, infatti, lasciano alla valutazione del legislatore nazionale l'individuazione delle finalità di raccolta dei dati, la cerchia di persone interessate alla raccolta dei dati e, infine, non regolano il periodo di conservazione dei dati schedati[153].

In conclusione, sul versante della condivisione di informazioni (*information sharingh)* tra le forze di polizia straniere nell'ambito delle indagini genetiche, lo sviluppo di efficaci strumenti di prevenzione e repressione dei reati a livello europeo non si è accompagnato dalla predisposizione di *standard* uniformi di tutela dei dati personali dei soggetti coinvolti nel procedimento penale sul piano dei singoli ordinamenti giuridici.

---

[152] La decisione quadro 2008/977/GAI del Consiglio del 27 novembre 2008, in *GUUE,* L 350, 30 dicembre 2008 disciplina esclusivamente l'*information sharingh* tra gli Stati e non prevede alcuna disposizione relativamente al trattamento nazionale dei dati, come avveniva con la presedente direttiva 1995/46/CE e successive modificazioni. Tali disposizioni, oltre ad avere un ambito applicativo ridotto, si applicano in via residuale rispetto alle norme disciplinanti il funzionamento di Eurojust, Europol, il sistema informativo di Shenghen (SIS), il sistema informativo doganale (SIS) e il sistema introdotto dalla cd. Decisione Prüm.

[153] Tali profili sono stati criticati anche dal Garante europeo (GEPD) che, in merito alla proposta di decisione di recepimento del Trattato, ha sollevato le seguenti censure al sistema di scambio stabilito nell'accordo di Prüm: mancanza dell'indicazione della finalità di raccolta dei dati, poiché non si precisa se le disposizioni sui profili di DNA si applichino a tutti i reati ovvero se un Stato aderente abbia la facoltà di restringerne l'applicazione agli illeciti più gravi; assenza di una delimitazione della cerchia di persone interessate dalla raccolta dei dati; mancanza di indicazioni per la disciplina interna del periodo di conservazione dei dati nelle banche dati genetiche. Garante europeo per la protezione dei dati, *Terzo parere sulla proposta di decisione quadro del Consiglio sulla protezione dei dati personali nell'ambito della cooperazione giudiziaria e di polizia in materia penale*, cit.

CAPITOLO II

Tutela della riservatezza e indagini informatiche

Sommario: 1. La *privacy* in ambito informatico - 2. Il difficile equilibrio tra conservazione di dati digitali (*data retention*), salvaguardia della riservatezza (*data protection*) e indagini informatiche - 3. Segue: le comunicazioni VoIP- 4. La salvaguardia della *privacy* nelle perquisizioni - 5. La garanzia del diritto riservatezza e i sequestri informatici.

1 . La *privacy* in ambito informatico.

La tutela del diritto individuale alla *privacy* deve tenere in considerazione la cd. rivoluzione tecnologica avvenuta nell'ambito informatico a partire dagli anni settanta, la quale ha determinato una progressiva espansione di questo settore nonché la diffusione degli strumenti a esso connessi[154].

La facilità di riproduzione, memorizzazione, trasmissione e trattamento automatizzato di dati digitali, unita al progresso tecnico e alla accessibilità dei sistemi di gestione, hanno comportato l'impiego dei mezzi informatici nei settori produttivi e nella vita comune.

[154] Per informatica si intende la scienza che si occupa dell'elaborazione, della conservazione e della trasmissione di dati attraverso elaboratori elettronici. Mentre con il termine *computer forensics* si fa riferimento alla disciplina che si occupa delle tecniche e degli strumenti usati per recuperare gli elementi di prova digitali all'interno di un elaboratore elettronico. Per le distinzioni create, a livello dottrinale, in base all'oggetto di analisi della *computer forensics.* cfr. S. ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. pen. proc., Dossier*, 2008, p. 60.

L'uso di questi nuovi strumenti ha fatto sì che i rapporti interpersonali e l'assetto economico fossero legati sempre più di frequente a raccolta, trattamento e circolazione di informazioni sotto forma di *file*. Inoltre, la crescita delle reti *internet*, negli ultimi quindici anni, ha rafforzato tale tendenza.

Di pari passo, si è sviluppata una criminalità che ha sfruttato queste nuove conoscenze per commettere reati già puniti dal codice penale o per tenere nuove condotte offensive non ancora sanzionate penalmente, determinando così l'introduzione da parte del legislatore di nuove fattispecie incriminatrici (cd. *computer crimes*)[155].

L'accertamento giudiziale di simili fatti illeciti necessita di tecnologie idonee a ricercare e acquisire elementi di prova digitali.

Per cui, i mezzi informatici rivestono un ruolo fondamentale nello svolgimento delle indagini preliminari e il loro utilizzo è dovuto alle caratteristiche intrinseche dei dati elettronici che, in quanto immateriali, sono volatili ed altamente modificabili anche per effetto di un semplice accesso[156].

Per tale ragione, oltre che per l'enorme capacità di archiviazione dei supporti informatici su cui sono memorizzati i dati digitali e per l'assenza

---

[155] L. LUPARIA, *La disciplina processuale e le garanzie difensive*, in L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Giuffré, Milano, 2007, p. 130; R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, p. 128 e ss.; L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, ID, *Il diritto penale dell'informatica nell'epoca di* internet, Cedam, Padova, 2004, p. 86 e ss.; C. SARZANA DI S. IPPOLITO, *Informatica*, internet *e diritto penale*, III ed., Giuffré, Milano, 2010, p. 61.

[156] O. DOMINIONI, *La prova penale scientifica*, Giuffrè, Milano, 2005, p. 37; L. MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4510. Tale ultimo Autore, tuttavia, precisa che l'accesso debba essere compiuto secondo modalità errate.

di barriere fisiche alla trasmissione degli stessi sui circuiti telematici, i dati digitali pongono evidenti problemi di tutela della riservatezza individuale.

Ciò ha determinato la nascita di un nuovo concetto di *privacy* che ha a oggetto le informazioni personali trattate con i mezzi informatici e riguarda la possibilità di accesso, controllo e trattamento dei dati personali in tale contesto[157]. Simile diritto soggettivo, tuttavia, deve essere posto in bilanciamento con l'esigenza di dotare gli organi inquirenti di efficaci strumenti investigativi per la repressione dei reati. Questa necessità investigativa pone la questione dell'adeguatezza della legislazione italiana a garantire, da un lato, la genuinità della fonti di prova raccolte nel corso delle cd. indagini informatiche e, dall'altro, la tutela del diritto alla riservatezza individuale.

L'assenza di norme specifiche, volte a disciplinare l'assunzione e l'utilizzo delle prove digitali nel processo[158], ha consentito per lungo tempo agli inquirenti di scegliere i metodi tecnici per l'acquisizione delle fonti di prova, che, a volte, minavano la genuinità degli elementi raccolti o consentivano condotte contrastanti con la *privacy* individuale, come nel caso di sequestri di componenti informatiche superflue all'accertamento dei fatti di reato[159].

---

[157] L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislative e beni giuridici tutelati*, in ID, *Il diritto penale dell'informatica nell'epoca di* internet, cit., p. 77.

[158] La lacuna sul piano normativo era peraltro aggravata dall'assenza, anche sul piano pratico, prassi o procedura acquisitive standard, che fossero generalmente riconosciute come valide.

[159] G. COSATBILE, D. RASETTI , Scena criminis, *documento informatico e formazione della prova penale*, in *Ciberspazio e diritto*, 2003, p. 273; A. MONTI, *La nuova disciplina del sequestro informatico*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, cit., Giuffrè, Milano, 2009, p. 199.

Solo con la l. del 18 marzo n. 48 del 2008 di conversione della Convenzione di Budapest (c.d. Convenzione sul *cybercrime*) si è, per la prima volta, tentato di introdurre una disciplina organica delle indagini penali informatiche per evitare attività investigative contrastanti con la riservatezza individuale e idonee a garantire la genuinità delle fonti di prova acquisite.

2. Il difficile equilibrio tra conservazione di dati digitali (*data retention*), salvaguardia della riservatezza (*data protection*) e indagini informatiche.

Il diritto alla riservatezza nell'ambito delle indagini digitali sempre più spesso subisce una compressione in occasione del *cd. tracing* (o "tracciamento"), espressione con cui si indica il "percorso a ritroso" finalizzato a trovare l'origine della condotta di reato posta in essere con strumenti informatici, individuando e conservando alcune informazioni "esterne" legate alla comunicazione effettuata dall'utenza, similmente a quanto si verifica con i tabulati telefonici [160].

[160] Semplificando può dirsi che il risultato concreto del *tracing* è un indirizzo IP (*Internet Protocol)* di connessione della macchina da cui - verosimilmente - è originato l'evento informatico costituente reato, cioè un numero telefonico relativo alla richiesta connessione. La definizione di indirizzo di protocollo internet (IP) univocamente assegnato è inserita nel d. lgs 109/2008 art. 1 lett. g) secondo il quale l'indirizzo *de quo* consente l'identificazione diretta dell'abbonato o utente che effettua comunicazioni sulla rete pubblica. In altri termini, si tratta di un numero che identifica univocamente i dispositivi collegati con una rete informatica che utilizza lo standard IP (*Internet Protocol*). Ciascun dispositivo (*router*, *computer*, *server* di rete, stampanti, alcuni tipi di telefoni, etc..) ha, quindi, il proprio indirizzo IP, che, in via di semplificazione, può essere visto come l'equivalente di un numero telefonico attribuito ai dispositivi collegati su *internet*. Infatti, come un numero telefonico identifica una data linea telefonica, così un indirizzo IP identifica univocamente uno specifico *computer* o un

In tale contesto, le frizioni con il diritto alla *privacy* sono dovute al fatto che per accertare il traffico telematico si conservano i *files* di *log* (o *files* di registro), che indicano le operazioni compiute dall'utente durante la navigazione e consentono, attraverso gli indirizzi IP (*Internet Protocol*)[161], l'identificazione dello stesso, del destinatario e, a volte, la ricostruzione del contenuto della comunicazione[162]. Per trovare un punto di equilibrio tra gestione dei dati in questione, garanzie individuali e necessità investigative[163] appare, quindi, necessario determinare quali possano essere le informazioni concretamente archiviate, quali siano i soggetti gravati da tale obbligo e quale possa essere il tempo massimo di conservazione delle stesse[164].

---

qualsiasi altro dispositivo di rete o una rete. Abbinato a questo IP possiamo trovare un *computer* singolo, un *computer* in rete (aziendale, *wireless*), un cd. *internet mobile phone* (cellulari che consentono le connessioni *internet*) con scheda prepagata. Probabilmente si possono avere risultati investigativi utili (ove effettivamente venga ritrovata la macchina interessata) solo nel primo caso, mentre con i *computer* in rete, soprattutto se *wireless*, si può incorrere in ipotesi in cui la rete è mal configurata o non protetta. In tale caso, è spesso possibile collegarsi ad *internet*, stando all'esterno del locale a cui l'utenza si riferisce (es. dalla pubblica via). Nel terzo caso, invece, può verificarsi che la sceda prepagata sia stata attivata con dati fittizi. F. CAJANI, Internet protocol. *Questioni operative in tema di investigazioni penali e riservatezza,* in *Dir. Internet.* 2008, p. 545.

[161] Cfr. nota 5 cap. II parte II.

[162] F. CAJANI, *Alla ricerca del* log *(perduto),* in *Dir. Internet*, 2006, p.572 e ss. In altri termini, si tratta di *files* che contengono informazioni relative alle attività compiute dagli utilizzatori dei sistemi informatici e telematici, generate dagli stessi sistemi per esigenze prevalentemente di carattere tecnico (per individuare guasti o anomalie funzionali) oppure di sicurezza (con l'intento di prevenire o rilevare intrusioni o violazioni all'interno della propria rete).

[163] Sul conflitto tra *data retention* e diritto alla riservatezza cfr. E. BASSOLI, *Acquisizione dei tabulati Vs. Privacy: la* data retention *al vaglio della Consulta*, in *Riv. dell*'internet, 2007, p. 237; A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni,* in *Riv. it. dir. e proc. pen*., 2005, p. 594.

[164] L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali,* Milano, Giuffrè, 2007, p. 178; A. GHIRARDINI,G. FAGGIOLI, Computer forensic, Milano, Apogeo, 2009, p. 347 e ss.

In questa prospettiva, giova soffermarsi sulla normativa interna concernente la *data retention*, che è stata interessata da plurime riforme nel volgere di pochi anni[165]. La disciplina sulla conservazione dei dati esteriori di traffico è stata introdotta nel nostro ordinamento giuridico con il d. lgs. 196/2003 (cd. Codice in materia di protezione dei dati personali o della *Privacy*), in seguito all'adozione della Direttiva 2002/58/CE[166], relativa al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico in quanto immessi su reti di pubblica comunicazione[167]. Particolarmente importante è l'art. 132 del

[165] A. STRACUZZI, Data retention: *il faticoso percorso dell'art. 132 Codice* privacy *nella disciplina della conservazione dei dati digitali*, in *Dir. inf.*, 2008, p. 585.

[166] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, in *GUUE*, L 201, 31 luglio 2002. Tale normativa pone a carico degli Stati membri l'obbligo di proteggere la riservatezza delle comunicazioni elettroniche e, a tale scopo, vieta di custodire i dati relativi al traffico delle comunicazioni, se non per la salvaguardia di interessi pubblici quali la sicurezza, la difesa nazionale o la prevenzione e l'accertamento dei reati (art. 15). Gli Stati membri hanno dovuto, dunque, introdurre normative relative alla conservazione, determinata nel tempo e solo per finalità di protezione della sicurezza pubblica, dei dati relativi a mittente, destinatario, ora e durata della comunicazione telefonica, di un SMS, di una e-mail e di un fax. Diversamente, tali informazioni, quando non siano più necessarie per la trasmissione della comunicazione, dovranno essere cancellate o rese anonime dal fornitore della rete pubblica o del servizio pubblico di comunicazione elettronica. S. VIGLIAR, *Privacy e comunicazioni elettroniche: la direttiva 2002/58/CE*, in *Dir. inf.*, 2003, p. 402.

