UNIVERSITA' DEGLI STUDI DI TRIESTE

DOTTORATO IN SCIENZE PENALISTICHE

Direttore Prof. Paolo Pittaro

LE BANCHE DATI TECNICO SCIENTIFICHE NELL'AMBITO DELL'INDAGINE FORENSE

Relatore:

Chiar.ma Prof.ssa Maria Riccarda Marchetti

Tutor:

Chiar.ma Prof.ssa Maria Riccarda Marchetti

Tesi di Dottorato di:

Dott. Salvatore Meloni

XXII CICLO

LE BANCHE DATI TECNICO SCIENTIFICHE NELL'AMBITO DELL'INDAGINE FORENSE

PREMESSA

CAPITOLO PRIMO

LA TECNOLOGIA INFORMATICA AL SERVIZO DEL PROCESSO PENALE

1)I sistemi logistici di *database*

1.1)(segue) Gli archivi elettronici criminalistici

2) Le impronte digitali

2.2) (segue) Il sistema A.F.I.S.

3) L'identificazione genetica

CAPITOLO SECONDO

PROTEZIONE E TUTELA DEI DATI INDIVIDUALI

1) Dalle banche dati al diritto all'autodeterminazione dei dati personali

2) Il diritto alla riservatezza

2.1)(segue) Il diritto alla *privacy* come diritto costituzionalmente garantito

2.2) Orientamento della Corte costituzionale

3) Il riconoscimento del diritto alla *privacy* nella Convenzione europea per la salvaguardia dei diritti dell'uomo

3.1) La libertà informatica

3.2) La Convenzione di Strasburgo 108/1981 sulla protezione degli individui rispetto al trattamento automatizzato dei dati personali

3.3)Diritto comunitario e informazioni personali: la direttiva 95/46 CE

3.4) (segue) La decisione quadro 2008/977/GAI del Consiglio, sulla tutela dei dati personali nelle materie del c.d. terzo pilastro

CAPITOLO TERZO

PROFILI PROBLEMATICI

1) La regolamentazione delle banche dati nel d.lgs. n. 196 del 2003

1.1)(segue) Il Centro elaborazione dati presso il dipartimento della pubblica sicurezza del ministero degli interni

2) Identità informativa e processo penale: scenari di una convivenza possibile

2.2)(segue) Riflessioni sulla previsione contenuta nell'art.240 comma 2 c.p.p.

3) L'informazione personale proveniente da una banca dati illecita

3.1)(segue) Alla ricerca del dato inutilizzabile: l'articolo 11 del Testo unico sulla *privacy*

3.2)(segue) Il tempo di conservazione del dato personale e il diritto all'oblio

CAPITOLO QUARTO

DALLA TRACCIA BIOLOGICA AL DNA *DATABASE*

1) I modelli di banche dati del dna

2) Il *codis* nordamericano

3) L' indagine genetica in Italia

3.1) (segue) Il prelievo coattivo di materiale biologico ad opera della polizia giudiziaria

3.2) (segue) Gli accertamenti tecnici sulla persona nella legge del 30 giugno 2009 n. 85

3.3) Archivi genetici atipici: una vicenda tutta italiana

4) La tutela del dato genetico nella normativa internazionale

4.1) Lo schema istitutivo previsto dal Trattato di Prum per il *database* statale dei profili genetici

5) La banca dati del dna nella legge 30 giugno 2009 n.85

5.1) (segue) Un *database* "emergenziale"

PREMESSA

Il ruolo delle banche dati tecnico scientifiche nell'ambito delle indagini giudiziarie è di primaria importanza, lo testimonia la massiccia implementazione di programmi operativi per la gestione combinata di informazioni individuali – anagrafiche, genetiche, fotografiche e biometriche –, avvenuta nel corso degli ultimi anni per agevolare le operazioni svolte dal pubblico ministero e dalla polizia giudiziaria; pertanto, il *database* può essere definito come un ausilio rilevante per l'esecuzione delle indagini legate alla consultazione dei dati, dal momento che gli elaboratori elettronici assistono le azioni investigative, attraverso una migliore gestione operativa delle notizie personali.

L'avvento sulla scena procedimentale di strumenti tecnici siffatti, col carico di garanzie e tutele che recano al loro interno – basti pensare alle recenti decisioni quadro del consiglio d'Europa sulla protezione dei dati personali oggetto di scambio tra gli stati dell' UE[1] –, impone una duplice osservazione; invero il rapporto tra le banche dati e il procedimento penale può essere analizzato sia in modo statico, con particolare riferimento alle regole preposte all'organizzazione del singolo dato all'interno della banca di raccolta, che in proiezione dinamica, cioè a dire, rispetto al possibile utilizzo che l'autorità giudiziaria può fare delle notizie provenienti dagli archivi informatici. A tal proposito, occorre sottolineare come l'acquisizione di una notizia derivante da un *database*, garantisca, di regola, all'autorità giudiziaria l'utilizzo di un'informazione calibrata sulla base delle norme stabilite a protezione dei dati personali dal Testo unico sulla *privacy* del 2003. Preso atto che la banca produttrice di informazioni utilizzabili, per essere considerata come tale, deve rispettare le regole fondamentali stabilite dal Testo unico per il trattamento dei dati personali, occorre interrogarsi sugli effetti che il dato trattato in modo illecito, o frutto di un'attività di raccolta non autorizzata, genera rispetto all'accertamento del fatto reato. In tal senso, si può parlare di "nuove questioni giuridiche" per tutti quei temi legati alla relazione tra le regole stabilite per disciplinare la conservazione dei dati all'interno di archivi elettronici, e il processo penale.

[1] 2006/960/GAI; 2008/615/GAI; 2008/977/GAI, consultabili sul sito http://eur-lex.europa.eu/lex.

A tutt'oggi, l'apprensione e la successiva utilizzazione del dato illecito non incontra divieti probatori stabiliti *ad hoc*, dal momento che la legge sulla *privacy* costituisce un riferimento di carattere amministrativo. A parere di chi scrive, la difesa del diritto alla riservatezza dei cittadini rispetto alle informazioni conservate in elaboratori illeciti – utilizzati dalla polizia giudiziaria o dal pubblico ministero nel corso delle indagini – dovrebbe essere regolata attraverso specifiche disposizioni, idonee a rappresentare un valido parametro normativo per la tutela del diritto alla *privacy* in ambito processuale.

La ricerca di questo difficile equilibrio costituisce l'oggetto del presente studio.

A tal fine, seguendo la linea argomentativa che prende le mosse dall'analisi delle banche dati usate per le indagini forensi – rappresentazione statica –, si cercherà di individuare le caratteristiche più importanti degli elaboratori elettronici, in modo tale da valutare i possibili intrecci col processo penale – proiezione dinamica –, alla luce delle legge sulla *privacy*, delle norme processuali esistenti in materia, e delle disposizioni internazionali.

CAPITOLO PRIMO

LA TECNOLOGIA INFORMATICA AL SERVIZO DEL PROCESSO PENALE

1. *I sistemi logistici di database*

Le notizie contenute in un *database* possono avere diversa natura e caratteristiche. In base al loro grado di modificabilità nel corso degli anni, la dottrina identifica due modelli distinti di banche dati: operative o analitiche[2].

Le prime sono archivi che contengono dati dinamici in continuo mutamento – come ad esempio i *database* degli scambi finanziari di borsa –, le seconde sono raccolte di dati storici – inquadrabili come informazioni stabili nel tempo –, consultabili per ricavare studi statistici o per realizzare altre forme di indagine di carattere sociologico o giudiziario. In quest' ottica occorre sottolineare come la differenza ontologica esistente tra i dati contenuti nei singoli archivi, cambi anche l'approccio logistico caratteristico delle rispettive banche di raccolta. Sicché i repertori d' informazioni c.d. analitici, sono contraddistinti da programmi applicativi che hanno come obiettivo primario la sistematica organizzazione del singolo dato, in modo tale da permetterne una facile e rapida consultazione; viceversa gli archivi elettronici operativi, necessitano di dispositivi tecnologici particolari, in grado di aggiornare di continuo l'informazione contenuta al loro interno, a seconda delle diverse trasformazioni che quest' ultima subisce nel corso del tempo, in modo tale da ottenere una notizia concreta, aderente alla realtà mutevole che la contraddistingue.

In tal senso occorre rilevare come un archivio elettronico, operativo o analitico, è composto da tre elementi fondamentali: l'insieme dei dati memorizzati, il *software* che li gestisce, la loro disposizione logica[3].

[2] BARBATO, *Le banche dati tecnico- scientifiche,* in *Dir. pen. proc*., 2000, 1659.

Gli strumenti *software* per la gestione di banche dati vengono indicati con l'acronimo DBMS dal nome inglese *database management system*. La loro funzione principale è quella di permettere agli utenti – e ad altre applicazioni *software* – di creare, consultare e aggiornare gli archivi elettronici. In quest'ottica il programma applicativo può essere definito come un *"trait d'union"* tra utilizzatori finali e dati, in quanto la sistemazione delle informazioni all'interno del *database* dipende dalle caratteristiche tecniche del *software* di riferimento.

Il moderno *database* è qualcosa che va al di là della statica catalogazione delle informazioni; invero i dati contenuti nelle attuali banche, rappresentano delle notizie congiungibili o intersecabili tra loro, in modo tale da creare delle informazioni integrate, sempre modificabili e perfezionabili in relazione al tipo di richiesta operata dall'utente che formula la ricerca. Pertanto, un individuo potrà usufruire di una notizia composta, in base al grado di relazione tra le informazioni collezionate all'interno del *database*, come dire che il risultato della consultazione esperibile dall'utente dell' archivio elettronico è calibrato sull' organizzazione logica dei dati *ivi* presenti.

A tutt'oggi si distinguono tre modelli logistici di banche dati, caratterizzati da altrettanti *software* di utilizzo: la forma gerarchica, reticolare e relazionale[4].

In realtà si tratta di tre schemi organizzativi che hanno avuto una loro contestualizzazione temporale ben definita – dal modello gerarchico più risalente a quello relazionale più recente –, che ha seguito l'evoluzione tecnica nel campo delle banche dati. Peraltro occorre sottolineare come i singoli programmi applicativi sono stati utilizzati fintantoché non è avvenuta l'implementazione di quelli successivi, secondo una logica di sostituzione progressiva.

Il primo modello logico di *database* risale agli anni ottanta, e permette la consultazione di un singolo dato in relazione con altri contenuti nella banca, solo nel caso in cui ci sia un rapporto di subordinazione tra gli stessi. In quest'ottica si identifica come una forma di organizzazione gerarchica, proprio perché l'intersezione delle informazioni segue una logica di relazione diretta e di dipendenza[5]. Per questo motivo si suole definire in dottrina come un rapporto tra

---

[3] ELMASTRI RAMIREZ – NAVATHE SHAMKANT, *Sistemi di base di dati. Fondamenti*, Milano, 2007, 46.
[4] ELMASTRI RAMIREZ – NAVATHE SHAMKANT, *Sistemi di base di dati* , cit., 135.
[5] GAMBOTTO MANZONE –CONSOLINI, *Matematica con applicazioni informatiche*, Milano, 1991, 443.

dato primario e dati secondari, in un legame che interfaccia sempre una singola informazione con più informazioni *id est* in una relazione uno a molti[6]. In altre parole l'organizzazione gerarchica della banca dati segue uno schema ad albero, che parte sempre dal riconoscimento di una informazione principale dalla quale far discendere a cascata tutte le altre.

E' evidente come siffatta costruzione si ponga in antitesi con una gestione dinamica del *database* inteso come flusso continuo di dati in entrata. Infatti risulta alquanto complesso pensare ad una nuova organizzazione gerarchica strutturata secondo la scansione suesposta ogniqualvolta si interponga una qualsiasi trasformazione dell'equilibrio raggiunto dall'organizzazione delle informazioni.