[167] Anteriormente alla direttiva 2002/58/CE, per acquisire i dati di traffico telefonico e telematico presso gli *internet providers*, il p.m. doveva semplicemente emettere un decreto motivato ex art 256 c.p.p., laddove queste informazioni fossero conservate ai fini della fatturazione o della commercializzazione del servizio (art. 4 d.lgs. 13 maggio 1998 n. 171). In punto di conservazione, infatti, il decreto citato stabiliva che i dati personali relativi al traffico telefonico venissero cancellati o resi anonimi, tranne che servissero alla fatturazione o alla commercializzazione del servizio. Dunque prima della direttiva in discorso, nulla era previsto a livello legislativo relativamente alla conservazione dei dati di traffico telematico, mentre per quelli relativi al traffico telefonico, non era stabilito nessun obbligo o limite, laddove essi fossero stati utili all'attività investigativa. Dato il vuoto legislativo materia, la Corte di cassazione a sezioni unite aveva affermato che, ai fini dell'acquisizione dei tabulati telefonici contenenti i dati esterni identificativi delle comunicazioni telefoniche conservati in archivi informatici presso il gestore del servizio, era sufficiente il decreto motivato dell'autorità giudiziaria, non essendo necessaria, per il diverso livello di intrusione nella

succitato decreto, che disciplina l'obbligo di conservazione dei dati di traffico telefonico e telematico a carico dei fornitori di servizi di comunicazione elettronica. Questa disposizione è stata interessata da molteplici riforme [168], tra le quali rileva in particolar modo il d.l. 27 luglio 2005, n. 144 (c.d. "decreto Pisanu" recante misure urgenti per il contrato al terrorismo internazionale), convertito con modificazioni dalla l. 31 luglio 2005, n. 155. Esso ha avuto il merito di colmare il vuoto legislativo presente nel testo dell'art. 132 comma 1, inserendovi l'obbligo di conservare i dati relativi al traffico telematico -con esclusione dei

---

sfera della riservatezza che ne deriva, l'osservanza delle disposizioni dettate in materia di intercettazioni di comunicazioni o conversazioni (artt. 266 c.p.p. e ss.). Cass, sez, un., 23 febbraio 2000, in *Cass. pen*., 2000, p. 2959 con nota di G. MELILLO, *Intercettazione ed acquisizione dei tabulati telefonici: un opportuno intervento correttivo delle Sezioni Unite.* In senso opposto cfr. Cass, sez. un., 13 luglio 1998, Gallieri, *ivi* , 1999, p. 465 con nota di ID, *L'acquisizione dei tabulati relativi al traffico telefonico tra limiti normativi ed equivoci giurisprudenziali*. Per una ricostruzione del dibattito dottrinale e giurisprudenziale sul punto F. DE LEO, *Controllo delle comunicazioni e riservatezza, ivi,* 2002, p. 2208 e ss.

[168] Nella versione originaria, l'art. 132 si componeva di un unico comma che obbligava il fornitore a conservare i dati relativi al traffico telefonico (c.d. tabulati telefonici) per un periodo di trenta mesi a fini d'accertamento e repressione di reati. Simile obbligo, invece, non era prescritto ai fornitori di servizi di comunicazione elettronica. A distanza di pochi mesi dall'entrata in vigore, la norma veniva riformata dal d.l. 24 dicembre 2003, n. 354 (convertito con modificazioni in l. 26 febbraio 2004, n. 45) che prescriveva la conservazione dei dati di traffico telefonico per un periodo di ventiquattro mesi prorogabile (per altri ventiquattro) esclusivamente per scopi di accertamento e repressione dei delitti più gravi (ex art. 407 comma 2 lett. a) c.p.p.). Nell'ottica di proteggere la riservatezza della persona, inoltre, la legge escludeva il potere autonomo del p.m. di disporre l'acquisizione dei dati prevedendo il necessario controllo del gip sull'istanza dell'organo inquirente. La legge di conversione attribuiva, inoltre, al difensore dell'indagato/imputato il potere di acquisire direttamente, senza filtro del giudice, i dati *de quibus* laddove vi fosse un effettivo pregiudizio per le indagini difensive.

Tale novella, però, non estendeva l'obbligo di conservazione anche ai dati relativi al traffico telematico, la cui acquisizione e custodia continuavano a non avere una disciplina espressa, nonostante le critiche sollevate da parte della dottrina. Cfr. G. BRAGHÒ, *Le indagini informatiche tra esigenze di accertamento e garanzie di difesa*, in *Dir. inf. e informatica*, 2005, 524 ss.

contenuti-[169] e le chiamate senza risposta[170] nonché prevedendo la possibilità di prorogare i tempi di conservazione limitatamente alle fattispecie incriminatrici di maggiore gravità, indicate all'art. 407, comma 2, latt. a) c.p.p., e ai delitti commessi in danno ai sistemi informatici[171].

Successivamente, in materia sono intervenute la legge 48/2008; il decreto legislativo 30 maggio 2008, n. 109, attuativo della direttiva 2006/24/CE (cd. Direttiva *data retention* o Frattini) relativa alla conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione; nonché il d.l. 151/2008 convertito con l. 86/2008[172].

---

[169] Il legislatore con l'espressione traffico telematico intende riferirsi ai movimenti effettuati nella rete *internet* dal singolo utente, sebbene la telematica possa avere applicazioni diverse. Crf. L. A. D'ANGELO, *La conservazione dei dati del traffico telefonico e telematico tra esigenze investigative e tutela della* privacy, in A. A. DALIA (a cura di), *Le nuove norme di contrasto al terrorismo*, Giuffré, Milano, 2006,, p. 121 e ss.

[170] Si tratta delle comunicazioni telefoniche non andate a buon fine per mancata connessione con l'apparecchio ricevente.

[171] L'articolo 132 del D.Lgs 196/03 rubricato conservazione di dati di traffico per altre finalità, nel testo vigente all'esito delle modifiche apportate dalla legge 155/05 stabiliva che «1. ... i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, sono conservati dal fornitore per 24 mesi, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per 6 mesi. 2. Decorso il termine di cui al comma 1, i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, sono conservati dal fornitore per ulteriori 24 mesi e quelli relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati per ulteriori 6 mesi per esclusive finalità di accertamento e repressione dei delitti di cui all'articolo 407, secondo comma, lett. a), Cpp, nonché dei delitti in danno di sistemi informatici». Sulle novità in tema di *data retention* introdotte l. n. 155/2005 v. T. RAFARACI, *Intercettazioni e acquisizione di tabulati telefonici*, in R. E. KOSTORIS, R. ORLANDI (a cura di), *Contrasto al terrorismo interno e internazionale*, Giappichelli, Torino, 2006, p. 265 e ss.

[172] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006, in *GUUE, L 105*, 13 aprile 2006.Tale direttiva ha modificato la precedente direttiva 2002/58/CE relativa alla riservatezza e alle comunicazioni elettroniche, con cui si era data applicazione alla direttiva 1995/46/CE.

Al fine di comprendere i punti di contrasto tra la disciplina sulla conservazione dei dati telematici e la tutela del diritto alla *privacy* bisogna, *in primis*, chiarire l'oggetto dell'obbligo di conservazione e individuare i soggetti tenuti a rispettarlo, accertando, in specie, se l'identificazione dei siti visitati durante la navigazione, a prescindere da ogni richiamo al contenuto delle pagine *web* visitate, rappresenti o meno un dato esteriore di traffico.

Il codice sulla protezione dei dati personali non fornisce alcuna indicazione utile in tal senso. Il decreto si limita a imporre al fornitore la conservazione dei dati relativi al traffico telematico con l'esclusione del contenuto della comunicazione (art. 132 comma 1), definendo genicamente tali dati come «qualsiasi informazione sottoposta a trattamento per la trasmissione di una comunicazione su una rete di comunicazione elettronica» o per la «relativa fatturazione» (art. 4 comma 2 lett. h)).

Queste disposizioni, purtroppo, non affrontano l'aspetto maggiormente discusso in tema di conservazione dei dati relativi al traffico telematico, ossia il fatto che essi consentano potenzialmente di tracciare gli accessi *internet* (i dati I.P. di destinazione, *id est* dei *servers* consultati, da cui è desumibile l'indirizzo *internet* almeno delle *homepage* visualizzate) [173] e i servizi utilizzati dall'utente (es. posta elettronica o *chat*).

Secondo parte della dottrina, custodendo tali informazioni, infatti, si ottiene una "mappatura" dei movimenti effettuati in rete da ciascun abbonato, idonea a ricostruire gusti, abitudini, preferenze di ogni tipo e, in definitiva, a rivelare anche notizie estranee alla commissione di illeciti

[173] Facendo un parallelismo con le comunicazioni telefoniche, esso equivarrebbe al numero di telefono chiamato.

penali e, come tali, vulneranti la tutela della riservatezza individuale[174]. Di conseguenza, gli indirizzi I.P. *destination* non dovrebbero essere custoditi[175].

Nell'intento di chiarire la portata delle disposizioni del Codice della *privacy* e di salvaguardare la riservatezza individuale, il 17 gennaio 2007, il Garante per la protezione dei dati personali ha emesso un provvedimento sulla sicurezza dei dati di traffico telefonico e telematico, in cui ha introdotto alcune indicazioni contenute nella Direttiva 24/2006/CE prima che la stessa fosse recepita nell'ordinamento interno. In esso, l'Autorità ha imposto ai fornitori di servizi di comunicazione elettronica la distruzione di una grande quantità di dati inerenti al traffico *on-line*, ritenuta in grado di documentare il contenuto della navigazione del singolo utilizzatore della connessione. Infatti, dopo aver circoscritto l'ambito soggettivo di applicazione della normativa ai soli fornitori, vale a dire ai soggetti che realizzano esclusivamente o prevalentemente una trasmissione di segnali su reti di comunicazioni elettroniche - a prescindere dalla proprietà delle stesse - offrendo indiscriminatamente servizi a utenti finali (*Internet Service Provider* o ISP), il Garante si è preoccupato di circoscriverne l'ambito oggettivo. In particolare, gli ISP sono tenuti a custodire, in distinti archivi, le informazioni che usano per la fatturazione e quelle di cui

[174] Senza, peraltro, considerare che la forma digitale di simili dati, che consentono un agile trasferimento, costituisce un pericolo ulteriore per la privacy, facilitando le divulgazioni indebite non finalizzate alla repressione dei crimini (ad es. per scopi commerciali e pubblicitari).
[175] M. VIGGIANO, I *dati personali nelle ricerche su* internet, in *Dir. inf. e informatica.*, 2007, p. 379.

dispongono per la trasmissione delle comunicazioni, cancellando gli IP di destinazione e le pagine *web* (o URL [176]) visitate[177].

In questo quadro, così, il provvedimento non impone alcun dovere di conservazione in capo, ad esempio, ai gestori dei motori di ricerca e dei contenuti dei siti *web* in *internet* (cd. *continet provider*)[178], ai gestori di esercizi pubblici come gli *internet point* e agli *internet café* oppure alle organizzazioni sia pubbliche sia private che dotino il proprio personale di postazioni connesse a reti informatiche e telefoniche non accessibili al pubblico[179].

Su tale scia si pone anche il d. lgs. 109/2008 che, nel recepire la direttiva 2006/24/CE, specifica il concetto di traffico telematico, comprendendovi le informazioni necessarie per identificare l'abbonato o l'utente, ossia gli indirizzi IP (art. 1), ed elenca dettagliatamente le categorie di dati da conservare per l'accertamento e la repressione dei reati ex art. 132 comma 1, non includendovi gli IP *destination* o i siti *web* visitati durante la navigazione (art. 3).

Pertanto, dalla lettura combinata delle norme del d. lgs 196/2003, del d.lgs. 109/2008 e delle prescrizioni emanate dal Garante della *privacy* si

---

[176] Acronimo di *Uniform Resource Locator* che indica una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in *Internet* (es. un documento o un'immagine), permettendo di trovarla: si tratta del nome del sito (es. www.nomesito.it)

[177] In tal senso si esprime anche il decreto Pisanu all'art. 6, in cui parla di informazioni che consentono la tracciabilità degli accessi nonché, qualora disponibili, dei servizi.

[178] Essi, in particolare, devono conservare esclusivamente i dati di traffico telematico funzionali alla fornitura e alla fatturazione del servizio di connessione e non i dati di traffico apparentemente "esterni" alla comunicazione (es. pagine web visitate o indirizzi IP di destinazione), poiché essi possono coincidere di fatto con il "contenuto" della comunicazione, consentendo di ricostruire relazioni personali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute(art. 3). Garante della *privacy, Relazione 2007, Garanzia e sicurezza dei dati: l'attività dell'Autorità,* in *www. garanteprivacy.it*

[179] Le eccezioni al divieto sono espressamente individuate all'art. 3 del provvedimento. Garante della *privacy, Relazione 2007, Garanzia e sicurezza dei dati,* cit.

deve concludere che l'IP di destinazione e i siti visionati sono, di fatto, esclusi dagli obblighi di conservazione, così da dover essere immediatamente cancellati.

Il fatto di limitare tali obblighi di conservazione ai soli IP di accesso, però, potrebbe costituire un grave limite nello svolgimento delle investigazioni digitali di polizia, determinando in molti casi l'impossibilità di identificare l'utente, e questo potrebbe finanche compromettere lo stesso diritto di difesa dall'indagato, che voglia dimostrare la propria innocenza in base a prove informatiche (ad es. costruendosi un cd. alibi informatico)[180], o della persona offesa, che voglia fornire una prova informatica a riscontro di quanto esposto in denuncia[181].