In tal senso le innovazioni tecnologiche intervenute nel corso degli anni hanno implementato nuovi schemi di *database* incentrati sull'idea di un rapporto meno "ingessato" tra i dati in essi contenuti, nell'ottica di una progressiva razionalizzazione dell'utilizzo dei repertori informatici. Peraltro, come detto in precedenza, il concetto di relazione tra le informazioni è coessenziale rispetto all'idea di banca dati organizzata, ed è proprio per migliorare tale rapporto, che hanno visto la luce i modelli organizzativi c.d. reticolare e relazionale di banche dati, sicuramente più flessibili rispetto al primigenio schema gerarchico[7].

Il sistema reticolare costituisce una evoluzione del modello gerarchico, a differenza di quest'ultimo il legame tra i dati contenuti nell' archivio elettronico non è dato dal solo rapporto di subordinazione esistente tra questi ma anche da un collegamento sostanziale di carattere più generale. Invero – per utilizzare una metafora tratta dalla stessa denominazione del modello logico – l'organizzazione delle notizie passa da una rappresentazione ad albero ad una a rete, tale da generare un rapporto "da molti a molti" . La dissomiglianza principale tra i due modelli sta proprio in quest'ultima caratteristica, nel senso che mentre nel sistema gerarchico un dato primario poteva relazionarsi solo ed esclusivamente a più dati secondari all'interno di un'unica banca dati – creando, come visto in precedenza, il c.d. sistema ad albero –, nella struttura reticolare non è escluso il rapporto di più dati primari appartenenti a banche dati differenti. Invero ciò che differenzia i due schemi suesposti è il risultato ottenibile dall'indagine delle notizie all'interno della raccolta dati, come dire che l'organizzazione gerarchica permette

[6] ALBANO – GHELI – ORSINI, *Fondamenti di base dati*, Bologna, 2005, 87.
[7] PALUMBO, *Progettare database. Modelli, metodologie e tecniche per l'analisi e la progettazione di basi di dati relazionali*, Bologna, 2009, 150.

unicamente la ricerca di informazioni direttamente legate da un rapporto di subalternità col dato primario, al contrario lo schema reticolare prescinde da relazioni siffatte e consente una consultazione dei dati appartenenti a più archivi informatici, a condizione che questi abbiano una qualsiasi relazione oggettiva con l' insieme delle informazioni contenute nei diversi *database*[8] collegati dal *network.*

In tal senso, grazie alla condivisione di alcune informazioni definite come "dati connettori", è possibile collegare due o più catene di dati primari, compresi peraltro dei relativi dati secondari subordinati.

E' evidente come tale innovazione tecnologica abbia permesso alle banche dati di allargare il proprio raggio d'azione consentendo una messa a punto di queste ultime anche nella gestione di informazioni particolarmente complesse. Invero nella successione dei due schemi si è passati da una modalità di archiviazione dati legata rigidi paradigmi oggettivi, ad un altra decisamente più dinamica caratterizzata da rapporti meno selettivi tra le varie informazioni. Va sottolineato come – posto che si rispettino i parametri caratteristici dello schema – non ci siano preclusioni oggettive di sorta rispetto all'utilizzo del modello gerarchico in situazioni legate alla gestione di dati particolari.

Il profilo caratteristico che ha contraddistinto il succedersi di programmi applicativi nel corso degli anni, è da ricercare in una più funzionale e più celere organizzazione delle informazioni da gestire.

In quest'ottica anche il modello relazionale si pone come evoluzione degli schemi logistici precedenti. A differenza di questi ultimi, tuttavia, l'organizzazione dei dati prescinde dalle relazioni oggettive, per privilegiare una sistemazione di tipo matematico. Invero se negli altri sistemi di banche dati le informazioni si legavano tra loro in virtù di un nesso sostanziale, nei *database* relazionali il rapporto tra le notizie si crea sulla base della loro organizzazione logica all'interno della banca stessa[9]. I dati contenuti in tali *database* sono suddivisi in *record,* e a loro volta ripartiti in campi; ogni campo è caratterizzato dal nome e dal tipo delle notizie che contiene, mentre i *record* sono individuati da numeri interi progressivi. *Record* e campi costituiscono le righe e le colonne di una tabella, denominata anche come "relazione" – da cui il nome *database*

[8] ALBANO – GHELI – ORSINI, *Fondamenti di base dati*, cit., 87.
[9] BENEVENTANO – BERGAMASCHI – GUERRA, *Progetto di base di dati relazionali. Lezioni ed esercizi*, Bologna, 2007, 276.

relazionale – in quanto stabilisce una vero e proprio rapporto tra i dati contenuti in ogni riga, ossia tra i campi di uno stesso *record*. La gestione di un archivio elettronico relazionale, avviene partendo dalla sistemazione delle informazioni all'interno di tabelle, seguendo le suddivisioni poc'anzi accennate, così da permettere la relazione delle notizie all'interno della stessa lista o di più tabelle tra loro. I dati vengono spogliati del loro significato per essere inseriti nella griglia di relazione, come numeri progressivi di un insieme. In quest'ottica si parla di sistemi matematici, in quanto il nesso tra le informazioni segue una dinamica dettata da modelli algoritmici.

I *software* attualmente in commercio permettono di gestire contemporaneamente più tabelle tra loro – composte da *record* e campi diversi –, in modo tale da poter operare indagini complesse sui dati, come: l'unione, l'intersezione, la divisione, la selezione, la proiezione, la congiunzione o la semplice ricerca di *record* contenuti in indici diversi[10]. In tal senso, pare evidente l'assoluta diversità tra il programma relazionale rispetto agli altri due, che ponevano il legame sostanziale esistente tra i vari dati, come fondamento logico dell'indagine effettuata negli archivi elettronici. Per le banche dati di tipo relazionale la "struttura logica" del dato – inteso come *record* y di una tabella *x* – è assolutamente indipendente da qualsiasi riferimento relativo al nome di quest'ultimo, o ad altre caratteristiche identificative dello stesso, come dire che il solo fatto di appartenere ad un indice determinato costituisce il presupposto oggettivo del legame. Tale caratteristica permette un elevata flessibilità nella consultazione dei dati a disposizione dell'intero sistema relazionale, che si riflette direttamente sulla portata dei risultati ottenibili con strumenti di ricerca di questo tipo, soprattutto in termini di celerità dell'indagine[11].

[10] BENEVENTANO – BERGAMASCHI – GUERRA, *Progetto di base di dati relazionali*, cit., 280.

[11] Anche l'ampia disponibilità di notizie a disposizione del Centro di elaborazione istituito presso la Direzione centrale della polizia criminale del Dipartimento di pubblica sicurezza, è strutturata secondo il modello organizzativo relazionale. Le informazioni contenute nel C.E.D., sono collegate tra loro nell'ambito del c.d. S.D.I. (sistema di indagine), attraverso un rapporto integrato che coinvolge le notizie provenienti da tutte le banche dati a diretta disposizione della polizia. Vedi cap. III, par. 1.1.

1.1. ***(segue) Gli archivi elettronici criminalistici***

Qualsiasi raccolta di dati personali organizzata e gestita da un *software* di riferimento, che ne disciplini modalità e dinamiche di consultazione, può costituire potenzialmente un ausilio per la polizia giudiziaria o per il pubblico ministero nell'esercizio delle attività d'indagine preliminare.

A tutt'oggi la dottrina classifica i *database* di questo tipo in due macroaree, a seconda che si tratti di banche dati nate con l'unico scopo di rappresentare strumenti d'indagine *tout court* – c.d. criminalistiche –, ovvero di un insieme di dati sorti per far fronte ad esigenze diverse da quelle emergenti nel corso di un processo penale. Vale a dire che, queste ultime possono essere utilizzate per lo svolgimento delle indagini, anche se tale scopo non rappresenta la principale finalità per la quale sono nate[12].

La differenza tra le due tipologie di *database* è teleologica, da ricercare in altre parole nella diversità di obiettivi perseguiti da ognuna di queste. Le banche dati criminalistiche svolgono una funzione assolutamente dissimile rispetto alle altre, infatti, il rapporto col processo penale costituisce il fine di una relazione esclusiva: *id est* l' unico motivo alla base dell'implementazione di simili strumenti nel nostro sistema processuale. Viceversa le altre banche dati, che potremmo definire "comuni"[13], condividono con le prime solo il fatto di essere mezzi d'indagine nelle mani dell'autorità giudiziaria, ma non il fine esclusivo legato al procedimento penale.

Rappresentano degli esempi del primo tipo di *database*: la banca dati del dna[14], il sistema A.F.I.S. per il riconoscimento delle impronte digitali, l'archivio

[12] Com' è avvenuto di recente per i dati raccolti nei tabulati telefonici, impiegati sempre più di frequente nel processo penale.

[13] Rimanendo nel campo dell'identificazione personale, va sottolineato come le caratteristiche fisiologiche o comportamentali di un individuo, rappresentano dei sistemi utilizzati da imprese pubbliche e private per controllare l'accesso alle strutture, o limitare la consultazione di alcuni documenti particolarmente importanti; a tal fine vengono create banche di dati contenenti: le caratteristiche della dinamica della firma, il segno delle labbra, la forma delle vene nella mano e nel polso, la salinità del corpo, la risposta dello scheletro ad uno stimolo fisico. Occorre sottolineare inoltre come le caratteristiche fisiche vengano utilizzate perché rispondono ad una serie di parametri importanti nelle attività di identificazione individuale come: l'universalità, l'unicità, la permanenza,la misurabilità.

[14] Vedi cap. IV.

dei parlatori per l'indagine fonetica[15], i sistemi di comparazione automatica per l'indagine balistica, la banca dati di esplosivi ed infiammabili [16].

Gli archivi informatici della criminalistica includono al loro interno dati storici immodificabili – trattasi perciò di *database* analitici – adatti, a causa di tale caratteristica, a specifiche tipologie di investigazione. In particolare alla ricerca di informazioni utili per identificare una traccia del colpevole reperita sul luogo del delitto, o a studi statistici o sociologici rivolti alla determinazione delle strategie di intervento per la prevenzione o repressione del crimine.

In un ottica più generale occorre sottolineare come la tecnologia informatica applicata al campo dell'elaborazione dei dati biologici ha progressivamente perfezionato gli strumenti classici utilizzati a tal fine, grazie soprattutto all'implementazione di nuovi *software* sempre più sofisticati. Tuttavia se per alcuni dati investigativi le nuove tecniche hanno di fatto migliorato la conservazione e l'elaborazione, per altri hanno rappresentato una assoluta novità: basti pensare alle difficoltà oggettive legate all'individuazione del profilo ricavato dalla molecola del dna, dalla scansione dell'iride e dall'impronta vocale. Per tali tipologie di informazioni l'evoluzione tecnologica è stata decisiva, in quanto ha permesso la creazione di strumenti per la materiale decodificazione del dato. La scansione della retina[17] ad esempio, può essere effettuata solo attraverso strumenti che sappiano distinguere ogni minima variazione della colorazione dell'occhio umano, e che soprattutto assegnino a queste differenze un valore alfanumerico, in modo da rappresentare una notizia particolare riconducibile solo ed esclusivamente ad un soggetto determinato. Per contro le attività eseguibili senza l'ausilio di uno scanner ottico applicato ad un *software* specifico per le analisi

[15] L'identificazione vocale utilizzata come strumento legato al riconoscimento individuale, è nata nel 1960 grazie alla creazione di un *software* specifico da parte della *texas instruments*. In tali casi il dato da confrontare può essere la pronuncia di una frase sempre uguale, oppure l'analisi di alcuni parametri legati alle caratteristiche di vocalità e pronuncia di un soggetto come il tono o la dinamica della parlata.

[16] BARBATO, *Le banche dati tecnico- scientifiche,* cit., 1659.