A ben vedere, però, i dati telematici detenuti dagli *internet providers*, ossia dai fornitori *ex* art. 132 comma 1 d.lgs. 196/2003, sono costituiti da informazioni per lo più relative alle registrazioni degli accessi (c.d. *files* di *log* degli indirizzi IP) e, come tali, assimilabili a quelle di telefonia, in quanto individuano il dispositivo elettronico (di norma un *computer*) che si è connesso alla rete e indicano l'associazione tra indirizzo IP assegnato all'utente e numero telefonico chiamato. Non dovrebbero, quindi, sussistere in linea di principio gravi violazioni della *privacy* individuale nella acquisizione di tali dati, anche se comprensivi di IP di destinazione[182].

---

[180] 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. 520.

[181] Autorevole dottrina, sotto questo profilo, osserva che la disciplina della *data retention* pare oggi far prevalere le necessità legate alla tutela della riservatezza più che al progredire delle indagini penali S. ATERNO, A. CISTERNA, *Il legislatore interviene ancora sulla* data retention, *ma non è finita*., in *Dir. pen e proc*., 2009, p. 279

[182] L'i*mpasse*, peraltro, sarebbe superabile se fosse stato concretamente attuato il disposto dell'art. 6 comma 5 d. lgs. 109/2008, che prescrive ai fornitori di servizi di comunicazione elettronica accessibili al pubblico i quali offrono servizi di accesso a internet (IAP) di garantire la disponibilità e l'effettiva univocità degli indirizzi di

Per quanto concerne, infine, i termini di conservazione del traffico telematico l'art. 132 d. lgs. 196/2003 ne prevede una archiviazione temporanea finalizzata in via esclusiva all'accertamento e alla repressione dei reati.

Inizialmente, il decreto Pisanu ha introdotto diversi termini di conservazione in base al tipo di dato archiviato (telefonico, telematico o chiamata senza risposta)[183], stabilendone l'acquisizione con decreto motivato del p.m.[184]. Le leggi di riforma adottate nel 2008, poi, hanno

---

protocollo internet. La normativa avrebbe dovuto essere attuata entro novanta giorni dall'entrata in vigore del decreto.
Infatti, esistono delle tipologie di reti che non attribuiscono un IP univoco a ciascun utente, ma attribuiscono un IP di rete pubblica a una serie indetermina di utenti titolari di un proprio indirizzo IP privato. In tal modo, al privato che richieda il servizio o la connessione al Provider viene attribuito un nuovo IP, che tuttavia è condiviso con altri utenti e con il quale verranno effettuate le operazioni sul *web*. L'individuazione del singolo utente, in simili condizioni, è possibile solo disponendo di tutto il traffico trattato dal fornitore, ossia dei *files* di *log* contenenti anche l'IP *destination*. Cfr. F. CAJANI, S. ATERNO, *La disciplina in tema di conservazione dei dati* (data retention), in S. ATERNO, F. CAJANI, G. COSTABILE, M. MATTEUCCI, G. MAZZARACO, Computer forensics *e indagini digitali*, Forlì, Experta, 2011, p. 249 e ss.

[183] Nello specifico, il periodo massimo di conservazione per i tabulati telefonici è pari a ventiquattro mesi prorogabile un'unica volta per altri ventiquattro, quello per i "tabulati telematici è di sei mesi prorogabile di ulteriori sei e, infine, il temine massimo di archiviazione dei dati relativi alle chiamate senza risposta è pari a trenta giorni. La proroga era possibile solamente laddove si procedesse per delitti di cui all'articolo 407, comma 2, lett. a), cpp.

[184] Invero, l'art 132 costituisce un'eccezione rispetto al generale divieto di custodire i dati relativi al traffico prevedendone una conservazione temporanea finalizzata in via esclusiva all'accertamento e alla repressione dei reati. Tuttavia, il decreto Pisanu, comprimendo il diritto alla riservatezza individuale sospende l'applicazione di ogni disposizione che preveda o permetta la cancellazione di dati di traffico telefonico o telematico da parte degli *internet providers* fino al 31 dicembre 2007; questa previsione è stata più volte prorogata fino al dicembre 2010 [Cfr. A.RODOLFI, *Il regime normativo della* data retention *nell'ordinamento italiano,* in *Ciberspazio e dir.*, 2010, p. 151]. La conservazione presso società private di moltissime informazioni sufficienti a tracciare il profilo di un utente telefonico o del singolo accesso alla rete *internet* ha suscitato diversi interventi del Garante della *privacy*, diretti a denunciare l'eccessiva compressione del diritto alla riservatezza individuale a favore delle ragioni di sicurezza pubblica. Garante della *privacy*, *Sicurezza dei dati di traffico telefonico e telematico*, 17 gennaio 2008, in *G.U.*, 5 febbraio 2008, n. 30.

riproposto sia la possibilità di acquisire le informazioni relative al traffico tramite decreto dell'organo inquirente sia la differenziazione dei periodi di conservazione in base al tipo di informazione conservata a prescindere dalla gravità del reato perseguito. Sicché, attualmente, si ha un termine massimo pari a ventiquattro mesi per il traffico telefonico, a dodici mesi per quello telematico e a trenta giorni per i dati relativi alle chiamate senza risposta. Simile distinzione temporale, che prevede un periodo di archiviazione più limitato per i dati di traffico telematico non è, invero, richiesta dalla direttiva comunitaria 2006/24/CE e non sembra trovare la sua ragion d'essere nella necessità di tutelare maggiormente la vita privata individuale con riferimento all'uso di tali dati. Infatti, come i dati relativi al traffico telefonico, i dati concernenti il traffico telematico archiviati si limitano, per espressa previsione normativa, ai soli contenuti esterni della comunicazione (art. 132, comma 1, d.lgs. 196/2003)[185]. Sotto questo profilo, allora, sarebbe stato preferibile introdurre dei termini di conservazione omogenei sia per i dati telefonici che per quelli telematici, prevedendo semmai tempi di archiviazione più lunghi[186] per i reati di maggiore gravità[187].

---

[185] Il problema limiti oggettivi e soggettivi dell'obbligo di conservazione dei dati telematici è stato affrontato nella parte antecedente del paragrafo.

[186] L'art. 6 della Direttiva 2006/24/CE ammette che il termine per la conservazione dei dati esterni di comunicazioni telefoniche e telematiche potesse essere stabilito fino a un massimo di 24 mesi.

[187] Come, peraltro, già era stato previsto dalla previgente 155/2005 cfr. nota 166. Invero, la disciplina di conservazione dei dati attualmente appare sbilanciata a tutela della *privacy*, ma questa protezione non è presidiata sul piano sanzionatorio dall'inutilizzabilità poiché non vi è alcuna norma processuale che vieti espressamente di acquisire i dati conservati oltre i termini fissati dalla legge. Nemmeno l'art. 11 comma 2 d.lgs. 196/2003 può soccorre in tal senso, poiché esso, nel comminare l'inutilizzabilità dei dati assunti in «violazione della disciplina rilevante in materia di trattamento dei dati personali» non opera un riferimento alle regole di ammissione probatoria. In tal senso M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc*., 2011, p. 283 e s.; *contra* C. CONTI, *L'attuazione della direttiva Frattini: un bilanciamento*

Le modalità di conservazione dei dati in discorso presso i soggetti privati sono regolamentate dalla disposizioni adottate dal Garante della *Privacy*, che ha il compito di individuare le misure adeguate a garantire i diritti individuali (es. sistemi di cifratura)[188] e di controllarne l'applicazione[189]. Tali presidi a garanzia della riservatezza avrebbero dovuto essere adottati dagli *internt providers* entro il 30 giugno 2009, ma gli elevati costi dell'operazione hanno reso difficoltoso, nei fatti, il rispetto della normativa, nonostante l'obbligatorietà della disciplina e le pesanti sanzioni comminate in caso di inadempimento[190]. Pertanto, sotto questo profilo, la protezione dei dati personali e la loro stessa genuinità risultano essere esposte a un concreto pericolo di lesione. Inoltre, emerge un ulteriore aspetto di criticità in relazione alla procedura di cancellazione o di riduzione ad anonimato dei dati, una volta trascorso il termine massimo di conservazione degli stessi: manca, infatti, la previsione di una procedura standardizzata che provi, ad

---

insoddisfacente tra riservatezza e diritto alla prova, in S. LORUSSO (a cura di), *Le nuove norme sulla sicurezza pubblica*, Cedam, Padova, 2008, p. 3 e s.

[188] L'art.132 comma 5 d. lgs. 196/2003, infatti, dispone che «Il trattamento dei dati per le finalità di cui ai commi 1 e 2 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'art.17, volti a garantire che i dati conservati possiedano i medesimi requisiti di qualità, sicurezza e protezione dei dati in reta nonché a: a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato; [b) e c) lettere abrogate *ex* d.lgs. 109/2008] d) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui ai commi 1 e 2.», mentre l'art. 17 stabilisce che sia il Garante della *Privacy* a prescrivere le misure di sicurezza e le modalità di trattamento dei dati che «presenta(no) rischi specifici per i diritti e le libertà fondamentali».

[189] Garante per la protezione dei dati personali, *Provvedimento 24 luglio 2008, Modifica al provvedimento del 17 gennaio 2008 sulla conservazione dei dati di traffico - Misure e accorgimenti a tutela dell'interessato in attuazione dell'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, recante: «Codice in materia di protezione dei dati personali»*, in G.U., 13 Agosto 2008, n. 189.

[190] F. CAJANI, S. ATERNO, *La disciplina in tema di conservazione dei dati* (data retention), in S. ATERNO, F. CAJANI, G. COSTABILE, M. MATTEUCCI, G. MAZZARACO, Computer forensics, cit.

esempio con verbali, l'effettivo e corretto svolgimento delle operazioni necessarie.

Molto più invasiva del diritto alla riservatezza personale rispetto a quanto sinora esposto pare essere, invece, l'ipotesi speciale di conservazione dei dati telematici a seguito di attività di investigazione preventiva penale, introdotta all'art. 132, comma 4-*ter* d. lgs. 196/2003 dalla legge 48/2008 (cd. "congelamento dei dati telematici)[191]. Si tratta di un'attività di carattere eccezionale ed urgente rimessa all'iniziativa della polizia giudiziaria, che può essere svolta preventivamente e, quindi, anche in assenza di una *notitia criminis*, finalizzata alla conservazione e protezione di dati relativi al traffico telematico per un periodo non superiore a novanta giorni, prorogabile fino a sei mesi[192].

Questa attività di "congelamento" (cd. *freezing*) di dati telematici si differenzia dall'ipotesi di conservazione dati disciplinata al primo comma, in quanto è rivolta, oltre che ai fornitori di rete, a 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*) ed i gestori dei motori di ricerca. I dati di traffico telematico trattati da queste ultime due categorie di soggetti, in particolare, sono equiparabili al

[191] L'art. 132 comma 4 ter Codice della *privacy* disciplina una ipotesi speciale di investigazione preventiva avente ad oggetto «i dati relativi al traffico telematico» ed 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 ed 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».

[192] In tal caso, mancherà anche un pubblico ministero titolare delle indagini con l'inevitabile rischio che il p.m. compente, ossia l'organo inquirente del luogo di esecuzione del congelamento dei dati o del luogo dove i dati sono conservati, aderisca in modo quasi acritico alle richieste delle forze di polizia procedenti. In tal senso, C. FATTA, *La tutela della* privacy *alla prova dell'obbligo di data retention e delle misure antiterrorismo,* in *Dir. dell'inf. e dell'inform.*, 2008, p. 395 e ss.

contenuto della comunicazione perché consentono di ripercorrere facilmente tutte le operazioni compiute dall'utente *on line* anche all'interno del singolo sito. Tali informazioni, quindi, non possono essere considerate meri "dati esterni", poiché essi riguardano precisamente il servizi forniti dai *provider* e spesso consentono di risalire all'oggetto della comunicazione [193].

Il c.d. "congelamento" dei dati telematici previsto all'art. 132 comma 4*ter* è finalizzato espressamente allo svolgimento delle indagini pre procedimentali[194] con conseguente inutilizzabilità nel procedimento penale vero e proprio *ex* art. 226 comma 5 disp. att. c.p.p.[195].

Tuttavia, detta attività pare improntata ad una genericità eccessiva in riferimento ai reati da prevenire, in quanto è ammessa anche «per finalità di accertamento e repressione di specifici reati». Questa formula aperta consente alla polizia giudiziaria di ricorrere allo strumento *de quo* per qualunque tipo di reato, anche laddove le finalità di giustizia non giustifichino la compressione del diritto alla riservatezza[196]. Sarebbe

---

[193] F. CERQUA, *Conservazione dei dati digitali e tutela della privacy*, in L. MARAFIOTI, L. LUPARIA, *Sistema penale*, cit., p. 236.

[194] Esso si differenzia nettamente dall'istituto della conservazione di dati previsto all'art. 132 comma 1 d. lgs 196/2003, il quale è indirizzato all'acquisizione degli stessi e al conseguente loro utilizzo processuale.

[195] Essa è, come detto, un'attività eccezionale ed urgente esperibile anche in assenza di una *notitia criminis* e rimessa al potere discrezionale delle forze di polizia e dei servizi segreti. Il successivo comma 4 *quinquies* stabilisce che i provvedimenti adottati a norma del comma 4 *ter* sono comunicati per iscritto, senza ritardo o comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione, quest'ultimo, se ne ricorrono i presupposti, li convalida.

[196] L'art. 226 comma 1 norme att. c.p.p. subordina l'esecuzione delle intercettazioni preventive alla necessità di acquisire «notizie concernenti la prevenzione dei delitti di cui all'art. 407 comma 2, lett. a), n. 4 e 51 comma 3 bis c.p.p.».
Se, inoltre, si pongono a confronto le due disposizione in esame si ricava come l'art. 132 comma *4ter* d. lgs. 196/2003 risulti, rispetto all'art. 226 comma 1 norme att. c.p.p, generico per tre ragioni. In primo luogo, esso non definisce i presupposti in base ai quali il p.m. può emettere il decreto di convalida. In secondo luogo, inoltre, tale disposizione non prescrive in capo alla polizia l'obbligo di motivare l'eventuale richiesta di proroga dell'attività di *freezing*. In terzo luogo, infine, la norma *de qua* non

preferibile, in un'ottica di maggiore rispetto delle riservatezza individuale, stabilire più rigorose condizioni di ammissibilità per lo svolgimento di tale attività d'indagine[197].

3. Segue: comunicazioni VOIP.

La disciplina relativa alla *data retention* deve essere esaminata anche alla luce del dibattito, sorto in dottrina, sulla possibilità di estendere la procedura prevista dalla legge per l'acquisizione e conservazione dei tabulati telefonici ai dati digitali concernenti le comunicazioni VOIP.

Le comunicazioni *Voice over* IP (Voce tramite protocollo *internet*) sono una tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione internet o un'altra rete dedicata che utilizza il protocollo IP, anziché passare attraverso la rete telefonica tradizionale. In concreto, tale sistema provvede a trasmettere sulla rete dati contenenti le informazioni vocali, codificati in forma digitale, quando uno degli utenti collegati sta parlando.[198]

---

stabilisce quale condizione di ammissibilità di tale attività investigativa preventiva il requisito della sua necessità. In questo senso anche cfr. E. FORLANI, *La conservazione preventiva dei dati informatici per l'accertamento dei reati*, in *Dir. dell'internet*, 2008, p. 520 e ss.

[197] Forse un utilizzo possibile dell'istituto in esame si abbia in occasione di rogatorie; in tale ipotesi l'ordine di conservazione avrà lo scopo di "congelare" i dati informatici, altamente volatili, in attesa dei tempi tecnici delle rogatorie. F. CAJANI, S. ATERNO, *La disciplina in tema di conservazione dei dati* (data retention), in S. ATERNO, F. CAJANI, G. COSTABILE, M. MATTEUCCI, G. MAZZARACO, Computer forensics, cit., p. 249.

[198] Il presente studio, limitandosi ad analizzare le prove digitali cd. statiche, non cerca di rispondere al quesito giuridico se tale forma di comunicazione ricada sotto la disciplina relativa all'intercettazione di conversazioni telefoniche oppure sotto quella dettata in materia telematica dall'art. 266-*bis* c.p.p. La soluzione del problema è

Negli ultimi anni, la disponibilità di connessioni *web* e la particolare semplicità di utilizzo del più noto e diffuso modello di comunicazione telefonica telefonia via *internet, Skype,* hanno determinato la diffusione massiva del VoIP sia in ambito professionale che privato[199].

Il d.lgs. 109 /2008 chiarisce, per la prima volta, la nozione di traffico telefonico, stabilendo che questo consiste nelle «chiamate telefoniche, incluse le chiamate vocali, di messaggeria vocale, in conferenza e quelle basate sulla trasmissione dati, purché fornite da un gestore di telefonia, i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata, la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve, servizi mediali avanzati e servizi multimediali».

Tale definizione, risolvendo numerosi dubbi interpretativi, comprende nel traffico telefonico le "chiamate" effettuate in base alla trasmissione di dati informatici e telematici, così includendovi quelle effettuate con sistemi di VOIP (chiamate effettuate tramite i servizi di telefonia vocale basati sul protocollo *internet* o con piattaforma *Skype*)[200]. In tal modo, si esclude definitivamente la lesione del diritto alla riservatezza personale in occasione dell'acquisizione delle informazioni esteriori relative a tale

---

complessa e non si esaurisce in una mera disputa dottrinale, perché l'ambito di applicazione della seconda norma è decisamente più vasto rispetto a quello della prima, considerato il rinvio che l'art. 266-bis c.p.p. fa a qualsiasi reato commesso mediante l'impiego di tecnologie informatiche o telematiche, oltre che alle fattispecie direttamente richiamate dalla normativa in tema di intercettazioni telefoniche.

[199] Sui profili tecnici connessi alla protezione e criptatura delle comunicazioni VOIP cfr. A. MAURO, G. GARGIULO, *VOIP security*, in *Ciberspazio e diritto*, 2010, p. 161 e ss.

[200] S. MARIOTTI, S. TACCONI, *Riflessioni sulle problematiche investigative e di sicurezza connesse alla comunicazione* VoIP, in *Dir. Internet*, 2008, p. 558; C. PARODI, VoIP, Skype *e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?, ibidem*, p. 1309.
Analogo discorso può essere svolto per la conservazione degli sms (*short message system)* che vengono considerati traffico telefonico.

tipologia di comunicazioni telefoniche, che sfruttano le tecnologia informatica e telematica.

4. La salvaguardia della *privacy* nelle ispezioni e nelle perquisizioni informatiche.

Per comprendere il rapporto tra la tutela della *privacy* e l'ispezione e la perquisizione in ambito informatico e telematico, è utile svolgere una sintetica premessa di carattere generale.

Le prove digitali, presentandosi quali entità immateriali, hanno una fisicità non percepibile in modo separato dal supporto che le incorpora. Infatti, gli elementi di prova ricavabili da un sistema informatico o telematico sono costituiti dagli impulsi elettrici memorizzati su un supporto (cd. *bits*)[201], nei quali sono state convertite sulla base di un sistema binario le informazioni (suono, immagine, numero o parola)[202]. Per questo motivo, in passato, le prove digitali venivano confuse con i loro "contenitori" (es. cd, dvd, *hard disk* interno ed esterni, *pen drive)*[203]. Di conseguenza,

[201] Il termine *bit* significa *binary digit* ed esprime, secondo una logica binaria, l'alternativa tra 0 e 1 come minima unità di informazione logicamente possibile: si tratta di una scelta tra acceso/spento, sì e no. Otto *bit* -cioè unità di informazione elementare- compongono il *byte*, che è la minima unità di informazione gestibile dal *computer*. S. ATERNO, *Acquisizione e analisi della prova informatica*, cit., p. 61.

[202] E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica,* in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, cit., Giuffré, Milano, 2009, p. 37; G. PICA, *Diritto penale delle tecnologie informatiche*, Utet, Torino, 2000, p. 83. Per un approfondimento cfr. R. BORUSSO, S. RUSSO, C. TIBERI, *L'informatica per il giurista. Dal* bit *a* internet, Giuffré, Milano, 2009, p. 37.

[203] La confusione concettuale in parola è stata facilitata dalla concezione di documento informatico introdotta dalla l. 547/1993, che all'art. 491*bis* c.p. lo definiva come «qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli» e, quindi, in via di sintesi, lo indentificava con il supporto dei dati digitali. Il legislatore, successivamente,

anteriormente alla legge 48/2008, dinanzi al vuoto normativo, l'autorità giudiziaria per eseguire le attività investigative informatiche ricorreva, tramite interpretazione analogica od estensiva, alle regole stabilite nel codice di rito per ispezioni, perquisizioni e sequestri[204], sebbene dette norme fossero state formulate avendo come punto di riferimento la realtà fisica e non quella "virtuale"[205].

Nella pratica, quindi, gli organi inquirenti spesso procedevano a duplicare l'intero contenuto del sistema informatico - *computer* o altro tipo di supporto - così acquisendo anche grandi quantità di informazioni assolutamente non pertinenti o non rilevanti per accertare i reati oggetto di

---

ha disciplinato nuovamente la materia nel codice dell'amministrazione digitale (art. 1 comma 1 *lett. p)* d. lgs. 7 marzo 2005 n. 82), dove il documento informatico è stato individuato come la «rappresentazione informatica di atti, dati o fatti». Queste due diverse definizioni, tra loro contraddittorie, hanno convissuto nell'ordinamento fino a quando nel 2008 la l. n. 48 ha abrogato l'art. 491 *bis* c.p., lasciando in vigore la seconda definizione. L'art. 247 dimostra di aver abbracciato la distinzione tra supporto o unita di memorizzazione dei dati informatici e informazione digitale poiché l'art. 247 c.p.p., in particolare, opera una lunga elencazione degli oggetti su cui può esplicarsi la attività a sorpresa della perquisizione. M. DANILE, *La prova digitale nel processo penale*, cit., p. 283 e s.

[204] Cfr. parte II capitolo II par. 5.

[205] Prima della legge di ratifica della Convenzione di Budapest, la ricerca e l'acquisizione di un documento informatico o di un *computer* erano affrontate dagli organi inquirenti prevalentemente ricorrendo ai mezzo di ricerca della prova tipici dell'ispezione, della perquisizione o del sequestro, senza però adottare cautele in relazione all'oggetto particolare su cui si interveniva. Per cui, di frequente, accadeva, ad esempio, che fosse operato un sequestro *tuot court* del p.c. e delle relative periferiche senza alcuna precauzione a tutela della riservatezza e dell'enorme quantità di dati anche ultronei negli stessi contenuti. Tuttavia, le investigazioni informatiche, nel silenzio normativo, non erano concepite concettualmente secondo un disegno unitario, poiché vi erano anche alcuni che in proposito richiamavano il concetto di mezzo atipico di ricerca della prova ex art. 189 c.p.p.
La legge di riforma ha ricondotto nell'alveo dei mezzi tipici di ricerca della prova la perquisizione, l'ispezione ed il sequestro di qualsiasi documento informatico, sia esso contenuto in un *computer* o di un intero sistema informatico o telematico. In tal senso P. TONINI, *Documento informatico e giusto processo,* in *Dir. pen. proc*., 2009, p. 404.

indagine con una compressione eccessiva della riservatezza a favore dell'attività di investigazione penale[206].

In questo contesto, la legge n. 48 del 2008 non è intervenuta introducendo una disciplina organica, ma si è limitata a modificare, in base a due direttive, le vigenti norme processuali sui mezzi di ricerca della prova (accertamenti urgenti della polizia giudiziaria[207], ispezione, perquisizione, sequestro[208]), adattandole alle peculiarità delle indagini eseguite su sistemi informatici e telematici[209]. Da un lato, l'individuazione e acquisizione delle prove digitali devono avvenire impiegando misure tecniche idonee ad assicurare la genuinità del dato conservato ed impedire l'alterazione degli originali[210]. Dall'altro, la copia informatica deve essere realizzata su

[206] Tale prassi si verificava, per lo più, in occasione dei sequestri informataci concernenti dati memorizzati sui *computer*, in relazione ai quali si provvedeva a sequestrare l'intero elaboratore per duplicare *in toto* l'*hard disk ex* art. 258 c.p.p. (V. paragrafo successivo). Altre volte, invece, si procedeva indiscriminatamente a stampare su fogli cartacei l'intero contenuto di un sistema informatico. Secondo l'orientamento dominante in giurisprudenza, infatti, non costituiva sequestro probatorio l'acquisizione, mediante riproduzione su supporto cartaceo, dei dati informatizzati contenuti in un archivio informatico visionato nel corso di una ispezione legittimamente eseguita ai sensi dell'art. 244 c.p.p., sicché non si poneva nemmeno un problema di restituzione dei supporti cartacei stampati cfr. Cass., Sez. III, 26 gennaio 2000, n. 384 testo citato in F. CAJANI, S. ATERNO, *Perquisizione ed ispezione,* S. ATERNO, F CAJANI, M. MATTIUCCI, G. MAZARACCO, Computer forensic *e indagini digitali,* cit., p. 465.

[207] Il presente lavoro non affronterà il suddetto profilo.

[208] I sequestri saranno oggetto di trattazione nel successivo paragrafo.

[209] La recezione della Convenzione di Budapest è stata indispensabile al fine di predisporre regole specifiche volte a uniformare la disciplina della raccolta e dell'utilizzo nel processo penale degli elementi di prova digitali. In assenza di ciò avrebbe dovuto essere la giurisprudenza a supplire alla carenza normativa con il rischio di interpretazioni e giudicati difformi.

[210] La genuinità del dato originale e il dovere di impedire l'alterazione dell'originale sono garantite nelle ispezioni disposte dall'autorità giudiziaria (art. 244, comma 2 c.p.p.), nelle perquisizioni disposte dall'autorità giudiziaria (art. 247, comma 1 *bis* c.p.p.), nelle perquisizioni su iniziativa della polizia giudiziaria (art. 352, comma 1*bis* c.p.p.), nel sopralluogo di polizia giudiziaria (art. 354, comma 2, c.p.p.).

adeguati supporti, tramite tecniche capaci di assicurare la conformità del duplicato all'originale e la sua immodificabilità[211]. La novella, tuttavia, non ha esplicitato le procedure da seguire in simili operazioni allo scopo di consentire un aggiornamento rapido, e costante, delle tecniche utilizzate dagli esperti alle *best practices* internazionali[212].

La scelta effettuata dal legislatore di incidere sui singoli mezzi di ricerca della prova esistenti lascia irrisolti alcuni profili ritenuti critici per la tutela della vita privata individuale.

Innanzitutto, sebbene le ispezioni e perquisizioni informatiche presentino una grande potenzialità lesiva per la *privacy*, in ragione della possibilità di memorizzare grandi quantità di informazioni in spazi ridottissimi, la legge 48/2008 non ha introdotto alcun controllo da parte del giudice. Esse, analogamente ai mezzi di ricerca della prova tradizionali, possono essere disposte in base a un semplice decreto motivato del p.m. oppure dalla polizia giudiziaria, nei casi di flagranza del reato e di urgenza, salva successiva convalida del p.m.[213].

---

[211] Il dovere realizzare una copia idonea ad assicurare la conformità del dato assunto rispetto all'originale è posto esclusivamente nel sopralluogo su iniziativa della polizia giudiziaria (art. 354, comma 2 c.p.p.) e nel sequestro disposto dall'autorità giudiziaria con esclusivo riferimento ai dati informatici presso i fornitori di servizi (art. 254 *bis* c.p.p.). Nei due casi menzionati si aggiunge la precisazione che la copia deve essere fatta su di un supporto «adeguato».

[212] O. DOMINIONI, *La prova penale scientifica*, cit., p. 15 e ss.