[17] Il riconoscimento biometrico di un soggetto, effettuato attraverso l'analisi delle caratteristiche morfologiche del bulbo oculare, rappresenta un sistema stabile e affidabile; nel senso che non esistono due iridi simili tra individui diversi, neanche tra gemelli omozigoti. A tal proposito il primo *software* in grado di riconoscere la configurazione e i dettagli oftalmici è stato *Eyedentifity 7.5* apparso nel 1985, mentre risale al 1994 la deduzione di una serie complessa di formule matematiche che ha permesso di trasformare tali caratteristiche in un dato catalogabile in modo tale da essere utilizzato nelle operazioni di identificazione.

spettrografiche, sarebbero limitate ad una descrizione del colore, ed al massimo ad una riproduzione fotografica del bulbo oculare[18].

La possibilità di associare alle generalità di un soggetto una serie di parametri morfologici individuali – a partire da eventuali segni distintivi fino ad arrivare alla determinazione delle caratteristiche biometriche come la lunghezza degli arti inferiori e superiori – amplia le informazioni sull'individuo sottoposto alle indagini, in modo tale da renderlo facilmente identificabile qualora si dovesse procedere ad una nuova ricerca dello stesso.

La natura tecnica dei *software* applicativi delle banche dati criminalistiche, rispecchia le ultime evoluzioni del modello logico relazionale[19].

In tal senso le innovazioni nel campo dei modelli logistici di gestione delle banche dati, hanno portato non pochi vantaggi rispetto alle attività di *intelligence*. Invero, la possibilità di mettere in relazione tra loro un grande numero di notizie, e altresì la contestuale opportunità di effettuare interpretazione d'informazioni sempre più complesse, ha permesso una maggiore penetrazione nell'analisi dei dati. Occorre sottolineare infatti come l'opera degli inquirenti il più delle volte non si fermi alla sola consultazione statica della singola informazione contenuta nella banca dati – per la quale peraltro il sistema di archiviazione elettronica ha dato un impulso decisivo in termini di celerità e precisione – ma si caratterizzi come un attività complessa di relazione e confronto tra tutte le possibili affinità riscontrabili fra le informazioni contenute nel *database*. Tale tipo di indagine, richiede la presenza tra gli investigatori di persone competenti, che sappiano sfruttare al meglio tutte le potenzialità che offrono i moderni programmi applicativi per *computer*. In quest'ottica, gli operatori delle banche dati vengono formati tra soggetti appartenenti alle forze di polizia attraverso attività specifiche di *training* alla presenza di tecnici che conoscono bene tutte le particolarità del *software,*. L'attività d'implementazione dei dispositivi, viene preceduta da corsi teorici di preparazione all'uso del *database*, che nei casi più complessi si articolano in periodi di affiancamento con personale esterno, in modo tale da finalizzare la preparazione attraverso dimostrazioni pratiche nel corso di attività d'indagine vera e propria[20].

---

[18]DOMINIONI, *La prova penale scientifica. Gli strumenti scientifici – tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005, 112.
[19] Vedi par. 1.
[20]AA.VV., *DNA: l'impronta che rivela*, in *Polizia moderna*, 2009, n. 6, 10.

L'operazione più comune per la quale le banche dati criminalistiche vengono chiamate in causa, è il raffronto con le informazioni rinvenute sulla scena del crimine. In situazioni siffatte il dato da ricercare nel *database* da parte dell'autorità giudiziaria costituisce una proiezione diretta della stessa notizia rinvenuta sul luogo del delitto. Tale atto d'indagine rappresenta generalmente l'abbrivio naturale dell'attività investigativa, considerato come avvenga in un momento immediatamente successivo alla commissione del reato. Le notizie rinvenibili dagli investigatori possono avere una diversa natura, appartenere cioè a soggetti sospettati della commissione del reato o essere degli elementi collegabili direttamente a oggetti impiegati a tal fine. In tal senso gli archivi elettronici criminalistici utilizzati dalla polizia giudiziaria per operare l'indagine sui reperti investigativi si differenziano – da un punto di vista sostanziale – in banche dati biologiche e merceologiche[21]. Oltre a ciò serve sottolineare come le operazioni di repertazione e conservazione dei dati svolte sulla scena del crimine, condizionano il grado di praticabilità del successivo confronto esperibile con le informazioni contenute nella banca dati; nel senso che, più sarà accurato il prelievo delle notizie, più risulterà attendibile l'esito dell' indagine sui dati detenuti dalla polizia giudiziaria.

A tal proposito pare interessante notare come la possibilità di rinvenire reperti biologici personali sul luogo del delitto accomuna, per certi versi, l'investigazione genetica a quella svolta sulle impronte digitali[22]. Invero, il processo logico che porta alla ricerca di un identità soggettiva precisa, si concretizza per ambedue le forme di indagine in un ragionamento di carattere induttivo[23], entrambe le indagini si fondano sul raffronto con le informazioni biologiche individuali, contenute nelle rispettive banche dati *id est* i profili soggettivi del dna e i tratti caratteristici individuali delle impronte digitali. Infatti, all'esito del confronto attuato dalle forze dell'ordine con i reperti rinvenuti sul luogo del delitto, l'identità di un soggetto viene data per certa nel caso in cui emerga la corrispondenza di tredici porzioni ben identificate del dna umano

[21] Si possono considerare come archivi criminalistici biologici: la banca dati del dna, il sistema di riconoscimento delle impronte digitali A.F.I.S., l'archivio dei parlatori per l'indagine fonetica; viceversa i sistemi di comparazione automatica per l'indagine balistica e la banca dati di esplosivi ed infiammabili costituiscono *database* merceologici.
[22] SPINELLA – SOLLA, *L'identificazione personale nell'investigazione scientifica: DNA e impronte digitali*, in *Cass. pen.*, 2009, 431.
[23] CHERUBINI, *Fallacie nel ragionamento probatorio*, in *La prova scientifica nel processo penale*, a cura di DE CATALDO NEUBURGER, Padova, 2007, 273.

(profilo identificativo genetico)[24] o nel caso in cui risulti l'identità di diciassette tratti caratteristici delle impronte digitali[25]. Ciò detto, si può affermare come, le leggi scientifiche che individuano l'identità di alcuni dati biologici personali – molecola del dna e delle impronte digitali – alla stregua di elementi distintivi utili per riconoscere un individuo, rappresentano la premessa maggiore del sillogismo, sul quale si fonda l' opera degli inquirenti. Di conseguenza l'attività di mero confronto, realizzata grazie all'ausilio della banca dati, costruisce la conclusione necessaria del ragionamento logico deduttivo rivolto all'identificazione del sospettato.

L'eventuale assonanza tra le informazioni confrontate con l'ausilio della banca dati da parte degli inquirenti offre un elemento di prova che, per la sua stessa natura, non può rappresentare in modo diretto il fatto illecito. Invero, l'affermare con assoluta certezza che un soggetto risponda a generalità determinate in relazione alla compatibilità delle proprie impronte digitali con quelle detenute dagli inquirenti negli archivi segnaletici, garantisce una base investigativa inequivocabile e scientificamente solida, ma che solo indirettamente e attraverso l'ausilio di massime d'esperienza può condurre ad una eventuale ricostruzione del fatto reato[26].

In quest'ottica occorre sottolineare come il dato rinvenuto grazie all'aiuto degli archivi elettronici necessiti di una contestualizzazione all'interno della trama accusatoria, attraverso la creazione di legami oggettivi con altri elementi investigativi che ne rafforzino il senso. Da ciò si evince la natura indiziaria di tale elemento di prova, e di conseguenza l'applicabilità della disciplina prevista dalla regola generale contenuta nella lettera nell'art. 192 c.p.p. . Per questo motivo anche il risultato dell' indagine condotta sui dati fissati negli archivi elettronici, impone la presenza di una pluralità di elementi convergenti – gravi precisi e concordanti – tali da permettere la valutazione della prova logica da parte del giudice.

Si pensi alla traccia biologica rinvenuta sul luogo del delitto; in tal caso una possibile identificazione del soggetto grazie alla corrispondenza del profilo genetico di quest'ultimo con quello repertato sulla scena del crimine, non costituisce da sola un elemento sufficiente per riconoscerne la colpevolezza. La

[24] Vedi, par. 3.
[25] Vedi, par. 2.
[26] UBERTIS, *La conoscenza del fatto nel processo penale*, Milano, 1990, 133.

natura indiziaria di tale informazione, deriva dal fatto che l'esegesi esperibile in tali casi non può andare al di là della chiarezza riflessa dal dato, ovvero oltre la considerazione della presenza in un certo luogo del soggetto individuato grazie alla banca dati criminalistica.

2. *Le impronte digitali*

Le forze di pubblica sicurezza utilizzano da oltre un secolo la catalogazione delle particolarità biologiche distintive di un soggetto per accertarne l'identità. La prima caratteristica fisica impiegata a tal fine è stata la misurazione degli arti, attraverso un sistema identificativo noto come antropometria[27]. La classificazione biometrica veniva impiegata per associare caratteristiche fisiche di facile reperibilità alle generalità di un individuo, in modo tale da confermarne l'identità al di là dei riferimenti anagrafici. A tal proposito si può considerare come tale sistema non rappresenti un tratto distintivo autonomo; vale a dire, in grado di qualificare l'identità di un soggetto in modo svincolato da altri parametri identificativi, dato che costituisce una informazione *ad abundantiam*, mediante la quale gli inquirenti impiegati nella ricerca di un soggetto particolare o nell'identificazione di un sospettato, possono confermare il risultato ottenuto attraverso altri canali investigativi.

Un significativo passo avanti in tema d'identificazione è avvenuto con lo studio delle impronte digitali[28]. Tale caratteristica fisica contraddistingue un individuo fin dalla nascita, in quanto la fase originaria delle impronte ha inizio verso il terzo mese di vita intrauterina e prosegue durante la gestazione, in questo lasso di tempo gli arti presentano dei rigonfiamenti detti *volar pads,* che

[27]Col sistema di riconoscimento antropometrico si identificavano i criminali misurando la lunghezza del braccio e delle dita, l'altezza la larghezza della testa e la lunghezza dei piedi. Tali misurazioni avevano un certo grado di attendibilità in quanto l'ossatura umana non si modifica più dal ventesimo anno d'età, e in considerazione del fatto che ogni scheletro umano è differente. RICCI – PREVIDERÈ – FATTORINI - CORRADI, *La prova del DNA per la ricerca della verità,* cit. , 21.

[28]Fin dal secondo secolo a.c., in Cina veniva utilizzata l'impronta digitale fissata su sigilli di cera come segno di riconoscimento da imprimere su documenti importanti. ARCUDI – MONTANARO, *La identificazione del vivente e le impronte digitali,* in *Trattato di medicina legale e scienze affini II*, diretto da GIUSTI, Padova, 1998, 46.

regredendo contribuiscono alla formazione della figura generale e dei relativi punti identificativi[29].

In Italia fu lo scienziato Gasti, brillante funzionario di polizia, a istituire il sistema deca dattiloscopico, basato sulla classificazione numerica – da 0 a 9 – delle impronte digitali. Tale sistema permise l'apertura nel nostro paese del servizio di segnalamento e identificazione avvenuto nell' agosto del 1906[30]. A tutt'oggi il raffronto delle impronte digitali costituisce ancora un valido strumento nelle mani degli investigatori – sia in chiave preventiva che giudiziaria –, anche se va segnalato come l'innovazione tecnologica ne abbia condizionato in modo diretto tutte le fasi. Per quanto riguarda la repertazione, si è passati dall'inchiostrazione delle dita e successiva digitazione su appositi cartoncini segnaletici, alla scannerizzazione fatta direttamente su processori multimediali *ad hoc*; allo stesso modo, le attività di conservazione e confronto sono gestite da sistemi computerizzati di catalogazione di tipo relazionale.[31] Peraltro, seguendo una procedura oramai consolidata, ogniqualvolta si deve operare un indagine delle tracce digitali, i dattiloscopisti ricavano dall'impronta la figura generale in relazione all'andamento delle creste papillari – che può essere: adelta, modelta, bidelta e composta – successivamente esaminano la presenza delle *minutiae*, i punti caratteristici identificativi, presenti allorquando il decorso naturale della linea papillare subisce delle variazioni. Siffatta verifica assume una rilevante importanza in ambito giudiziario, in quanto i giudici della suprema corte considerano una legge scientifica attendibile il riferimento alla corrispondenza tra le due impronte confrontate di un numero minimo minuzie caratteristiche, come parametro utile per un giudizio d'identità dattiloscopica[32]. Tale assioma

[29] ARCUDI – MONTANARO, *La identificazione del vivente e le impronte digitali*, cit., 25.