[213] I motivi forniti dall'autorità per giustificare l'ingerenza nella sfera di riservatezza devono essere pertinenti e proporzionati allo scopo da perseguire, rilevando sia le modalità operative sia i presupposti giuridici. L'azione degli organi inquirenti, pertanto, deve essere idonea ad evitare abusi. In tale prospettiva, quanto più dettagliati sono la legge e il provvedimento che dispone l'ispezione o il sequestro, tanto più si riduce il rischio di condotte arbitrarie degli investigatori. F.CASSIBBA, *Le perquisizioni presso lo studio del difensore alla luce della Convenzione europea dei diritti dell'uomo*, in *Ind. pen*., 2008, p. 77. La Corte europea dei diritti dell'uomo, inoltre, offre alcune indicazioni specifiche per circoscrivere le possibilità di abusi da parte degli organi inquirenti nel corso di perquisizioni e sequestri di materiale informatici. Essa, in particolare, ha ravvisato la violazione dell'art. 8, comma 2, CEDU nonostante il mandato di

Inoltre, tali atti investigativi, essendo atti a sorpresa, garantiscono al difensore esclusivamente il diritto di assistere alle attività senza preavviso del loro compimento, pena la frustrazione delle finalità per cui il mezzo di ricerca della prova stesso è stato disposto[214]. La presenza del difensore, però, sebbene costituisca una mera facoltà[215], risulta utile al fine di proteggere la riservatezza dell'indagato, considerato che egli può far verbalizzare le proprie osservazioni sulla pertinenza del materiale ispezionato, perquisito[216] ed eventualmente copiato.[217]

---

perquisizione fosse fondato su un "ragionevole sospetto", a causa della sua eccessiva ampiezza. La mancanza di un'indicazione specifica delle cose e dei documenti o *files* da ricercare si è riflessa nel modo in cui è stata eseguita l'attività investigativa, rendendola sproporzionata a qualsiasi scopo legittimo perseguito: la polizia infatti ha rimosso l'intero *computer* del ricorrente, comprese le sue periferiche, così come tutti i *floppy disk* trovati nel suo ufficio. È vero - osserva la Corte - che successivamente il perito ha utilizzato parole chiave per selezionare i dati in essi contenuti, limitando l'intrusione; tuttavia, questo è accaduto soltanto dopo alcuni giorni che era stata eseguita la perquisizione locale e il sequestro dei supporti informatici: in tale lasso di tempo, né erano state predisposte garanzie per evitare che l'intero contenuto del disco fisso potesse essere ispezionato (o i *floppy disk* copiati), né il ricorrente aveva a disposizione alcun mezzo per contestare la legittimità del mandato o della sua esecuzione. Corte eur., Sez. Ilya Stefanov c. Bulgaria ,V, sent. 22 agosto 2008.

[214] Il diritto di assistenza all'attività svolta in sede di ispezione, perquisizione e sequestro è garantito da codice in base a una nullità di ordine intermedio ex art. 178 lett. c) e 180 c.p.p.. P. FELICIONI, *Le ispezioni e perquisizioni*, in G. UBERTIS, G.P. VOENA, *Trattato di procedura penale*, Giuffré, Milano, 2012, p. 90

[215] È valido, infatti, un atto a sorpresa – ispezione, perquisizione o sequestro che sia- svolto in assenza di un difensore ritualmente avvisato, ma non comparso. In tal senso Cass., sez. VI, 22 ottobre 2008, n. 13523, in *Ced*, n. 243826. La facoltà di presenziare allo svolgimento degli atti a sorpresa non si estende, tuttavia, fino sospendere l'attività investigativa in caso di irreperibilità del difensore. Cfr. Cass., sez. fer, 25 luglio 2006, n. 27372.

[216] Inoltre, questi potrebbe fornire indicazioni al consulente tecnico, qualora si proceda a estrarre le prove digitali contenute nel dispositivo elettronico attraverso accertamenti tecnici ripetibili ex art. 359 c.p.p., come generalmente accade. [Per una trattazione approfondita v. F. GIUNCHEDI, *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, Utet, Torino, 2009; R.E. KOSTORIS, *I consulenti tecnici nel processo penale*, Giuffré, Milano, 1993, p. 135 e ss; ID, *Consulente tecnico extraperitale e gratuito patrocinio*, in *Cass. pen.*, 1999, p. 2789.]. Difatti, la giurisprudenza assolutamente maggioritaria [Cass., Sez. I, 05 marzo 2009, n. 14511, in in *Cass. pen.*, 2010, p. 1522, con nota di. E. LORENZETTO, *Utilizzabilità dei dati*

Passando a una trattazione più analitica dei due istituti in esame, è possibile rilevare come l'ispezione sia l'attività investigativa meno invasiva sul piano della riservatezza (art. 244 c.p.p.). Essa consiste nella ricerca visiva delle tracce del reato[218] e può riguardare, per espressa previsione

---

informatici incorporati sul computer *in sequestro: dal contenitore al contenuto passando* per la copia e in *Dir. pen. e proc*., 2009, p. 337 con nota di A.E. RICCI, digital evidence *e irripetibilità delle operazioni acquisitive.* Conforme tra le molte: Cass, sez. un., 25 febbraio 2010, n. 15208, in *Cass. pen*., 2010, p. 2995] ritiene discutibilmente che l'operazione di duplicazione del sistema informatico con la creazione di una copia-clone inalterabile faccia venir meno il requisito dell'irripetibilità necessario per applicare le maggiori garanzie riconosciute dall'art. 360 c.p.p.(diritto di preavviso al difensore, diritto di partecipazione con un perito e diritto di instaurare l'incidente probatorio). L'art. 360 c.p.p. potrà operare laddove gli accertamenti non abbiano il carattere di urgenza e riguardino prove digitali che non sono più nella disponibilità di chi potrebbe alterarle. In tale evenienza il preavviso alla difesa può svolgere la sua funzione di garanzia senza compromettere le esigenze cognitive. L'ipotesi paradigmatica è quella dell'estrazione dei dati digitali da un personal computer che sia trovato spento e sottoposto a sequestro.

[217] Il legislatore si è preoccupato di richiamare normativamente l'esigenza normativa di assicurare la conservazione dei dati originali e di impedire l'alterazione imponendo agli organi di polizia giudiziaria (o loro incaricati) l'adozione di misure tecniche idonee alla tutela della prova digitale. Attualmente, si ritiene che la metodologia più idonea a non alterare il sistema informatico sia la copiatura con il metodo *bitstream image* (o clonazione, vale a dire creazione di una copia identica all'originale) del supporto su cui i dati sono memorizzati (di solito un *hard disk*). Invero, qualsiasi operazione effettuata su un sistema informatico o telematico, anche la semplice attività di copiatura, può determinare una modifica seppur minima del sistema. Basti pensare che la sola procedura di accensione di un sistema operativo come Windows è in grado di produrre numerose modifiche. Si discute, peraltro, la circostanza che l'attività di copiatura abbia una natura irripetibile, in quanto implichi ridottissime modifiche al sistema informatico. La reiterabilità o meno delle operazioni acquisitive di dati informatici dipende prevalentemente della natura modificabile o immodificabile del supporto contenente i dati oggetto di interesse e dello stato, acceso o spento, del sistema informatico. L'ipotesi più semplice è indubbiamente costituita dalla copia di un supporto non modificabile, come cd e dvd non riscrivibili: in questo caso, l'acquisizione del contenuto si traduce in un'operazione sicuramente ripetibile. Uno scenario diverso si profila, invece, nel caso di supporti modificabili (es. *hard disk*, memorie usb, etc…), perché, in tali ipotesi, il rischio di modifiche irreversibili dei dati originali è molto elevato. Si vedano sul punto gli approdi raggiunti dai ricercatori dell'Università di Princeton in tema di copia della memoria RAM in A. Grillo, U.E. Moscato, *Riflessioni sulla prova informatica*, in *Cass. pen*., 2010, p. 384.

[218] F. CORDERO, *Procedura penale*, Giuffré, Milano, 2006, p. 828, P. FELICIONI, Le *ispezioni e perquisizioni*, in G. UBERTIS, G.P. VOENA, *Trattato di procedura penale*,

normativa, i sistemi informatici[219] o telematici[220], non anche i dati, le informazioni e i programmi, come si verifica nelle perquisizioni (ex artt. 247 comma 1 bis e 352 comma 1 bis c.p.p.)[221]. Sicché, il suo campo di operatività è quello di un'osservazione e rilevazione preliminare delle componenti esteriori del sistema informatico o telematico, finalizzate ad accertare la presenza, negli stessi, di programmi e dati[222]. L'ambito oggettivo in cui l'ispezione può esplicarsi è, dunque, circoscritto in ragione della funzione di ricerca visiva che essa svolge, poiché gli elementi di

---

cit., p. 95; P. TONINI, La prova penale, Cedam, Padova, 2000, p. 246. In giurisprudenza, tra le molte, Cass., sez. VI, 26 ottobre 1992, in *Cass. pen*, 1994, n. 470, Torcaso p. 676 con nota di D. CENCI, *Sui controlli di polizia giudiziaria in materia di stupefacenti.*

[219] Il sistema informatico è definito all'art. 1 *lett. a)* della Convenzione di Budapest, il quale definisce il sistema informatico come «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, compiono l'elaborazione sistematica dei dati». Questa ampia nozione è in grado di comprendere qualsiasi apparecchiatura informatica o telematica. In riferimento alle disposizioni in esame, però, sembra che il legislatore nazionale abbia inteso abbracciare una nozione più ridotta di sistema informatico, intendendo riferirsi a elaboratori di qualsiasi dimensione e potenza (*personal computer* o grandi sistemi di elaboratori di dati) e, soprattutto, al sistema operativo o *software* di base, costituito dal complesso dei programmi che ne consentono il funzionamento, e al *software* applicativo, costituto dal complesso dei programmi per specifiche funzioni.

[220] Il sistema telematico è il 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 oppure anche un sistema di *computer* in rete o, ancora, le reti di comunicazione sia pubbliche sia private, aventi copertura nazionale o internazionale.

[221] Il comma 1 bis subordina la possibilità di procedere a perquisizione di sistemi informatici o telematici all'esistenza dei presupposti descritti nei commi 1 e 2 dell'art. 352 c.p.p.

[222] G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Giuffré, Milano, 2009, p. 193; S. ATERNO, Art. 8, in G. CORASANTI, G. CORRIASLUCENTE (a cura di), Cybercrime, *responsabilità degli enti, prova digitale*, Cedam, Padova, 2009, p. 205 e s. Nelle ispezioni, quindi, non rientra l'attività di realizzazione di una copia. Contra: A. CISTERNA, *Perquisizioni in caso di fondato motivo*, in *Guida al diritto*, 16, p. 166, secondo cui l'attività ispettiva includerebbe pure operazioni come il sequestro di una copia dell'*hard disck*.

prova digitali difficilmente sono percepibili *ictu oculi* grazie all'esame esteriore.

Al contrario, la perquisizione di un dispositivo digitale, volta a trovare dati, informazioni, programmi o tracce, pertinenti al reato perseguito e suscettibili di essere cancellati o dispersi, determina un maggiore compressione della vita privata individuale. Per questo mezzo di ricerca della prova il legislatore ha previsto un ambito di applicazione più ampio che per l'ispezione, in quanto esso si attua accedendo a ogni sistema telematico o informatico, comprese la memoria interna (o centrale) e le eventuali memorie esterne (o ausiliarie) del *computer* [223], quando esiste un fondato motivo di ritenere che vi si trovino tracce informatiche pertinenti all'illecito penale. In questa prospettiva, nella formulazione degli artt. 247 e 252 c.p.p è stata inserita la possibilità di superare le «misure di sicurezza» poste a protezione dei sistemi da perquisire, adottando gli accorgimenti diretti «ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»[224].

Cionondimeno, affinché la limitazione della *privacy* individuale sia proporzionata, la perquisizione deve essere dettata da reali esigenze legate alle indagini penali[225]. Allo scopo potrebbe giovare indicare, nel decreto che dispone la perquisizione, i protocolli procedurali da seguire, magari

[223] cd *rom*, dvd, *pen drive*, schede esterne, etc.

[224] Simile esigenza potrebbe emergere anche in riferimento alle ispezioni, sebbene l'art. 244 c.p.p. non consenta espressamente agli organi di polizia giudiziaria tale operazione. Invero, però, la necessità di coerenza e non contraddizione all'interno del sistema, suggeriscono di ritenere ammissibile il superamento di eventuali misure di protezione con le moderne tecniche crittografiche anche in occasione di esperimento di una ispezione, in quanto quest'ultima è un mezzo di ricerca della prova spesso propedeutico e strumentale al successivo esperimento della perquisizione.

[225] Sulla difficoltà di controllare il requisito della pertinenza e sul rischio di utilizzi distorsivi cfr. R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, cit., p. 136

individuando anche le parole chiave collegate al fatto illecito per cui si investiga e in base alla quali impostare la ricerca nel sistema informatico[226]. Diversamente si rischia che tale mezzo di ricerca della prova venga indebitamente strumentalizzato allo scopo esclusivo di reperire notizie di reato[227].

Preferibile sarebbe, dunque, accedere, successivamente all'ispezione, al sistema per perquisirlo, selezionando i dati che risultino pertinenti al reato da sottoporre successivamente a eventuale sequestro e copiatura. Ciò, tuttavia, richiederebbe la possibilità di svolgere accertamenti tecnici irripetibili ex art. 360 c.p.p. in contraddittorio, considerato l'elevato rischio di alterare il sistema informatico durante la procedura di selezione dei dati penalmente rilevanti[228].

Un rilievo conclusivo deve essere dedicato a evidenziare l'incompatibilità delle perquisizioni *on-line* svolte tramite programmi *spyware* all'oscuro del destinatario (dette anche perquisizioni occulte o elettroniche) con le

---

[226] La scelta dei metodi procedurali è di fatto rimessa, nel silenzio normativo, alla capacità professionale degli organi inquirenti. Una soluzione è rappresentata dall'impiego delle metodologie di individuazione e apprensione delle prove digitali ritenute migliori per l'attuale stato della tecnica informatica.

[227] Un'interpretazione più ampia è accolta in giurisprudenza. La Suprema corte, infatti, ritiene che qualunque elemento -persino le mere supposizioni logiche legate al tipo di reato commesso- possa motivare il provvedimento che dispone il sequestro, senza dover individuare in anticipo cosa trovare, In tal senso, ma sul sequestro in generale, cfr. Cass. pen., sez. II, 19 giugno 2008, n. 35866, in *Ced* 241113.

[228] In tali casi, peraltro, intervengono ufficiali di p.g. specializzati e muniti di *software* apposito per discernere i *files* o le parti di *files* utili alle investigazioni. Questa operazione, tuttavia, spesso richiede diverso tempo, non essendo quasi mai sufficiente un esame superficiale al contenuto del *computer* in quanto il dato probatorio digitale frequentemente è nascosto, in settori di files (*clusters*) o addirittura cancellato, pur essendo "ripristinabile" con sofisticati procedimenti tecnici Così, nella prassi si verificherà di frequente che gli agenti intervenuti a eseguire il sequestro effettuino una copia-clone dell'intero sistema G. COSTABILE, Scena criminis, *documento informatico e formazione della prova penale*, 2004, in, *www.altalex.com.*

disposizioni della legge 48/2008[229]. Esse rappresentano un mezzo di indagine piuttosto recente, che consente di duplicare, parzialmente o totalmente, le unità di memoria del sistema informatico interessato (cd. *onlinesearch* o *one-timecopy*), nonché di rilevare e registrare nel tempo quali siti *web* vengono visitati attraverso quel sistema od attraverso i particolari *account* che si riferiscono a quel sistema (c.d. *on line surveillance),* all'insaputa dell'utilizzatore. È possibile persino giungere a carpire ciò che viene digitato sulla tastiera collegata al sistema stesso[230].

Stando così le cose, non pare possibile armonizzare le perquisizioni *on line*, aventi carattere occulto, con le garanzie difensive previste dal codice di rito per la perquisizione disposta dall'autorità giudiziaria ovvero effettuata d'urgenza dalla polizia giudiziaria.

Inoltre, simile attività potrebbe essere ricondotta all'istituto giuridico delle intercettazioni regolamentato dall'art. 266 *bis* c.p.p solo laddove essa riguardasse comunicazioni e conversazioni in corso tramite sistemi informatici sottoposti a controllo[*231*]. Al contrario, la captazione segreta di informazioni statiche memorizzate in un *computer* e non destinate a essere condivise con terzi è incompatibile con le norme processuali [232]. Pertanto,

---

[229] Le perquisizioni *on line* si sono trovate al centro di un acceso dibattito nell'ordinamento tedesco, a seguito di una importante sentenza del Bundesverfassungsgericht (Corte costituzionale federale) del febbraio del 2008 sulla c.d. OnlineDurchsuchung. Cfr. La traduzione di alcuni stralci della sentenza in *Riv. trim. dir. pen. econ.*, 2009, p. 679 e s. con nota di R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla cd*. Online Durchsuchung.

[230] Ciò è possibile inserendo, nel sistema informatico da "osservare", un programma spia ad hoc idoneo a captare i dati sopra descritti e di trasmetterli, in tempo reale o ad intervalli prestabiliti. R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla cd.* Online Durchsuchung, cit., p. 695 e s.

[231] P. GUALTIERI, *Diritto di difesa e prova scientifica,* in *Dir. pen e proc*., 2011, p. 500 e s.

[232] S. ATERNO, Art. 8, in G. CORASANTI, G. CORRIASLUCENTE (a cura di), Cybercrime, *responsabilità degli enti, prova digitale,* cit., p. 213.

le perquisizioni *de quibus* possono essere qualificate come atti di indagine irrituali, giuridicamente improduttivi di effetti[233].

5. La garanzia del diritto riservatezza e i sequestri informatici.

Nel corso delle indagini preliminari, gli inquirenti, di fronte alla necessità di sottoporre a sequestro elementi di prova aventi natura informatica, devono affrontare un duplice problema: individuare l'oggetto da sequestrare e correlativamente determinare l'estensione del vincolo.

Fin dalle prime investigazioni di tipo informatico, la dottrina più accorta aveva evidenziato l'importanza di limitare l'estensione di tale mezzo di ricerca della prova ai soli dati digitali senza includervi il supporto che li contiene, nonostante l'art. 253 c.p.p. individui quale oggetto del sequestro la «cosa», intesa come *res*[234].

Inizialmente, tuttavia, tranne casi eccezionali[235], nei procedimenti penali in cui era coinvolto materiale probatorio digitale, l'autorità giudiziaria procedeva a sequestrare l'elaboratore ed ogni componente periferica dello stesso (*mouse, monitor*, stampanti), motivando la misura in base al vincolo

---

[233] M. DANIELE, *La prova digitale nel processo penale*, cit., p. 285. Esse, invece, non possono essere considerate prove atipiche ai sensi dell'art. 189 c.p.p., poiché detta disposizione non può essere richiamata per eludere le norme codicistiche che regolano i mezzi di ricerca della prova. A sostegno di tale ultima ricostruzione cfr. S. MARCOLINI , *Le cosiddette perquisizioni* on line (o *elettroniche*) in *Cass. pen*. 2010, p. 2855 e s.; P. FELICIONI, *Le ispezioni e le perquisizioni*, in G. UBERTIS, G.P. VOENA, *Trattato di procedura penale,* cit., p. 61; questi autori richiamano, tra l'altro, i concetti di inutilizzabilità e di incostituzionalità in relazione agli elementi di prova raccolti con le perquisizioni *online.*

[234] G. BUONUOMO, *Profili penali dell'informatica*, Giuffré, Milano, 1994, p. 166.

[235] Per un approfondimento anche della casistica giurisprudenziale A. MONTI, *No ai sequestri indiscriminati di* computer, nota a Tribunale di Brescia, sez.2., 9 ottobre 2006, in *Dir internet*, 2007, p. 269.

di pertinenza[236]. Invero, però, nella maggior parte delle ipotesi, la "cosa pertinente" al reato non è l'elaboratore, l'*hard disk* o un'altra periferica, ma solamente alcuni dei *files* o documenti informatici in essi salvati.

Perciò, il sequestro probatorio dell'intero supporto digitale (es. *computer* o *hard disk*), così come la clonazione integrale di quest'ultimo, soprattutto quando effettuate nei confronti di soggetti terzi rispetto alla commissione del reato perseguito dovrebbero essere disposti dagli organi inquirenti con particolare cautela, dato l'inevitabile sacrificio arrecato alla riservatezza.

Purtroppo, la legge di riforma n. 48 del 2008, pur recependo la distinzione tra prova digitale e suo contenitore[237], non affronta la questione dell'estensione del vincolo giuridico imposto nel sequestro informatico, limitandosi a incidere su alcune specifiche disposizioni (art. 254[238], 256,

---

[236] *Ex multis*: Cass., sez. I, 16 febbraio 2007, n. 25755.

[237] In tal senso, indicativo è il testo del novellato art. 247 c.p.p., che parla di ricerca di dati, informazioni, programmi e, comunque, tracce. Cfr. le considerazioni svolte nel precedente paragrafo alla nota 198

[238] L'art. 254 c.p.p. consente il sequestro, presso i gestori di servizi telematici e di telecomunicazione, della corrispondenza inoltrata in via telematica. Tale intervento ha determinato il superamento dei dubbi circa la riconduzione della posta elettronica alla nozione di corrispondenza [P.P. RIVELLO, *Sub art. 254*, in A. GIARDA, G. SPANGHER, (a cura di), *Commento al nuovo codice di procedura penale*, Ipsoa, 2010 p. 2496] Parte della dottrina ha, tuttavia, osservato che, giacché la norma consente esclusivamente il sequestro di posta elettronica immessa nel sistema di comunicazione e che si trovi temporaneamente nella disponibilità del gestore o fornitore del gestore telematico e non ancora trasmessa al destinatario, la modifica sarebbe marginale se si considera la velocità di inoltro delle comunicazioni via internet, che sono normalmente immediate. Si rende, perciò, necessario distinguere tra sequestro della corrispondenza telematica e presso il gestore e l'intercettazione di comunicazione informatica e telematica (art. 266 bis c.p.p.) [A. MACRILLÒ, *Le nuove disposizioni in tema di sequestro probatorio e di custodia e di assicurazione dei dati informatici*, in *Dir. internet*, 2008, p. 503; L. LUPARIA, *La ratifica della Covenzione* Cybercrime *del consiglio d'Europa*, in *Dir. pen e proc.* , 2008, p .721] Il legislatore ha, inoltre, inteso adottare particolari cautele a garanzia della riservatezza consistenti nel divieto, per la p.g., non solamente di aprire i relativi *files*, ma altresì' di alterarne il contenuto. In questo modo, si ha una equiparazione tra posta elettronica e lettera in piego chiuso A. MACRILLÒ, *op. loc. ult. cit*.

259 e 260 [239] c.p.p.) nonché introducendo anche un'ipotesi speciale di sequestro (art 254 bis c.p.p.)[240].

Nel silenzio normativo, per superare il problema, in via interpretativa, si può fare riferimento al collegamento esistente tra reato perseguito e supporto informatico (ossia il *computer* o una sua memoria interna o esterna). Se tale collegamento non riguarda il supporto informatico ma semplicemente una parte del suo contenuto, sequestrarlo integralmente o crearne una copia-clone significherebbe sacrificare ingiustificatamente la sfera di riservatezza personale.

Conseguentemente, qualora vi sia motivo fondato di ritenere che rilevino, ai fini investigativi, dati digitali conservati all'interno del supporto elettronico (*computer* o altra memoria), sarebbe opportuno che il sequestro fosse preceduto da un'attività mirata a verificare, attraverso l'ispezione e la perquisizione, il contenuto del dispositivo per accertare la presenza delle informazioni ricercate, così da acquisire unicamente queste ultime.

---

[239] La legge di riforma, inoltre, modifica rispettivamente la disciplina novellando la disciplina del dovere di esibizione facente capo a persone tenute al segreto professionale, della custodia e, infine, dell'apposizione dei sigilli informatici.

[240] Esso stabilisce che l'autorità giudiziaria, quando dispone il sequestro presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti (inclusi quelli di traffico e ubicazione), può stabilire per esigenze legate alla regolare fornitura dei servizi stessi, che la loro acquisizione avvenga mediante copia sui su adeguato supporto, con procedura che ne garantisca genuinità e non alterabilità. Parte della dottrina evidenziando la sovrapponibilità di questa norma all'art. 132 d. lgs. 296/2003, ha concluso che il p.m., in base al codice di rito, potrebbe acquisire tutti i dati di traffico telefonico e telematico conservati dai fornitori, aggirando i limiti temporali e le garanzie stabilite dal codice della *privacy*. Alcuni autori hanno proposto allora una lettura sistematica in base alla quale l'art. 254 bis c.p.p. disciplinerebbe solo le modalità in cui deve avvenire il sequestro (*quomodo*), mentre i presupposti del provvedimento ablatorio sarebbero fissati dall'art. 132 d. lgs. 296/2003 (*an*). A. CISTERNA, *Il legislatore interviene ancora sulla* data retention, *ma non è ancora finita*, in *Dir. pen e proc.* 2009, p. 279 e s. ; F. CERQUA *Conservazione dei dati digitali e tutela della privacy*, in MARAFIOTI L. e LUPARIA L., *Banca dati del DNA e accertamento penale*, cit., p. 239.

Diversamente, il sequestro dell'intero dispositivo digitale non sarebbe giustificato da un effettivo nesso di collegamento con l'oggetto dell'investigazione e risulterebbe indebitamente limitato il diritto alla *privacy* dell'indagato (o del soggetto interessato dal sequestro), mancando una esigenza concreta di accertamento dei reati.

Nei casi di maggiore complessità tecnica, invece, si potrebbe sequestrare il supporto contenente le prove digitali allo scopo di analizzarne il contenuto, per poi, in tempi brevi, restituirlo al proprietario, mantenendo il sequestro solo sulle copie dei *files* rilevanti ai fini delle indagini, così riducendo al minimo il sacrificio di diritti soggettivi quali il diritto di proprietà e la riservatezza.

Il sequestro avente ad oggetto dati informatici, altamente volatili e alterabili, dovrebbe essere sempre accompagnato dalla creazione di una copia[241] su idonei supporti informatici capaci di assicurare genuinità e immodificabilità del dato digitale; cosa che la legge non impone obbligatoriamente[242]. Inoltre, analogamente a quanto osservato con riferimento all'ispezione e perquisizione, la presenza del difensore alle operazioni di sequestro potrebbe essere utile a garantire la pertinenza dei dati sequestrati dagli inquirenti[243]

---

[241] Il dovere di realizzare una copia idonea ad assicurare la conformità del dato assunto rispetto nel sequestro disposto dall'autorità giudiziaria con esclusivo riferimento ai dati informatici presso i fornitori di servizi (art. 254 bis c.p.p.), ove si aggiunge la precisazione che la copia deve essere fatta su di un supporto «adeguato». La circostanza garantita secondo la dottrina solo dalla tecnica *bitstream image* usata su un supporto vergine [cfr. M.A. SENOR, *Legge 18 marzo 2008, n. 48 di ratifica ed esecuzione della Convenzione di Budapest sulla criminalità informatica*, in *www.altalex.* com;S. ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. pen e proc., Dossier*, 2008, p. 60]. Le altre ipotesi di sequestro (es. sequestro presso banche ex art. 248, comma 2 c.p.p.) non impongono né l'obbligo di effettuare la copia né la necessaria adeguatezza del supporto.

[242] Cfr. parte II cap.II par. 4 nota 216.

[243] Cfr. parte II, cap. II, par. 4 nota 217.

Nella disciplina in esame, però, la riservatezza appare eccessivamente compromessa di fronte alla detenzione delle prove digitali da parte degli inquirenti. La ragione è dovuta al fatto che la giurisprudenza prevalente tende a distinguere il regime di conservazione delle prove digitali originali, sottoposte a sequestro insieme ai supporti che le incorporano, dal regime di conservazione di eventuali copie (duplicazioni su cd, dvd, creazione di copie-clone) realizzate su diversi supporti. Così, nell'ipotesi in cui si proceda a estrarre una copia dai dati informatici originali, la Suprema Corte ammette la restituzione dell'originale al legittimo proprietario, venuta meno l'esigenza probatoria *ex* 262 c.p.p.[244], senza, però, riconoscere all'indagato, il diritto di entrare in possesso anche delle copie, una volta ottenuta la restituzione degli originali[245].