[30] Il sistema del Gasti partiva dal presupposto che l'impronta lasciata da ogni singolo dito potesse essere ricondotta ad una forma caratteristica di appartenenza – fino a nove differenti tra loro – dedotta dalla particolare conformazione delle creste papillari. Tale indicazione ripetuta per tutte le dita della mano, forniva un vero e proprio profilo identificativo caratteristico soggettivo. ARCUDI – MONTANARO, *La identificazione del vivente e le impronte digitali* , cit., 46.

[31] Vedi par. 1.

[32] Ad avviso della giurisprudenza, "le risultanze delle indagini dattiloscopiche offrono piena garanzia di attendibilità senza bisogno di ulteriori elementi sussidiari di conferma,anche quando riflettano una sola impronta purché evidenzino la sussistenza di almeno sedici punti caratteristici uguali per forma o posizione." Cass., sez. II, 5 luglio 1985, Solla, in *Cass. pen.*, 1987,171; Altre sentenze hanno richiesto la sussistenza di sedici o diciassette punti di convergenza. Cass., sez. II, 2 marzo 1983, Mattolini, in *ivi*, 1984, 2248; In un caso la cassazione ha ritenuto sufficiente a provare l'identificazione

rappresenta il risultato degli studi compiuti in campo dattiloscopico in base ai quali, non può esistere una corrispondenza numerica dei tratti caratteristici di un impronta digitale in due soggetti distinti. Di conseguenza l'identità numerica genera una valutazione di assoluta certezza sull'identità del soggetto nei confronti del quale viene riscontrata[33]. Inoltre la scoperta dei tratti distintivi delle creste cutanee papillari può essere considerata come l'archetipo di una nuova forma d'indagine; *id est* l'investigazione sulla scena del crimine. A tal proposito, la predisposizione di archivi segnaletici[34] in chiave preventiva contenenti le impronte di soggetti indagati – presso gli uffici di polizia giudiziaria –, permette lo svolgimento di indagini finalizzate alla ricerca della corrispondenza di queste con i segni digitali reperiti sul luogo del delitto[35].

Peraltro la dottrina è concorde nel ritenere come un'eventuale giudizio identificativo operato sulla base delle impronte digitali dovrebbe tenere in debita considerazione oltre ad un fondamento numerico, ovvero di una soglia minima di punti da raggiungere, anche di un sistema qualitativo d' interpretazione[36]. Invero l'eventuale presenza di accidentalità, quali ad esempio cicatrici profonde, contribuisce ad un'analisi qualitativa non di poco conto sull'impronta stessa, in tali casi viene infatti fornita un'informazione supplementare a carico di eventuali giudizi d'identità espressi, specie sui frammenti papillari.

Pertanto, allorché venisse riscontrata sull'impronta digitale la presenza di una rara figura, oppure l'esistenza di uno sfregio o una minuzia insolita, pare

---

dell'indagato l'esistenza di almeno quattordici punti d'identità. Cass., sez. II, 29 marzo 1982, Mistioni, in *ivi*, 1983, 2063.

[33]In senso contrario va segnalata la posizione dell' INTERPOL e dell'A.I.A. (*associazione per l'identificazione Americana*) che nel 1973, a seguito di un'indagine statistica, ha rilevato come non esista alcuna base valida per richiedere un numero minimo di punti corrispondenti tra due figure papillari per giungere ad una valutazione che riguardi il riconoscimento di un soggetto. Sulla scorta di queste affermazioni nei paesi anglosassoni, contrariamente a quanto avviene in Italia, manca una soglia minima di punti utili all'attribuzione di un giudizio d'identità. *Interpol European Export Group in Fingerprint Identification, Method for fingerprint identification*, in www.interpol.int/public/forensic/fingerprnts/working; SPINELLA – SOLLA, *L'identificazione personale nell'investigazione scientifica* , cit. , 433.

[34] L'impronta digitale permette l'identificazione di un soggetto grazie al fatto che quest'ultima è unica – nel senso che la probabilità di trovare due impronte digitali coincidenti, anche tra gemelli omozigoti, è praticamente nulla – e non è soggetta a mutazione nel tempo, a meno che non ci sia un cambiamento dovuto a cause innaturali come ad esempio scottature o incidenti.

[35]BOLINO – GRANDE, *L' identificazione individuale mediante la metodica di rilievo dattiloscopico F.I.T.* (Fingerprint identification technology), in *Arch. med. leg. ass.*, 1994, 273.

[36] TONINI, *Prova scientifica e contraddittorio*, in *Dir. pen. proc*., 2003, 1460.

logico pensare come l'operatore non abbia bisogno di raggiungere la soglia minima di punti caratteristici per l'attribuzione dell' identità al soggetto. In tali casi sarà sufficiente la redazione di una relazione tecnica argomentata, che puntualizzi il riferimento alle caratteristiche particolari della traccia

2.1 ***(segue) Il sistema A.F.I.S.***

Tra le banche dati criminalistiche attualmente in uso da parte della polizia giudiziaria, riveste una particolare importanza il sistema di riconoscimento delle impronte digitale A.F.I.S. . L'impiego di tale banca dati è sostanzialmente duplice, rivolto cioè ad un uso di carattere preventivo di pubblica sicurezza e di ricerca in ambito giudiziario[37].

Il sistema operativo acquisisce e registra i cartellini foto segnaletici e le impronte digitali prodotti dalle forze di polizia nel corso delle attività deputate all'identificazione del soggetto arrestato o fermato. Le impronte vengono conservate in una sezione del sistema operativo dedicata – c.d. *database* cartellini – che include tutti i dati provenienti dagli operatori della polizia giudiziaria e – tramite *INTERPOL* – dalle forze di polizia straniere[38].

A tutt'oggi il *database* A.F.I.S. contiene i riferimenti digitali di oltre sette milioni di individui, quest'ultimo viene alimentato da qualsiasi punto si disponga di un lettore di impronte, quindi nei luoghi stessi in cui le forze dell'ordine effettuano i controlli; *id est* da una volante, in aeroporto, sui treni o alle frontiere[39]. Il *software* implementato in Italia è lo stesso utilizzato dal sistema operativo EURODAC per il controllo dell'immigrazione e dall'FBI americana[40]. Tale caratteristica consente ai diversi sistemi di colloquiare tra loro in modo immediato, facilitando la cooperazione internazionale in campo investigativo[41].

---

[37] BARBATO, *Le banche dati tecnico- scientifiche* , cit. , 1663.
[38] RICCI – PREVIDERÈ – FATTORINI - CORRADI, *La prova del DNA per la ricerca della verità. Aspetti giuridici biologici e probabilistici*, Milano, 2006, 19
[39] BARBATO, *Le banche dati tecnico- scientifiche,* cit. , 1660.
[40] RICCI – PREVIDERÈ – FATTORINI - CORRADI, *La prova del DNA per la ricerca della verità. Aspetti giuridici biologici e probabilistici*, cit., 21.
[41] GANDINI, *Il Trattato di Prum articolo per articolo ecco le nuove frontiere per la sicurezza. Banche dati antiterrorismo e interventi congiunti in sette stati UE*, in *Dir. giust.*, 2006, n. 37, 60.

Peraltro, occorre notare come oltre a rappresentare un elemento necessario per qualificare l'identità di un soggetto, la raccolta delle tracce digitali è funzionale rispetto alla verifica dell'eventuale coinvolgimento dello stesso in fatti criminosi antecedenti. L'attività di controllo, sui possibili precedenti del sospettato, segue una serie di passaggi di carattere tecnico caratterizzati da una sequenza di operazioni poste in essere al fine di ottenere un risposta finale dal sistema operativo. A tal proposito, la scheda segnaletica – una volta creata – viene scansionata[42] ed inviata telematicamente al gabinetto scientifico della polizia di Stato, ovvero al reparto di dattiloscopia preventiva dei carabinieri, qui il dattilo scopista realizza il controllo di qualità sulle impronte, in modo tale da iniziare l'attività di ricerca nel *database*. L'attività di ricognizione si conclude nel giro di pochissimi minuti, all'esito della ricerca telematica lo stesso archivio elettronico proporrà una serie di candidati compatibili con i dati inseriti dall'operatore, concludendo così l'accertamento tecnico con un responso che può essere negativo oppure positivo.

L'esito negativo della verifica implica che il soggetto sottoposto ai rilievi non è stato foto segnalato in precedenza, viceversa l'esito positivo evidenzia la presenza – negli archivi della polizia giudiziaria – delle informazioni relative al sospettato. In tali casi, contestualmente ai dati di diretto interesse per gli investigatori, il *database* fornisce una ulteriore serie di elementi utili alle indagini come ad esempio la data dei rilievi già effettuati nel corso della segnalazione antecedente, il reparto segnalante e il motivo della comunicazione.

L'utilizzazione in ambito giudiziario del sistema operativo A.F.I.S., presuppone la repertazione sulla scena del crimine di un frammento papillare – digitale o palmare – appartenente ad un soggetto sconosciuto alle forze dell'ordine. Qualora si verifichi una situazione di questo tipo, gli inquirenti hanno la possibilità di rinvenire il nome del soggetto al quale la traccia appartiene, grazie all'ausilio dei repertori conservati nell' archivio elettronico delle impronte digitali.

La prima operazione da porre in essere in situazioni siffatte consiste nella scansione del supporto adesivo utilizzato per asportare la traccia dal luogo del delitto, in modo tale da ricavare un impronta digitale potenzialmente riconducibile all'autore del reato.

[42] Esiste anche un metodo di rilevazione ottico dell'impronta digitale, effettuato attraverso il contatto diretto del polpastrello con un prisma di vetro, che ritrae l'immagine dell'impronta conservandola direttamente nel *database*.

Una volta ottenuto il dato da confrontare con le informazioni contenute nella banca dati, gli operatori sono in grado di realizzare il raffronto telematico. All'esito della ricerca il *software* produce, in pochissimi minuti, la lista segnaletica del soggetto ricercato. Tuttavia, come rimarcato in precedenza, tale indagine permette di risalire al nominativo del sospettato solo nel caso in cui questi in passato sia entrato in contatto con le forze dell'ordine e le sue impronte digitali siano censite in banca dati. Qualora il raffronto non dia alcun esito il frammento papillare rinvenuto sulla scena del crimine verrà conservato comunque nella banca dati in una ripartizione speciale denominata *database* frammenti, che contiene tutte le impronte repertate sui luoghi di commissione di reati, ma non ancora attribuite a nessuno.

E' necessario evidenziare in ultima analisi come sino alla metà degli anni novanta l'impiego delle impronte digitali in campo giudiziario era condizionato dall'assenza di sistemi operativi in grado di operare un confronto immediato e a largo raggio come quello attuabile a tutt'oggi grazie al sistema di riconoscimento A.F.I.S. , nel senso che mancava di fatto lo strumento necessario per porre in essere una comparazione veloce con i milioni di cartellini segnaletici presenti negli schedari nazionali. Nel caso in cui gli inquirenti avessero rinvenuto sulla scena del crimine un frammento papillare, le indagini su tale dato procedevano attraverso il confronto diretto di quest'ultimo con una serie di cartellini segnaletici recanti le impronte digitali di soggetti già schedati in precedenza dalla polizia giudiziaria, scelte dagli investigatori, tra quelle appartenenti a soggetti potenzialmente riconducibili alla commissione del reato.

3. ***L'identificazione genetica***

Nel corso degli ultimi vent'anni l' attenzione degli operatori del processo penale – biologi, genetisti e autorità inquirenti – si è focalizzata sull' esame delle peculiarità genetiche della molecola del dna, in particolare sullo studio di alcune parti di questa, da utilizzare per l' identificazione degli individui[43].

[43]GAROFANO, *Genetica identificativa e biobanche: aspetti tecnici e problematiche connesse*, in *Dir.pen.proc. dossier*, *La prova scientifica nel processo penale*, a cura di TONINI, 2007, 44; DOMENICI, *Prova del DNA*, in *Dig.disc.pen.*, Torino, 1997, 373.

Per definire in modo chiaro il concetto di identificazione genetica, occorre partire dalla nozione di unicità del dna[44]. La possibilità di poter parlare di singolarità allorché ci si riferisca ad una molecola di acido desossiribonucleico, deriva dal fatto che la composizione della cellula madre dalla quale nasce e si sviluppa un individuo scaturisce dall'incontro del patrimonio genetico ereditato dai genitori. In tal senso, la composizione del nucleo cellulare fatta di quarantasei cromosomi – ventidue coppie comuni a maschi e femmine, più due cosiddetti cromosomi sessuali (xy nei maschi e xx nelle femmine) – deriva dall' apporto diviso in egual misura dal padre e dalla madre di un determinato soggetto[45].

Una molecola di dna consiste in due lunghe catene polinucleotidiche collegate tra loro da un legame di idrogeno, i singoli nucleotidi – anelli della catena – sono formati da due delle basi azotate caratteristiche della molecola – adenina, citosina, guanina, timina – che si appaiano tra loro sempre allo stesso modo[46]. Tale specificità costituisce il presupposto biologico sul quale si fonda il c.d. processo di replicazione del dna; *id est* il passaggio del medesimo patrimonio genetico da una cellula all'altra del corpo umano. Quando una cellula si divide, tutto il dna si duplica, cosicché ogni cellula figlia eredita una copia identica alla cellula madre[47].

In quest'ottica la separazione – c.d. denaturazione – e successiva ricomposizione della catena nucleotidica deriva dal rapporto speculare che regola l'accoppiamento tra le basi azotate, per cui diviene impossibile l'eventuale confusione di legami biochimici, in quanto questi rispondono per la loro collocazione a "relazioni prestabilite". In tal modo la trasposizione della stessa molecola in ogni cellula del corpo umano, è possibile in virtù di questa relazione lineare tra le sue componenti chimiche.

Siffatta funzionalità reciproca costituisce la base del concetto di ereditarietà di un carattere, che viene trasmesso per generazioni e perpetrato nel tempo. Inoltre il fenomeno della duplicazione del dna spiega il motivo per cui ogni cellula di uno stesso individuo contiene il medesimo dna e chiarisce perché

[44] La molecola del dna è stata scoperta dal biologo inglese Francis Crick e dal biochimico americano James Watson nel 1953.
[45] AA.VV., *Biologia molecolare della cellula*, Bologna, 2000, 204.
[46] Per questo motivo avremo continuamente la base di adenina collegata a quella di timina e quella di citosina legata alla guanina, in una successione che in biologia viene definita come complementare.
[47] AA.VV., *Biochimica*, Bologna, 2003, 300.

sia possibile, ai fini identificativi, comparare il profilo genetico ricavato da tessuti diversi come una traccia di saliva e il sangue del sospettato. Si tratta tra l'altro, di un informazione eccezionalmente stabile, a dimostrazione dell'efficienza del meccanismo che vi sovrintende[48].

Ogni sezione di dna in grado di fornire informazioni sulla costruzione di una proteina è denominata in biologia molecolare[49] "gene", quest'ultimo a sua volta si caratterizza per essere formato da una parte codificante detta "esone" e una non codificante detta "introne"[50]. Inoltre, viene definito "allele" una delle due o più forme alternative di un gene riscontrabili in soggetti diversi[51].

Invero, posto che la costruzione della molecola del dna risulta identica da individuo a individuo – con riferimento al numero di cromosomi e alla dislocazione dei vari geni sulla struttura polinicleotidica –, si possono riscontrare delle differenze nella composizione genetica della singola porzione di dna, in ragione di tale modificabilità si parla di polimorfismo[52] come caratteristica propria di alcune zone[53] particolarmente soggette a differenze strutturali. I genetisti forensi sono particolarmente interessati a quelle porzioni del dna che presentano variazioni tra individui localizzate al di fuori delle sequenze codificanti, peraltro gli alleli impiegati dagli inquirenti nelle operazioni di identificazione si trovano nelle parti introniche del dna – c.d. *junk* dna –, tali sezioni costituiscono le zone polimorfiche più importanti utilizzate a fini identificativi[54]. Occorre sottolineare inoltre come tale scelta è dettata, oltreché dall'altissimo grado di variabilità che contraddistingue questi tratti particolari della molecola, dal fatto che, con l'indagine attuata attraverso profili identificativi tipizzati da parti non codificanti del dna, risulta maggiormente garantito il diritto alla *privacy* genetica. Infatti Le zone introniche, non contengono informazioni particolari, per tal motivo possono

[48] AA.VV., *Biologia molecolare*, cit. , 204.

[49] La biologia molecolare e quella branca della genetica che studia la molecola del dna, ne analizza la forma e le possibili trasformazioni attraverso le operazioni di c.d. ingegneria genetica.

[50] Solo il cinque per cento dell'intero dna umano è costituito da sequenze codificanti, viceversa sono praticamente sconosciute le funzioni delle altre componenti geniche.

[51] LEWIN, *Il gene*, Milano, 1999, 142.

[52] CAVALLI SFORZA– MENOZZI –PIAZZA, *Storia e geografia dei geni umani*, Milano, 2000, 188.

[53] FIORI, *I polimorfismi del DNA nuove frontiere e problemi del laboratorio medico – legale*, in *Riv.it.med.leg.*, 1988, 399.

[54] RICCI – PREVIDERÈ – FATTORINI - CORRADI, *La prova del DNA per la ricerca della verità*, cit. , 71.

essere conservate nelle banche dati senza alcun pericolo di *discovery* genetica di dati sensibili[55].

A tal proposito, per determinare quelli che nei laboratori di genetica forense vengono definiti come marcatori – in virtù dell'alto grado di variabilità – si fa riferimento ai c.d. studi di popolazione, in base ai quali viene calcolata la possibilità di ripetizione di una certa sequenza di dna nell'ambito di una popolazione di riferimento[56]. Tale calcolo statistico costituisce il nesso principale in mano ai biologi per stabilire il livello di reiterazione proprio di ogni dato genetico, e di conseguenza un parametro oggettivo certo per identificare quali porzioni del dna possono essere utilizzate per l'individuazione di un soggetto. Invero, l'utilizzo di alcuni tratti della molecola in funzione identificativa segue la logica del livello di variabilità della stessa[57].

Nello specifico, i *locus* della molecola utilizzati in genetica forense per la catalogazione nelle banche dati sono definiti come c.d polimorfismi di lunghezza. In particolare vengono utilizzati i c.d. STR, acronimo inglese traducibile in italiano come sequenze ripetute in tandem. Tale definizione chiarisce la caratteristica fondamentale di queste porzioni di dna nucleare, ovvero la ripetizione in coppia di brevi sequenze delle singole basi azotate caratteristiche della composizione del dna. Per cui avremo due o più basi di adenina, citosina, timina o guanina che si reiterano, tali da creare la differente lunghezza di ripetizioni rilevabili tra gli individui, che di fatto generano il marcatore genetico.

In passato uno dei più grossi problemi col quale si sono dovuti confrontare i biologi impegnati in indagini penali, è stato la scarsità di materiale biologico da analizzare, necessario per porre in essere le pratiche identificative. Questo limite ha inciso negativamente anche sulla creazione di archivi elettronici del dna.

Tale attività, infatti, è possibile soltanto nel momento in cui diventa agevole individuare – e di conseguenza archiviare – il dna di un sospettato o repertare profili genetici sulla scena del crimine, in quanto solo la disponibilità massiccia di dati permette un confronto su larga scala, così com'è da intendere quello posto in essere attraverso l'ausilio dei *database* genetici.

---

[55] Vedi cap. IV.

[56] RICCI – PREVIDERÈ – FATTORINI - CORRADI, *La prova del DNA per la ricerca della verità*,cit. , 211.

[57] BARBATO – CORRADI – LAGO, *L' identificazione personale tramite Dna*, in *Dir. proc. pen.*, 1999, 216.

A tal proposito, a metà degli anni ottanta alcuni ricercatori di una compagnia americana hanno sviluppato una metodica di laboratorio finalizzata alla moltiplicazione del materiale genetico. La tecnica conosciuta come PCR, sfrutta le caratteristiche proprie della molecola del dna – in particolare il principio di complementarietà – per ottenerne la replicazione[58]. Invero a tutt'oggi grazie a tale metodo, è possibile riprodurre le sezioni di dna che interessano per l'identificazione genetica a fini investigativi in milioni di copie anche da piccolissime quantità di materiale biologico[59].

La replicazione si ottiene grazie alla successione di una serie di azioni, che ripetute nel giro di poco tempo – cicli – consentono la produzione di un numero elevatissimo di molecole del dna[60].

Va sottolineato come tale replicazione riguardi solo i tratti di dna che il genetista è interessato a ispezionare. Questa considerazione proiettata nella dinamica delle indagini genetiche a scopo forense, assume particolare importanza, considerato come l'attenzione degli investigatori si polarizza su alcune zone circoscritte della catena polinucleotidica, caratteristiche per effettuare le operazioni di identificazione soggettiva.

Prima dell'avvento della PCR – che ha permesso l'implementazione a livello mondiale di sistemi di catalogazione e conservazione del genoma umano – l'indagine genetica non veniva effettuata in modo estensivo. Invero la comparazione del dna era limitata a pochi casi particolarmente complessi o di interesse pubblico. In quest'ottica i laboratori della polizia confrontavano il materiale genetico rinvenuto nella scena del crimine con quello estratto dai soggetti sospettati di un determinato reato, confinando in tal modo ad una cerchia limitata di individui l'attività di raffronto. Per contro, il miglioramento continuo delle tecniche dei laboratori di biologia molecolare – che ormai permette l'estrazione di dna da una vasta serie di campioni di materiale genetico anche in stato di decomposizione o in condizioni di conservazione precaria – col conseguente avvento di sistemi computerizzati in grado di contenere un numero elevatissimo di profili genetici, ha permesso una espansione di una nuova forma di investigazione, attraverso l'uso massiccio della banca dati del dna. Tale

[58] POLI, *Biotecnologie, principi e applicazioni dell'ingegneria genetica*, Torino, 2000, 41.
[59] La quota di dna richiesta per la PCR è veramente piccola : nei normali esperimenti di laboratorio è sufficiente una quantità inferiore ad un microgrammo.
[60] POLI , *Biotecnologie,* cit. , 47.

strumento permette infatti di confrontare in contemporanea un profilo genetico del quale non si sa niente con tutti quelli contenuti al suo interno, e di rilevare una corrispondenza, qualora esista.