Il mantenimento nella disponibilità dell'autorità giudiziaria del materiale duplicato determina una compressione della *privacy* individuale, non presa in considerazione da tale orientamento; infatti, i duplicati dei documenti informatici contengono i medesimi dati degli originali e, perciò, in caso di una loro indebita diffusione, manifestano la stessa potenzialità lesiva.

La circostanza che dette copie rimangano per un tempo indefinito a disposizione dell'autorità giudiziaria senza che siano previste quanto meno procedure di cancellazione o distruzione attivabili dall'interessato aumenta esponenzialmente il rischio di una loro apprensione e successiva diffusione da parte dei terzi. Per tale ragione, sarebbe preferibile sostenere un'interpretazione favorevole a riconoscere all'indagato/imputato

[244] Ciò accade, al più tardi, successivamente al passaggio in giudicato della sentenza. In tal senso cfr. Cass., sez. VI, 26 giugno 2009, n. 26699, in *Cass. pen*, 2010, p. 253.

[245] In questo senso Cass., sez. un., 24 aprile 2008, n. 18253 con nota di S. CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen e proc*, 2009, p. 481 e s.

l’interesse a impugnare il provvedimento di sequestro anche dopo la restituzione degli originali.[246]

[246] Peraltro, la garanzia della installazione di sigilli informatici sulle cose sequestrate – che potrebbe essere un utile strumento per una custodia più sicura dei *files* sequestrati- è prevista come meramente facoltativa, e non come obbligatoria, dall'art. 260.

Bibliografia

ABRUSCI I., *Cancellazione dei profili e distruzione dei campioni*,in MARAFIOTI L. e LUPARIA L., *Banca dati del DNA e accertamento penale. Commento alla legge di ratifica del trattato di Prüm istitutiva del database genetico nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85),* Giuffrè, Milano, 2009,p. 112.

ADORNO R., *Il prelievo coattivo a fini investigativi,* in *Giur. It.,* 2010, 5, II, c. 1232.

ATERNO S., *Acquisizione e analisi della prova informatica*, in *Dir. pen. proc.*, *Dossier*, 2008, p. 60.

ATERNO S., *Art. 8*, in G. CORASANTI, G. CORRIASLUCENTE (a cura di), Cybercrime, *responsabilità degli enti, prova digitale*, Cedam, Padova, 2009, p. 205.

ATERNO S., CISTERNA A., *Il legislatore interviene ancora sulla* data retention, *ma non è finita*., in *Dir. pen e proc*., 2009, p. 279.

AULETTA T.A., *Riservatezza e tutela della personalità,* in *Pol. Dir*., 1974, p. 54.

BALDASSARRE A., Privacy *e costituzione. L'esperienza statunitense,* Bulzoni Ed.,Roma, 1984.

BARBATO V., CORRADI F., LAGO G., *L' identificazione personale tramite Dna*, in *Dir. pen. e proc*., 1999, p. 215

BARBERA A., FUSARO C., *Corso di diritto pubblico*, Il Mulino, Bologna, 2008.

BARBERA A., *Commento all'art. 2 della Costituzione*, in G. BRANCA (a cura di), *Commentario della Costituzione italiana*, Zanichelli –Foro Italiano, Bologna-Roma, I, 1975, p. 84.

BARGIS M., *Costituzione per l'Europa e cooperazione giudiziaria in materia penale*, in *Riv. it. dir. proc.pen*., 2005, p. 144.

BARILE P., *Diritti dell'uomo e delle libertà fondamentali*, Il Mulino, Bologna, 1984.

BARILE P., CHELI E., GRASSI P., *Istituzioni di diritto pubblico*, Cedam, Padova, 2009.

BASSOLI E., *Acquisizione dei tabulati Vs. Privacy: la* data retention *al vaglio della Consulta*, in *Riv. dell*'internet, 2007, p. 237.

BERNARDI E., *Strategie per l'armonizzazione dei sistemi penali europei*, in *Riv. Trim. dir. pen. ec*., 2002, p. 789.

BLASI A., *La protezione dei dati personali nella giurisprudenza della Corte Europea dei diritti dell'uomo*, in *Riv. trim .dir. u.*, 1999, p. 543.

BLUOSTEIN E. J., *Privacy an as aspect of human dignity: an aswer: to Dean Prosser*, in *New York University Law Review*, 1964, vol. XXXIX, p. 970.

BONETTI M., *Riservatezza e processo penale*, Giuffrè, Milano, 2003.

BORUSSO R., RUSSO S., TIBERI C., *L'informatica per il giurista. Dal* bit *a* internet, Giuffré, Milano, 2009.

BRAGHÒ G., *Le indagini informatiche tra esigenze di accertamento e garanzie di difesa*, in *Dir. inf. e informatica*, 2005, 524.

BRAGHÒ G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica*, Giuffré, Milano, 2009, p. 193.

BUONUOMO G., *Profili penali dell'informatica*, Giuffré, Milano, 1994.

BUSIA G., Privacy *a rischio per la durata della conservazione*, in *Guida dir*.,2009, 30, p. 77.

BUTTARELLI G., *Banche dati e tutela della riservatezza. La* privacy *nella società dell'informazione*, Giuffrè, Milano, 1997.

CAJANI F., *Alla ricerca del* log *(perduto),* in *Dir. Internet*, 2006, p. 572.

CAJANI F., ATERNO S., *La disciplina in tema di conservazione dei dati* (data retention), in ATERNO S., CAJANI F., COSTABILE G., MATTEUCCI M., MAZZARACO G., Computer forensics *e indagini digitali*, Experta, Forlì, 2011, p. 249.

CAJANI F., ATERNO S., *Perquisizione ed ispezione*, ATERNO S., CAJANI F., MATTIUCCI M., MAZARACCO G., Computer forensic *e indagini digitali*, Experta, Forlì, 2011, p. 465.

CALVANESE E., *Adesione al Trattato di Prüm e cooperazione transfrontaliera*, in SCARCELLA A. (a cura di), *Adesione al Trattato di Prüm e cooperazione transfrontaliera per il contrasto alla criminalità. Prelievo del DNA e banca dati nazionale*, Cedam, Padova .2009, p. 11.

CARNEVALE S., *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen e proc*, 2009, p. 481 e s.

CAMON A., *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. e proc. pen*., 2005, p. 594.

CAMON A., *Le riprese visive come mezzo di indagine: spunti per una rioflessione sulle prove incostituzionali*, in *Cass. Pen.*, 1999, p. 1195.

CARNELUTTI F., *Il diritto alla vita privata*, in *Riv. trim. dir. pubbl*., 1955, p. 3.

CARTABIA M., *Il Trattato di Lisbona*, in *Giornale dir. amm.*, 2010, 3, p. 221.

CASASOLE F., *Prelievi e accertamenti tecnici coattivi*, in MARAFIOTI L. e LUPARIA L., *Banca dati del DNA e accertamento penale. Commento alla legge di ratifica del trattato di Prüm istitutiva del database genetico nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85)*, Giuffrè,, Milano, 2009, p. 243.

CASSIBBA F., *Le perquisizioni presso lo studio del difensore alla luce della Convenzione europea dei diritti dell'uomo,* in *Ind. pen*., 2008, p. 77.

CASTELLANETA M., *Uno scambio di informazioni tra gli Stati per rafforzare la lotta al crimine organizzato,* in *Guida al diritto*, 30, 2009, p. 63.

CELOTTO A., *Il Trattato di Lisbona ha reso la CEDU direttamente applicabile nell'ordinamento italiano*?, in *www.giustamm.it.*

CENCI D., *Sui controlli di polizia giudiziaria in materia di stupefacenti*, in *Cass. pen*, 1994, p. 676.

CERQUA F., *Conservazione dei dati digitali e tutela della privacy*, in MARAFIOTI L. e LUPARIA L., *Banca dati del DNA e accertamento penale. Commento alla legge di ratifica del trattato di Prüm istitutiva del database genetico nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85)*, Giuffrè, Milano, 2009, p. 236.

CHIAVARIO M., *Cooperazione giudiziaria e di polizia in materia penale a livello europeo,* in *Riv. it. dir. proc. pen.*, 2005, p. 974.

CIAMPI S., *Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea*, in PERONI F., GIALUZ M.(a cura di),*Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009, p. 34.

CISTERNA A., *Il legislatore interviene ancora sulla data retention, ma non è ancora finita,* in *Dir. pen e proc*. 2009, p. 279.

CISTERNA A., *Perquisizioni in caso di fondato motivo,* in *Guida al diritto*, 16, p. 166.

CLOONEY T. C., *A Treatise on the Law of Torts or the Wrongs which Arise Indipendent of contract*, Challagan & Company, Chicago IL, 1888, p. 29.

COCITO A., *L'ambito definitorio,* in MARAFIOTI L. e LUPARIA L., *Banca dati del DNA e accertamento penale. Commento alla legge di*

ratifica del trattato di Prüm istitutiva del database genetico nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85), Giuffrè, Milano, p. 44 .

COCITO A., *Parametri internazionali e affidabilità dei laboratori nell'analisi dei reperti e dei campioni*, in MARAFIOTI L. e LUPARIA L., *Banca dati del DNA e accertamento penale. Commento alla legge di ratifica del trattato di Prüm istitutiva del database genetico nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85)*, Giuffrè, Milano, 2009,p. 93.

COLAIACOVO C. , *Competenza del Garante per la protezione dei dati personali sull'applicazione del Trattato di Prüm*,n SCARCELLA A. (a cura di), *Adesione al Trattato di Prüm e cooperazione transfrontaliera per il contrasto alla criminalità. Prelievo del DNA e banca dati nazionale*, Cedam, Padova ,2009, p. 173.

COLAVITTI G., PAGOTTO C., *Il Consiglio di Stato applica direttamente le norme CEDU grazie al Trattato di Lisbona: l'inizio di un nuovo percorso?, Guida al diritto*, 14, 2010, p. 88.

CONFORTI B., *Diritto internazionale*, 1992, Ed. Scientifica, Napoli, p. 294.

COSATBILE G., RASETTI D., Scena criminis, *documento informatico e formazione della prova penale*, in *Ciberspazio e diritto*, 2003, p. 273.

COSTABILE G., Scena criminis, *documento informatico e formazione della prova penale*, 2004, in *www.altalex.com.*

D'ANGELO L., *"Comunitarizzazione" dei vincoli CEDU in virtù del Trattato di Lisbona? No senza una* expressio causae, in www.forumcostituzionale.it.

D'ANGELO L. A., *La conservazione dei dati del traffico telefonico e telematico tra esigenze investigative e tutela della* privacy, in A. A. DALIA (a cura di), Le nuove norme di contrasto al terrorismo, Giuffré, Milano, 2006,, p. 121 e ss.

DANIELE L., *Diritto dell'Unione europea. Sistema istituzionale, ordinamento, tutela giurisdizionale, competenze*, Giuffrè, Milano, 2010.

M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 283.

DE AMICIS G., UZZOLINO G., *Lo spazio di libertà, sicurezza e giustizia nelle disposizioni penali del Trattato che istituisce una Costituzione per l'Europa*, in *Cass. pen.*, 2004, p. 3067.

DE CUPIS A., *I diritti della personalità*, in *Trattato di diritto civile e commerciale*, CICU, MESSINEO (a cura di),, Giuffrè, Milano, I, 1982, p. 326.

DE LEO F., *Controllo delle comunicazioni e riservatezza*, *Cass. pen*, 2002, p. 2208.

DE SIERVO U., *Tutela dei dati personali*, in *Diritti, Nuove tecnologie, trasformazioni sociali. Scritti in memoria di P. Barile*, Cedam, Padova, 2003, p. 299.

DE VERGOTTINI G., *Oltre il dialogo tra le Corti. Giudici, diritto straniero e comparazione*, Il Mulino, Bologna, 2010.

DOMENICI R. , *Prova del DNA*, in *Dig. disc. pen.*, Torino, UTET, 1997.

DOMINIONI O., *La prova penale scientifica*, Giuffrè, Milano, 2005.

FANUELE C. , *Dati genetici e procedimento penale*, Giuffré, Milano, 2009.

FATTA C., *La tutela della* privacy *alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Dir. dell'inf. e dell'inform.*, 2008, p. 395.

FELICIONI P., *Accertamenti sulla persona e processo penale. il prelievo del materiale biologico*, Giuffré, Milano 2007.

FELICIONI P., *L'Italia aderisce al Trattato di Prüm: disciplinata l'acquisizione e l'utilizzazione probatoria dei profili genetici* , in *Dir. Pen e proc., Speciale banche dati* , p. 18.

FELICIONI P., *Le ispezioni e le perquisizioni*, in G. UBERTIS, G.P. VOENA, *Trattato di procedura penale, Giuffré, Milano*, 2012, p. 61

FERRI G. B., Privacy *e libertà informatica*, in ALPA, BESSONE (a cura di), *Banche dati telematiche e diritti della persona*, Cedam, Padova 1984, p. 47.

FILIPPI L., *L'home –watching: documento, prova atipica o prova incostituzionale?*, in *Dir. pen. e proc.*, 2001, p. 92.

FLOR R., *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla* cd. Online Durchsuchung, in *Riv. trim. dir. pen. econ.*, 2009, p. 679.

FORLANI E., *La conservazione preventiva dei dati informatici per l'accertamento dei reati*, in *Dir. dell'internet*, 2008, p. 520.

GABRIELLI C., *Accertamenti medici dai confini troppo incerti*, in *Guida dir.*, 2009, 30, p. 71.

GALANTINI N., *L'inutilizzabilità della prova nel processo penale*, Cedam, Padova, 1992.

GALEOTTI S., *La libertà personale*, Giuffrè, Milano, 1953, p. 29.