In particolare, il dato che noi conosciamo come tale e che individua il profilo genetico di ogni soggetto catalogato nei *database* è composto da una serie di numeri, una sorta di codice a barre identificativo; siffatta traduzione in cifre è possibile grazie ad una procedura utilizzata nei laboratori di biologia molecolare chiamata elettroforesi[61]. Tale metodica consiste in una vera e propria misurazione, fatta utilizzando un principio elementare della fisica elettronica, in base al quale un oggetto caricato positivamente viene attratto da un campo magnetico caratterizzato da una carica elettronica di segno opposto. Infatti il dna, estratto e amplificato in milioni di copie, viene caricato elettronicamente con ioni positivi e collocato su un gel di una sostanza c.d. agarosio che ne permette il movimento. Posto successivamente su una base con un polo negativo e uno positivo, il dna tende a muoversi – attratto elettronicamente – verso il primo. In tal modo l'intensità dello spostamento – misurato grazie ad una scala numerica posta sul lato della base – esprime in cifre il valore della molecola[62].

Pertanto – facendo riferimento ai tratti di dna utilizzato per l'identificazione forense – più sarà cospicuo il numero di STR, *id est* di ripetizione delle basi azotate per quella porzione di molecola, più sarà lento – perciò caratterizzato da un numero basso – lo spostamento elettronico. Viceversa un ridotto numero di ripetizione si ripercuote sul peso del dna, permettendone uno spostamento più rapido e quindi l'espressione di un valore numerico alto.

[61] GLICK – PASTERNAK, *Biotecnologia molecolare, principi e applicazioni del DNA ricombinante*, Bologna, 2001, 7.
[62] POLI, *Biotecnologie,* cit. , 47.

CAPITOLO SECONDO

PROTEZIONE E TUTELA DEI DATI INDIVIDUALI

1) Dalle banche dati al diritto all'autodeterminazione dei dati personali

La tecnologia informatica nel campo dei *database* ha raggiunto ormai un grado di evoluzione tale da garantire alle parti del processo penale informazioni di ogni tipo. Nel corso della fase dell'istruttoria dibattimentale la trasposizione dell'elemento d'indagine – dato catalogato nella banca – in mezzo di prova, può avvenire in due modi distinti: attraverso la prova documentale – documento che riproduce l'informazione utilizzabile – o la prova tecnica: *id est* perizia, ovvero consulenza tecnica.

La differente modalità di acquisizione del dato è legata al grado di autonoma rappresentatività di quest'ultimo. In quest'ottica, sarà necessaria l'opera di un esperto ogniqualvolta il dato personale richieda, per essere decodificato, un'azione estrinseca, in modo da realizzare la corretta interpretazione dell'informazione[63]. Costituisce un esempio di quest'ultima ipotesi, l'interpretazione del profilo identificativo contenuto nella banca dati del dna[64].

In tali situazioni l'intervento di un biologo in grado di condurre l'intera indagine genetica è indispensabile per la riuscita stessa dell'investigazione, in quanto senza l'intervento del genetista il giudice, nel corso del processo, si troverebbe a disposizione, tra gli atti del fascicolo del dibattimento, un dato indecifrabile e incomprensibile qual è un codice alfanumerico, rispondente ad un tratto ben preciso del dna, da confrontare con un'altra prova recante un dato dello

[63] L'intervento di un ausiliare esterno può essere legato anche alla comprensione linguistica del dato personale, espresso in lingua straniera. In tali casi l'intervento chiarificatore del senso dell'informazione spetterà ad un traduttore nominato dal giudice, secondo quanto previsto dal primo comma dell'art. 143 c.p.p. , che prevede la nomina di un esperto ogniqualvolta sia necessario tradurre documenti trascritti in lingua straniera.
[64] FANUELE, *Dati genetici e procedimento penale*, Padova, 2009, 21.

stesso tipo e appartenente ad una persona diversa[65]. E' ovvio come in tali casi il lavoro dell'ausiliare tecnico vada ben al di là di un chiarimento sul contenuto del documento, ma si traduca nell'attività tecnico interpretativa, tipica della perizia o della consulenza tecnica.

Diverso è il discorso in relazione alle operazioni di analisi dei dati nel corso delle indagini preliminari. In tali casi l'approccio del pubblico ministero o della polizia giudiziaria cambia, a seconda che le banche dati di raccolta dei dati personali siano a disposizione diretta dell'autorità giudiziaria o collocate presso soggetti terzi.

Nella prima ipotesi la ricerca del dato impone la presenza di un soggetto preparato all'uso delle banche dati elettroniche che sia, cioè, in grado di ottenere le informazioni ricercate in modo corretto e nel più breve tempo possibile. Invero, per gli inquirenti, l'approccio iniziale con la banca dati passa sempre attraverso una ricerca computerizzata, la quale presuppone una conoscenza dettagliata del sistema logistico utilizzato dall'archivio oggetto della consultazione. Questa considerazione suggerisce la necessità dell'intervento di un esperto – quantomeno per la "gestione operativa" della banca dati criminalistica – capace di riprogrammare i *software* allo scopo di ottenere un miglioramento delle caratteristiche tecniche degli elaboratori dei dati, in linea con le nuove scoperte tecnologiche in campo informatico.

Il ragionamento muta in tutte quelle situazioni in cui l'autorità giudiziaria non ha una diretta disponibilità degli archivi elettronici da utilizzare e deve iniziare un'indagine sui dati contenuti in questi ultimi. In tali contesti l'organo inquirente, procederà al sequestro dei documenti relativi ai dati necessari per le indagini presso il soggetto detentore della banca di raccolta delle informazioni, o reperirà le notizie a sua insaputa – nel caso in cui sia necessario farlo in segreto – per garantire la riuscita delle indagini: ad esempio, attraverso operazioni di intercettazione telematica dei flussi di informazioni o altri mezzi atipici di ricerca della prova[66].

Il fatto di poter confrontare notizie personali diverse, ma soprattutto la possibilità di disporre dei mezzi di ricerca per carpire e conservare queste ultime

[65] FANUELE, *Dati genetici e procedimento penale,*cit. , 26.

[66] In relazione all'applicabilità della disciplina prevista dall'art. 189 c.p.p. anche ai mezzi di ricerca della prova atipici vedi; D.SIRACUSANO, *Le prove*, in D.SIRACUSANO - GALATI - TRANCHINA – ZAPPALÀ, *Diritto processuale penale*, Milano, 2004.

con estrema facilità, ha indubbiamente rappresentato un argomento a favore nell'implementazione di archivi elettronici criminalistici o dell'impiego di strumenti investigativi nuovi per sottrarre informazioni dalle banche dati "comuni". L'utilizzo che l'autorità giudiziaria fa nel corso delle indagini preliminari di tali elementi di prova, è direttamente proporzionale al numero e alla tipologia di notizie potenzialmente ricavabili dall'interpretazione dei *database*; nel senso che l'uso di *databases* – criminalistici o comuni – nel processo penale cresce di riflesso al progresso tecnologico nel campo dell'elaborazione dei dati. Né potrebbe essere altrimenti, visto e considerato come la maggior parte delle attività investigative o d'*intelligence* poste in essere dalla polizia e dall'autorità giudiziaria hanno ad oggetto la vita privata delle persone. Avere a disposizione strumenti sempre più sofisticati, che permettano una penetrazione maggiore nella sfera intima di un soggetto, rappresenta, pertanto, per gli inquirenti un punto di forza. Tale riflesso, assume importanza se si pensa al numero di notizie che rientrano nella definizione di "dato personale"[67], e si osserva quanti di quelli rientranti in questa categoria siano a tutt'oggi potenzialmente catalogabili in un archivio elettronico.

Spostare il discorso sulla facilità odierna di reperire dati personali introduce, ad avviso di chi scrive, un'altra questione data dalla tutela del diritto alla *privacy* D'altra parte, la ricerca del risultato ottenibile attraverso un utilizzo massiccio di tutti i dispositivi di riproduzione e archiviazione di informazioni che la scienza informatica mette a disposizione degli inquirenti, non può non tener conto dell'equilibrio con le norme giuridiche – per certi versi antagoniste – che a tutti gli effetti ne limitano l'impiego. Questo punto costituisce il rovescio della medaglia del ragionamento fin qui condotto. Invero, la stessa nascita delle banche dati e stata accompagnata negli anni da uno sviluppo progressivo di situazioni giuridiche attive a tutela degli interessi intaccati da tali strumenti di invasione della sfera personale, con le quali, storicamente, l'interprete ha dovuto fare i conti. In quest'ottica il rapporto tra banca dati e diritto alla riservatezza non può essere scisso, e va inteso come una specie di tutt'uno: come dire che la catalogazione dei dati personali concretizza di fatto il prodotto del bilanciamento dei due fattori

[67] CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in *Protezione dei dati personali e accertamento penale, verso la creazione di un nuovo diritto fondamentale?*, a cura di NEGRI, Roma, 2007, 10.

succitati. Per certi versi potremo definire tale aspetto dell'archiviazione informatica come un elemento imprescindibile nell'ottica della definizione dei "limiti giuridici" oltre il quale l'autorità inquirente, nella veste di recettore di informazioni, non può andare.

1.1) Il diritto alla riservatezza

Il diritto alla *privacy*, inteso sotto un profilo di carattere puramente concettuale, nasce dalle rivendicazioni della *middle class* americana del diciottesimo secolo, verso una maggiore tutela di tutte quelle informazioni personali – che per certi versi potevano pregiudicare l'onorabilità, l'immagine o la reputazione del privato agli occhi della comunità in cui viveva – considerate di esclusiva pertinenza soggettiva, e per le quali veniva sollecitato un grado di protezione rafforzata rispetto alla conoscibilità all'esterno[68]. Per questo motivo il *rigth to be let alone* – testualmente il diritto ad essere lasciati soli – richiesto a gran voce da ricchi commercianti e proprietari terrieri statunitensi, venne bollato dagli studiosi dell'epoca come un reclamo elitario, tipico della borghesia conservatrice e settaria: una sorta di orpello ad uso e consumo di pochi[69].

Nel tempo è sicuramente cambiato il riferimento esclusivo al ceto medio, che per certi versi costituisce l'archetipo del diritto alla *privacy*, e la considerazione di quest'ultimo alla stregua di un diritto legato alla proprietà privata[70]. Tale mutazione è dovuta principalmente alla progressiva standardizzazione delle condizioni di vita individuale che ha caratterizzato lo sviluppo del mondo occidentale ed al simultaneo appiattimento delle differenze tra le classi sociali. Invero, l'idea che la riservatezza potesse rappresentare un valore individuale, e indipendente dall'appartenenza ad un ceto sociale speciale[71],

[68] PATRONO, Privacy *e vita privata (dir. pen.)*, in *Enc. dir.*, XXXV, Milano, 1986, 558.
[69] E' nel 1890, anno in cui un articolo di Warren - Brandeis, dal titolo *The right to privacy*, fu pubblicato dalla *Harvard Law Review*, che il concetto di privacy comincia ad avere una prima consistenza giuridica come *"the right to be let alone"*. WARREN – BRANDEIS, *The Right to* Privacy, in *Harvard Law Review*, 1891, 4, 193.
[70] GIACOBBE, *Riservatezza (diritto alla)*, in *Enc. dir.*, XL, Milano, 1977, 1249.
[71] MATTEUCCI, *Pubblico e privato,* in AA.VV., Privacy *e banche dati*, Bologna, 1981, 23.

ha generato di fatto un nuovo diritto, orientato verso la tutela contro illecite interferenze nella sfera privata della persona, intesa come soggetto integrato ad ogni livello nel tessuto sociale e produttivo di una comunità organizzata in modo democratico[72]. In tal senso viene considerato dalla Convenzione europea per la salvaguardia dei diritti dell'uomo, che all'art. 8 lo riconosce senza sottintesi come un diritto inviolabile, alla stessa stregua della libertà personale. Tale enunciazione da la percezione di come nella cultura occidentale il diritto *de quo* costituisca ormai una parte integrante ed indispensabile per l'affermazione di un essere umano[73].

In tempi più recenti, tale rappresentazione si è ampliata, nel senso che il diritto alla riservatezza viene interpretato anche come il diritto alla protezione dei dati personali, lecitamente appresi da soggetti pubblici o privati e contenuti in banche dati[74].