GANDINI F., *Trattato di Prüm: modello di cooperazione transfrontaliera*, in *D. & G.*, 2006, 37, p. 56.

GARGANI A., *I rischi e le possibilità dell'applicazione dell'analisi del DNA nel settore giudiziario, in Riv. it. dir. e proc*. pen., 1993, p. 1307.

GAROFANO P., *Genetica identificativa e biobanche: aspetti tecnici e problematiche connesse*, in *Dir.pen.proc*., *Dossier*, 2008, p. 44.

GAROFANO P., *Genetica identificativa e biobanche: aspetti tecnici e problematiche connesse*, in *Dir.pen.proc*., *Dossier*, 2008, p. 44.

GENNARI G., *Identità genetica e diritti della persona*, in *Riv. crit. dir. priv.*, 2005, p. 624.

GENNARI G., SANTOSUOSSO A., *Il prelievo coattivo di campioni biologici*, in *Dir. pen proc*., 2007, p. 398.

GENNARI G., *La istituzione della banca dati nazionale del DNA ad uso forense: dalla privacy alla sicurezza*, in SCARCELLA A. (a cura di), *Adesione al Trattato di Prüm e cooperazione transfrontaliera per il contrasto alla criminalità. Prelievo del DNA e banca dati nazionale*, Cedam, Padova, 2009, p. 50.

GENTILE D., Tracking *satellitare mediante gps: attività atipica di indagine o intercettazione di dati*, in *Dir. pen. e proc*., 2010, p. 1464.

GHIRARDINI A., FAGGIOLI G., Computer forensic, Milano, Apogeo, 2009, p. 347.

GIALUZ M., *La cooperazione informativa quale motore del sistema europeo di sicurezza*, in PERONI F., GIALUZ M.(a cura di),*Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009, p. 18.

GIAMPICCOLO G., *La tutela giuridica della persona umana e il cd diritto alla riservatezza*, in *Riv. Trim. dir. proc. civ.*, 1958, p. 461.

GIUNCHEDI F., *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, Utet, Torino, 2009.

GUALTIERI P., *Diritto di difesa e prova scientifica*, in *Dir. pen e proc*., 2011, p. 500.

GROSSI P., *Introduzione a uno studio sui diritti inviolabili nella Costituzione italiana*, Cedam, Padova, 1972, 172.

KILKELLY U., *The Right to Respect for Private and Family Life. A Guide to the Implementation of Article 8 of European Convention on Human Right*, Strasburg, 2003, p. 8.

KOSTORIS R. E. , *Alt ai prelievi di sangue coattivi*, in *Dir. pen. e proc*., 1996, p.1091.

KOSTORIS R. E., *Consulente tecnico extraperitale e gratuito patrocinio,* in *Cass. pen*., 1999, p. 2789

KOSTORIS R.E., *I consulenti tecnici nel processo penale*, Giuffré, Milano, 1993.

KOSTORIS R. E., *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella risoluzione del XVIII Congresso internazionale del diritto penale,* in *Riv. dir. proc*., 2010, p. 330.

KOSTORIS R. E., *Prelievi biologici coattivi*, in R.E. KOSTORIS, R. ORLANDI (a cura di), *Contrasto al terrorismo interno e internazionale*, Giappichelli, Torino, 2006, p. 343.

LABAYLE H., *Le droit des étrangers au regroupement familial, regards croisés du droit interneet du droit européen*, in *Revue Française de Droit Administratif*, 2007, fasc. 1, p 110.

LAGO G. , *Il trattamento dei dati e dei campioni biologici: la banca dati nazionale del DNA e il bilanciamento tra le ragioni di giustizia e la tutela della* privacy, in SCARCELLA A. (a cura di), *Adesione al Trattato di Prüm e cooperazione transfrontaliera per il contrasto alla criminalità. Prelievo del DNA e banca dati nazionale*, Cedam, Padova, 2009, p. 128.

LA PERGOLA A., *Costituzione e adattamento dell'ordinamento interno al diritto internazionale*, Giuffrè, Milano, 1961, p. 267.

LARONGA A., *Le prove atipiche nel processo penale*, Cedam, Padova, 2002.

LORENZETTO E., *Le attività urgenti di investigazione informatica e telematica,* in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Giuffré, Milano, 2009, p. 37.

E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati sul computer in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen*., 2010, p. 1522

LUGARESI N., Internet, privacy *e pubblici poteri negli Stati uniti,* Giuffrè, Milano, 2000, p. 51.

LUPARIA L., ZICCARDI G., *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali,* Giuffrè, Milano, , 2007, p. 178.

LUPARIA L., *La disciplina processuale e le garanzie difensive*, in LUPARIA L., ZICCARDI G., *Investigazione penale e tecnologia informatica*, Giuffré, Milano, 2007, p. 130

LUPARIA L., *La ratifica della* Covenzione Cybercrime *del consiglio d'Europa,* in *Dir. pen e proc*., 2008, p .721

MACRILLÒ A., *Le nuove disposizioni in tema di sequestro probatorio e di custodia e di assicurazione dei dati informatici*, in *Dir. internet*, 2008, p. 503.

MARAFIOTI L., Digital evidence *e processo penale*, in *Cass. pen*., 2011, p. 4510.

MARCOLINI S., *Le cosiddette perquisizioni* on line *(o elettroniche),* in *Cass. pen*. 2010, p. 2855.

MONTI A., *No ai sequestri indiscriminati di* computer, in *Dir* internet, 2007, p. 269.

MARIOTTI S., TACCONI S., *Riflessioni sulle problematiche investigative e di sicurezza connesse alla comunicazione* VoIP, in *Dir. Internet*, 2008, p. 558.

MARTINES T., *Diritto Costituzionale,* Giuffrè, Milano, 2005.

MAURO A., GARGIULO G., VOIP *security*, in *Ciberspazio e diritto,* 2010, p. 161.

MELILLO G., *Intercettazione ed acquisizione dei tabulati telefonici: un opportuno intervento correttivo delle Sezioni Unite*, in *Cass. pen*, 1999, p. 473.

MIGLIAZZA M., *Profili internazionali ed europei del diritto all'informazione e alla riservatezza*, Giuffré, Milano, 2004.

MONTI A., *Catena di custodia e "doppio binario" per campioni e reperti,*in MARAFIOTI L. e LUPARIA L., *Banca dati del DNA e accertamento penale. Commento alla legge di ratifica del trattato di Prüm istitutiva del database genetico nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85)*, Giuffrè, Milano, 2009, p. 102.

MONTI A., *La nuova disciplina del sequestro informatico*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2009, p. 199.

MORTATI C., *Isituzioni di diritto pubblico*, Cedam, Padova, 1991, p. 158.

MUSUMECI A. , *La ratifica del Trattato di Prüm,* in MARAFIOTI L. e LUPARIA L., *Banca dati del DNA e accertamento penale. Commento alla legge di ratifica del trattato di Prüm istitutiva del database* genetico *nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85)*, Giuffrè, Milano, 2009, p. 14.

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. 520.

NIGER S., *Le nuove dimensioni della* privacy*: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006, p. 27.

ORLANDI R., *Attività di* intelligence *e di diritto penale della prevenzione*, in G. ILLUMINATI (a cura di), *Nuovi profili del segreto di stato e dell'attività di* intelligence, Giappichelli, Torino, 2010, p. 227

ORLANDI R., *Il processo nell'era di* internet, in *Dir. pen e proc*., 1998, p. 140.

ORLANDI R., *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc*., 2009, p. 128.

PACE A., *Libertà personale* (dir. cost.), in Enciclopedia del diritto, XXIV, Giuffrè, Milano, 1974, p. 287 e ss.

PACE A., *Problematica delle libertà costituzionali*, Cedam, Padova, 1990.

PACE A., *Problematiche sulle libertà fondamentali*, Cedam, Padova,III ed., 2003

PARISI N., *Funzione e ruolo della Carta di diritti fondamentali nel sistema delle fonti alla luce del Trattato di Lisbona,* in *Dir. Un. Eur.*, 2008, p. 653.

PARODI C., VoIP, Skype *e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?, Dir. Internet,* 2008, p. 1309.

PECORELLA C., *Il diritto penale dell'informatica*, Giuffrè, Milano, 1994.

PICA G., *Diritto penale delle tecnologie informatiche*, Utet, Torino, 2000.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislative e beni giuridici tutelati*, in Aa. Vv., *Il diritto penale dell'informatica nell'epoca di* internet, 2004, Cedam, Padova, p. 77.

PICOTTI L., *Trattamento dei dati genetici, violazioni della* privacy *e tutela dei diritti fondamentali nel processo penale*, in *Dir. dell'informazione e dell'inf*, 2003, p.689

PICOTTI L., *Trattamento dei dati genetici, violazioni della* privacy *e tutela dei diritti fondamentali nel processo penale*, in D. DE. LEO, S. TURRINA, M. ORRICO (a cura di), *Lo stato dell'arte nella genetica forense*, Giuffrè, Milano, 2003.

PISANI M. , *La tutela penale della riservatezza": aspetti processuali*, in *Riv. it. dir. proc. pen*., 1967, p. 787.

PIZZETTI F. , *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in BILANCIA P., D'AMICO M., *La nuova Europa dopo il Trattato di Lisbona, ,* Giuffrè, Milano2011, p. 85.

QUATTROCOLO S., *I risvolti attuativi della novella in tema di prelievi coattivi: raccolta di campioni su incapaci; verbalizzazione delle*

operazioni; distruzione dei campioni, in MARAFIOTI L. e LUPARIA L., *Banca dati del DNA e accertamento penale. Commento alla legge di ratifica del trattato di Prüm istitutiva del database genetico nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85)*, Giuffrè, Milano, 2009, p. 336.

RAFARACI T., *Intercettazioni e acquisizione di tabulati telefonici*, in R. E. KOSTORIS, R. ORLANDI (a cura di), *Contrasto al terrorismo interno e internazionale*, Giappichelli, Torino, 2006, p. 265.

RAVÀ A., *Istituzioni di diritto privato*, Cedam, Padova, 1938.

RICCI A. E., Digital evidence *e irripetibilità delle operazioni acquisitive,* in *in Dir. pen. e proc.*, 2009, p. 337.

RIVELLO P.P., *Sub art. 254*, in GIARDA A., SPANGHER G., (a cura di), *Commento al nuovo codice di procedura penale*, Ipsoa, 2010 p. 2496

SENOR M.A., *Legge 18 marzo 2008, n. 48 di ratifica ed esecuzione della Convenzione di Budapest sulla criminalità informatica*, in *www.altalex. com*.

RODOLFI A., *Il regime normativo della* data retention *nell'ordinamento italiano*, in *Ciberspazio e dir.*, 2010, p. 151.

RODOTÀ S., *La* privacy *tra individuo e collettività*, in *Pol. dir.*, 1974, 3, p. 551.

RODOTÀ S., *Tecnologie e diritti*, Il Mulino, Bologna, 1995, p. 66.

SALAZAR L., *La costruzione di uno spazio di libertà, sicurezza e giustizia dopo il consiglio europeo di Tampere,* in *Cass. pen.*, 2000, p.1114.

SALAZAR L., *La lotta alla criminalità nell'unione: passi avanti verso uno spazio giudiziario comune prima e dopo la costituzione per l'Europa ed il programma dell'Aia*, in *Cass. pen*, 2004, p. 3510.

SARZANA DI S. IPPOLITO C., *Informatica*, internet *e diritto penale*, III ed., Giuffré, Milano, 2010.

SCROLLO G., *Il regime transitorio,* in MARAFIOTI L. e LUPARIA L., *Banca dati del DNA e accertamento penale. Commento alla legge di ratifica del trattato di Prüm istitutiva del database genetico nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85),* Giuffrè, Milano, 2009, p. 167

SORRENTINO F., *Nuovi profili costituzionali dei rapporti tra diritto internale, internazionale e comunitario,* in *Dir. pubbl. comp. eur*., 2002, p. 1359.

SPRIANO M., *Acquisizione del DNA dall'imputato e dai suoi parenti* in *Dir. pen. proc,* 2005, p. 347.

STEFANINI E., *Dati genetici e diritti fondamentali,* Cedam, Padova, 2008.

STRACUZZI A., Data retention: *il faticoso percorso dell'art. 132 Codice* privacy *nella disciplina della conservazione dei dati digitali*, in *Dir. inf*., 2008, p. 585.

STRAMAGLIA M. , *Prelievi coattivi e garanzie processuali*, in MARAFIOTI L. e LUPARIA L., *Banca dati del DNA e accertamento penale. Commento alla legge di ratifica del trattato di Prüm istitutiva del database genetico nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85),* Giuffrè, Milano, 2009, p. 336.

TONINI P., *Accertamento del fatto e informazioni genetiche: un difficile bilanciamento,* in *Dir. pen. e proc,* 2009, *Gli speciali,* p. 5;

TONINI P., *Documento informatico e giusto processo*, in *Dir. pen. proc*., 2009, p. 404.

TONINI P., *Informazioni genetiche e processo penale a un anno dalla legge*, in *Dir. pen e proc.*, 2010, p. 833.

TONINI P., *La prova penale*, Cedam, Padova, 2000.

TONINI P., *Prova scientifica e contraddittorio*, in *Dir. pen. proc*., 2003, p. 1459.

TRONCHIA T., *Cenni problematici sulla tutele della vita privata nell'ordinamento giuridico italiano*, Cedam, Padova, 1990.

UBERTIS G., *Attività investigativa e prelievo dei campioni biologici*, in *Cass. pen*, 2008, p. 6.

VIGGIANO M., I *dati personali nelle ricerche su* internet, in *Dir. inf. e informatica*, 2007, p. 379.

VIGLIAR S., *Privacy e comunicazioni elettroniche: la direttiva 2002/58/CE*, in *Dir. inf*., 2003, p. 402.

WARREN S.D. –BRANDEIS L.D., *The right to privacy*, in *Harvard Law Review*, vol. IV, n.5, 1890, trad. it. S. Serra in V. FROSINI, *jus solitudinis*, Giuffrè, Milano, 1993, p. 52 e ss.