In quest'ottica le considerazioni complessive legate sia all'oggetto che alla portata della tutela garantita dalla situazione attiva riconosciuta, sono state man mano calibrate sulle esigenze emergenti collegate al rapporto tra il dato personale e la sua concreta diffusione all'esterno. Il tutto in sintonia col capillare sviluppo di strumenti di catalogazione elettronica, e con le esigenze collegate alla progressiva modernizzazione della società, nelle cui dinamiche, il contatto del soggetto con altri soggetti, e di riflesso la diffusione di dati personali è agevolato rispetto al passato[75].

Ciò nondimeno, occorre sottolineare come tale diritto non abbia pertanto nel corso degli anni l'originaria caratteristica *ad escludendum*. Invero il diritto alla riservatezza si sostanzia a tutt'oggi nel suo significato primigenio, più forte e rappresentativo: *id est* nella pretesa soggettiva di uno spazio personale inviolabile.

---

[72] CARNELUTTI, *Diritto alla vita privata (contributo alla teoria della libertà di stampa)*, in *Riv. trim. dir. pubbl.*, 1955, 5.

[73] In questi termini si sono espressi i rappresentanti delle autorità di protezione dati a livello mondiale, che nella dichiarazione conclusiva della ventisettesima conferenza internazionale dei garanti della *privacy* svoltasi a Montreux nel 2005, hanno definito il diritto alla protezione dei dati personali come un diritto universale che rispetta le diversità. Il testo completo della dichiarazione è disponibile nella sezione atti e documenti del sito *www.garanteprivacy.it*

[74] RODOTÀ, *Tecnologie dell'informazione e frontiere del sistema socio - politico*, in AA.VV., *Banche dati e diritti della persona*, Bologna, 1982, 90.

[75] V.FROSINI, *La protezione della riservatezza nella società informatica*, in *Inf. e dir.*, 1981, 7

In tal senso si realizza quello che alcuni autori[76] considerano come una sorta di paradosso del concetto originario del diritto alla riservatezza; come dire che dalla nascita di un diritto inteso da tutti come una sorta di "scudo protettivo" verso indebite intrusioni nella sfera privata, si è arrivati fino a far rientrare, nel novero delle tutele garantite dal diritto alla riservatezza, un controllo delle informazioni personali tutto rivolto all'esterno – definito in dottrina come il diritto all'autodeterminazione dei dati personali – teso ad evitare la diffusione dei dati già conosciuti da altri ed archiviati in *database* elettronici[77].

Invero, se fin dagli esordi il diritto *de quo* veniva considerato dalla dottrina d'oltre oceano – culla del diritto alla *privacy* – come un *right from*, ovvero come un diritto che in un certo qual modo rappresentava una garanzia di tutela contro illegittime intromissioni nella sfera privata di un soggetto[78], a tutt'oggi lo si ritiene un diritto qualificabile come *rigth of* , cioè a dire, alla stregua di un diritto al controllo dei dati personali appresi e detenuti da altri soggetti[79]. Quest'ultimo ha fatto ufficialmente il suo ingresso nel nostro ordinamento giuridico da poco più di un decennio, grazie al riconoscimento operato dalla legge del 1996, n. 575 prima, e dal d.lg. n. 196 del 2003 – Testo unico sulla *privacy* – in un secondo momento[80].

L'attuale legge sulla *privacy* raccoglie, sostanzialmente l'impostazione del *right of*, assicurando al soggetto privato un coacervo di garanzie sia di carattere soggettivo, che di carattere oggettivo, rivolte in particolare alla descrizione delle regole di trattamento dei dati personali – di carattere generale e speciale – alle quali si deve uniformare il titolare dell'elaborazione informativa. In quest'ottica, la normativa in questione reca un'articolata regolamentazione del diritto all'accesso delle informazioni personali detenute da altri soggetti e catalogati in elaboratori elettronici[81], del consenso alle attività di trattamento e del diritto ad una corretta informazione sulla portata di quest'ultimo. Introduce altresì nuove

[76] PATRONO, Privacy *e vita privata (dir. pen.)*, cit. , 568.
[77] STILO, *Il diritto all'autodeterminazione informativa: genesi storica di un diritto fondamentale dell'*Homo tecnologicus, in *Nuovo dir.*, 2002, 20.
[78] GIACOBBE, voce *Riservatezza (diritto alla)*, cit., 1254.
[79] CARNEVALE, *Autodeterminazione informativa e processo penale*, cit., 18.
[80] Vedi, cap. III.
[81] CARNEVALE, *Autodeterminazione informativa e processo penale*, cit., 4.

forme di tutela della riservatezza, in particolare attraverso la previsione di alcuni illeciti penali, previsti dagli artt. 167[82] - 172 del Testo unico[83].

Preso atto di ciò, è tuttavia da notare come, ben prima dell'*imprimatur* normativo dato dalle leggi sulla *privacy*, la dottrina si sia interrogata sulla corretta definizione da attribuire al bene giuridico tutelato dal diritto alla riservatezza;

[82] Il delitto di trattamento illecito di dati personali previsto dall'art. 167 richiede il dolo specifico: *id est* ottenere vantaggio o recare ad altri un danno, e che dal fatto derivi nocumento. Il testo dell'articolo è il seguente "salvo che il fatto costituisca più grave reato, chiunque , al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126, e 130, ovvero in applicazione dell'articolo 129 è punito, se dal fatto deriva nocumento , con la reclusione da 6 a 18 mesi, o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da 6 a 24 mesi – 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22 commi 8 e 11, 25, 26, 27, e 45, è punito, se dal fatto deriva nocumento, con la reclusione da 1 a 3 anni". In particolare, ai fini del delitto di cui all'art. 167 comma 1 del Testo unico, l'art. 18 concerne i principi applicabili a tutti i trattamenti effettuati da soggetti pubblici; l'art. 19 i principi applicabili al trattamento di dati diversi da quelli sensibili o giudiziari da parte dei soggetti pubblici, l'art. 23 il consenso per il trattamento di dati personali da parte di privati o enti pubblici economici; l'art. 123 la conservazione dei dati relativi al traffico a fini di fatturazione; l'art. 126 il trattamento dei dati relativi all'ubicazione; l'art. 130 la materia dell'invio di comunicazioni indesiderate. Ai fini dell'art. 167 comma 2, L'art. 17 concerne il trattamento che presenta rischi specifici e la necessaria adozione di misure di sicurezza; l'art. 20 i principi applicabili al trattamento di dati sensibili da parte di soggetti pubblici; l'art. 21 i principi applicabili al trattamento di dati giudiziari da parte di questi ultimi soggetti; l'art. 22 comma 8 stabilisce il divieto di diffusione di dati idonei a rivelare lo stato di salute; l'art. 22 comma 11 concerne particolari trattamenti di dati sensibili e giudiziari; l'art. 25 prevede il divieto di comunicazione e diffusione di determinati dati; l'art 26 detta ulteriori regole per i dati sensibili e l'art. 27 per i dati giudiziari; l'art. 45 vieta alcuni trattamenti.

[83] ANTONINI, *Il trattamento illecito di dati personali nel codice della* privacy*: nuovi confini della tutela penale*, in *Dir. pen. proc.*, 2005, 338; MANNA, *Codice della* privacy*: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali*, in ivi, 2004, 17. Oltre all'articolo 167 il Testo unico indica altri illeciti penali: l'art. 168 sulla falsità nelle dichiarazioni e notificazioni fatte al garante, l'art. 169 sull'omissione delle misure minime di sicurezza previste per i trattamenti dei dati personali dall'art. 33 del Testo unico, l'art. 170 sull'inosservanza dei provvedimenti del garante, l'art. 171 sulla violazione delle disposizioni degli artt. 113 e 114 del Testo unico che, in particolare, "è punita con le sanzioni di cui all'art. 38 della legge 20 maggio 1970 n. 300"; peraltro la trasformazione in illecito penale di determinate violazioni del codice sulla *privacy*, serve a fare da discrimine tra le condotte penalmente illecite e le altre violazioni di norme rilevanti in tema di trattamento previste dal Testo unico che non lo sono. Inoltre, va sottolineato come prima dell'intervento del Testo unico, il bene giuridico tutelato dal diritto alla *privacy* – *id est* la riservatezza della vita privata intesa come protezione rispetto ad atti illeciti di intrusione o diffusione della stessa – non avesse una tutela penale diretta ed esclusiva; poiché, la fattispecie prevista dall'art. 615 *bis* c.p. "interferenze illecite nella vita privata", viene considerata in dottrina come una protezione parziale e circoscritta, in quanto limitata ai soli luoghi indicati dall'art. 614 c.p., e ai soli casi in cui le notizie personali vengano acquisite attraverso strumenti di ripresa visiva o sonora. Vedi PATRONO, Privacy *e vita privata (dir. pen.),*cit., 570.

infatti "premesso che l'accordo regna sulla necessità di prevedere due distinte ipotesi criminose, l'una di indiscrezione, e l'altra di divulgazione, […] il problema sorge in ordine al fatto se le due distinte fattispecie siano poste a tutela di un medesimo bene giuridico, oppure diversi"[84].

Secondo alcuni autori, costituisce una lesione della riservatezza, tanto la diffusione di informazioni personali, quanto l'atto intrusivo *tout court* nel privato dell'interessato, rivolto cioè a carpire notizie personali caratterizzate da una conoscenza limitata[85]. Diversamente altra parte della dottrina, considera un pregiudizio alla riservatezza solo gli atti del primo tipo, dato che l'atto di indiscrezione realizza esclusivamente una violazione della vita privata[86].

Queste due teorie rappresentano entrambe una rielaborazione ermeneutica della dottrina di matrice tedesca sulle c.d. sfere "concentriche" del privato. In base a tale impostazione i dati personali non sarebbero tutti sullo stesso piano, ma dovrebbero venir differenziati in relazione al loro grado di conoscibilità. Vale a dire, le informazioni padroneggiate dal soggetto titolare delle stesse, e conosciute da un numero limitato di altre persone, rientrano nella c.d. sfera privata, le notizie comunicate ad una cerchia ristretta di soggetti in particolari rapporti di parentela o amicizia col soggetto al quale i dati appartengono, alla c.d. sfera confidenziale, le informazioni di dominio di un numero limitatissimo di individui legittimati a conoscerle, alla c.d. sfera del segreto, "la quale ricomprende, in particolare, notizie o fatti che per interessi o ragioni specifiche sono inaccessibili a chiunque non sia titolare del segreto"[87].

Partendo da questa impostazione, gli autori che considerano sia gli atti di indiscrezione o diffusione dei dati personali, come lesivi del diritto alla riservatezza, definiscono tali informazioni come l'oggetto di una conoscenza

[84] In particolare " la riservatezza appare, in realtà, integrare un bene giuridico "fittizio", perché, a ben vedere ponendosi l'accento sul fatto che certe notizie, o immagini, devono rimanere riservate, non si fa altro che riferirsi alla condotta lecita, che, appunto, preserva il bene giuridico […] il vero interesse tutelato dalle fattispecie di indiscrezione e di rivelazione non può che consistere nella "vita privata", offesa, a ben vedere, sia pure in modi diversi e dalla indiscrezione, e dalla divulgazione, le quali pertanto ledono un unico bene giuridico" . MANNA, *I beni della personalità e limiti della protezione penale*, Padova, 1989, 299 – 300.

[85] MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità di fatti criminosi*, in *Arch. giur.*, 1968, 41.

[86] BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen*., 1967, 1079.

[87] BRICOLA, *Prospettive e limiti della tutela penale della riservatezza,* cit., 1087.

esclusiva, che può essere di un solo soggetto – conoscenza esclusiva assoluta –, o di più individui – conoscenza esclusiva relativa – , in tale ottica, ogni azione rivolta ad intaccare quest'unica sfera cognitiva viene considerata come una lesione del diritto alla *privacy*[88]; infatti, dal momento che "il diritto alla riservatezza si sostanzia nell'esclusività, assoluta o relativa, della conoscenza col corrispettivo obbligo di non alterare questa esclusività, consegue, logicamente, che esso può essere parimenti offeso sia attraverso una abusiva presa di conoscenza, sia portando abusivamente a conoscenza di altri ciò che si conosce; e a maggior ragione, attraverso la abusiva presa di coscienza e la successiva rivelazione"[89]. Viceversa chi sostiene che vi sia una differenza tra i beni giuridici tutelati, a seconda della qualificazione dell'atto lesivo della sfera privata posto in essere – intrusivo o di diffusione –, afferma che " il diritto alla riservatezza difende la sfera privata dalla divulgazione di notizie legittimamente acquisite dal soggetto; mentre il diritto al rispetto della vita privata difende il soggetto da interferenze esterne in questa sfera. Pertanto, nella violazione del diritto al rispetto della vita privata l'accento dell'illiceità cade sull'interferenza […] nella violazione del diritto alla riservatezza l'accento dell'illiceità cade sulla diffusione, la quale ontologicamente assume una diversa portata a seconda che si tratti di notizie o dati concernenti la sfera privata, per le quali occorre la divulgazione al pubblico ovvero la sfera confidenziale, per le quali è sufficiente la comunicazione a persone diverse da quelle dalle quali si instaura il rapporto di fiducia"[90].

Oltre all'inquadramento sostanziale, la dottrina ha ricercato uno spazio costituzionale all'interno del quale collocare il diritto alla riservatezza, considerato che non esistono nella nostra Carta fondamentale riferimenti espliciti a tal fine[91].

[88] MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero,* cit., 64.
[89] MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero,* cit., 66.
[90] BRICOLA, *Prospettive e limiti della tutela penale della riservatezza,* cit., 1088 - 1089.
[91] PATRONO, Privacy *e vita privata (dir. pen.),* cit. , 575.

2.1)(segue) Il diritto alla privacy come diritto costituzionalmente garantito

La Costituzione non inserisce la riservatezza nel novero dei diritti inviolabili riconosciuti alla persona. Nello specifico non esiste una norma, tra quelle rientranti nei principi fondamentali, che direttamente preveda alcuna forma di tutela o protezione sulle notizie che dovrebbero rimanere segrete nell'interesse del soggetto a cui appartengono.

Malgrado questa "assenza", la dottrina in modo pressoché unanime, riconosce dignità costituzionale al diritto alla *privacy*, affermando che la mancanza di una previsione esplicita, che elevi al rango di principio costituzionale il diritto *de quo*, costituisce solo un ostacolo formale. Invero la presenza di un principio come quello previsto dall'art. 2, tra le regole poste a base della nostra Carta fondamentale, non può che condurre ad interpretazioni estensive del senso dello stesso, volte cioè a comprendere anche il diritto alla riservatezza sotto l'ala protettrice dei diritti inviolabili della personalità[92]. La *ratio* deve essere ricercata in una logica inclusiva. In tal senso l'articolo *de quo* rappresenta una previsione aperta, fonte di tutela per tutte quelle situazioni giuridiche riconducibili all'individuo, non richiamate da nessuna altra previsione costituzionale[93].

Peraltro, una interpretazione differente da quella suesposta genererebbe un sistema chiuso: una situazione che può essere raffigurata come una sorta di "dittatura dei valori" espressamente riconosciuti dalla Carta fondamentale. Si consideri poi che l'idea di una previsione dei principi costituzionali alla stregua di un *numerus clausus*, va irrimediabilmente a discapito di situazioni giuridiche nuove, derivanti dal progresso tecnologico – si pensi ad esempio al diritto alla autodeterminazione informativa – direttamente riconducibili alla sfera delle libertà individuali. In quest'ottica il diritto alla riservatezza sarebbe condannato a rimanere fuori dall'orbita costituzionale, non avendo nessun tipo di riconoscimento esplicito, con grave nocumento per tutte quelle situazioni tutelate dal diritto alla *privacy*. Per contro – come sottolineato da alcuni autori[94] – l'interpretazione estensiva della lettera dell'art. 2, genererebbe un ampliamento

[92] In tal senso; BARBERA, *Commento all'art. 2,* in *Commentario della Costituzione. Principi fondamentali*, a cura di BRANCA, Bologna 1975, 80; MESSINETTI, *Personalità (diritti della),* in *Enc. dir.*, XXXIII, Milano,1983, 371.
[93] BARBERA, *Commento all'art. 2*, cit., 85.
[94] BARILE, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, 54; CATAUDELLA, *La tutela civile della vita privata*, Milano, 1972, 32; GROSSI, *Inviolabilità dei diritti* , in *Enc. dir.*, XXII, Milano, 1972, 728.

incontrollato dei diritti inviolabili garantiti dalla Costituzione e condizionerebbe in modo poco ortodosso il numero di questi ultimi; tutto ciò in ossequio ad esegesi distorsive della Carta fondamentale che si rifanno alla logica della c.d. Costituzione materiale[95].

Il riferimento alla tutela dei diritti inviolabili dell'uomo inteso in senso ampio, ricomprende a tutti gli effetti anche la difesa della sfera privata, se si osserva come l'idea comune di quest'ultima raffiguri la protezione di tutta una serie di notizie che nel caso in cui dovessero essere diffuse all'esterno potrebbero provocare gravi scompensi individuali. A ben vedere si può affermare come la rivendicazione di uno spazio esclusivo, relativo alla conoscenza di determinate notizie, rappresenti una condizione esistenziale importante per un individuo, da proteggere rispetto a indebite intrusioni provenienti dall'esterno. Allo stesso modo anche l'esercizio di un controllo diretto su dati detenuti da altri soggetti pubblici o privati, raccolti in archivi elettronici, costituisce un riflesso della propria personalità. In tali casi, peraltro, il diritto alla riservatezza ha come situazione giuridica diametralmente opposta il dovere assoluto alla non diffusione di informazioni private. Nel caso in cui alcuni dati personali confluiscano all'interno di una banca dati organizzata, il soggetto che gestisce l'archivio elettronico ha l'obbligo di non divulgarle all'esterno, a meno che non venga autorizzato dalla persona alla quale appartengono le informazioni detenute[96].

Il coacervo di situazioni potenzialmente riconducibili al significato di "diritto alla riservatezza", crea una serie di difficoltà di carattere oggettivo legate alla individuazione della situazione da garantire in concreto; fermo restando come il nucleo fondamentale della situazione giuridica sia cristallizzabile sostanzialmente nella duplice accezione di diritto alla non intrusione nella sfera personale e all'autodeterminazione informativa dei dati personali legittimamente detenuti da altri soggetti pubblici o privati. Allo stesso modo, anche la definizione di dato personale genera analoghi problemi, preso atto di come nella determinazione nel *genus* delle informazioni richiamabili per rappresentare tali notizie, rientrino dati personali diversi tra loro e di ogni specie, tra i quali ad

[95] MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, Torino, 1995, 5.

[96] Il consenso informato alla divulgazione dei dati personali – inteso come principio generale rispetto al trattamento di alcune tipologie di informazioni – è stato introdotto nella direttiva 95/46 CE, e successivamente ripreso anche dal Testo unico sulla *privacy* d.lg. 2003 n. 196. Vedi par. 3.3.

esempio, rientrano le generalità, l'attività professionale, lo *status* familiare, le informazioni sui redditi e la salute, le caratteristiche fisiche, la mappa genetica, i dati identificativi di comunicazioni telefoniche ed il loro contenuto, le notizie su operazioni bancarie, sugli spostamenti nello spazio e via proseguendo verso un elenco di conoscenze potenzialmente illimitato[97].

In dottrina si rinvengono anche altre interpretazioni sul riconoscimento costituzionale del diritto alla riservatezza, alternative all'esegesi estensiva dell'articolo 2 Cost. . Invero quest'ultima norma viene considerata alla stessa stregua di una "sponda" normativa, insufficiente da sola a riconoscere la sussistenza del diritto alla *privacy*[98].

Il ragionamento logico coinvolge diversi articoli della prima parte della carta fondamentale, e si può definire come un' *analogia iuris*, poiché gli autori che interpretano in modo più rigido la lettera dell'articolo 2 Cost., non negano in assoluto che nuove situazioni giuridiche soggettive possano essere richiamate tra i diritti inviolabili degli individui [99], ed a tal fine, indicano quale presupposto oggettivo dell'inclusione, il collegamento con i diritti individuali già previsti nella nostra Costituzione; in modo tale che questi ultimi possano rappresentare la matrice delle nuove fattispecie. Pertanto, l'esegesi estensiva dei principi regolati nella carta fondamentale costituirà la legittimazione costituzionale dei "nuovi" diritti individuali[100].

Il richiamo ad una singola disposizione, come referente normativo in seno al quale innestare la copertura costituzionale del diritto alla riservatezza, è fondata sulle affinità particolari esistenti tra l'oggetto della tutela garantito dalla fattispecie tipizzata e la vita privata, intesa come bene protetto dal diritto alla *privacy*.

Le relazioni riguardano nelle specifico le norme poste dalla Costituzione a tutela della libertà personale, del domicilio, della corrispondenza e di ogni altra forma di comunicazione e quelle sulla libera manifestazione del proprio pensiero. Infatti, in questi casi si possono ritrovare dei caratteri in comune con la riservatezza, nell'esigenza cioè di mantenere confinata la conoscenza di una determinata notizia all'interno del domicilio o nello svolgimento di un colloquio

[97] GRANELLI, *Banche dati e riservatezza*, in *AIDA*, 1997, 235.
[98] MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, cit., 92.
[99] BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., 56.
[100] MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, cit., 105.

ristretto a due o più persone[101]. In tal senso l'inviolabilità del domicilio, così come quella delle comunicazioni tra soggetti, costituiscono per certi versi delle forme di tutela direttamente riconducibili alla protezione della vita privata, intesa come difesa della conoscenza esclusiva di notizie, relative alla sfera intima di un soggetto.

Viceversa, il riferimento all'art. 21 Cost. prende le mosse da una lettura fatta in chiave negativa della stessa norma costituzionale. Questa disposizione, così interpretata, offrirebbe una tutela contro i comportamenti volti ad apprendere e diffondere notizie che si vorrebbero invece mantenere riservate. Secondo l'opinione di alcuni autori[102], l'affermazione contenuta nella lettera dell'articolo *de quo* genera anche una forma di protezione differente; come dire che se la Costituzione riconosce ad un individuo il diritto a manifestare liberamente il proprio pensiero non si può non estendere la medesima tutela anche per la situazione diametralmente opposta: *id est* al soggetto che liberamente sceglie di non manifestare all'esterno la propria opinione o informazioni che lo riguardano.

Allo stesso modo anche la relazione con l'art. 13 Cost. viene ricondotta ad una connessione esistente col diritto alla riservatezza sulla base di un particolare legame che collegherebbe la libertà personale, interpretata in senso lato, alla riservatezza delle informazioni soggettive. Si parla in tal senso di *habeas data,* per individuare quella particolare forma di protezione dei dati personali ispirata al principio dell'*habeas corpus.*[103]

Parte della dottrina, richiama l'articolo *de quo* facendo riferimento al diritto alla *privacy* inteso come diritto all'autodeterminazione informativa[104].

In quest'ottica si afferma che la catalogazione di informazioni personali potrebbe essere considerata come una forma di "ispezione individuale", che viene compiuta in forma morale e non fisica. Si osserva infatti che, se al termine "ispezione" si attribuisce il significato di una indagine, di un controllo, di un accertamento, di un'osservazione attenta e minuziosa effettuata sullo spazio fisico e morale che è proiezione di una persona umana – ispezione personale, domiciliare, ispezione amministrativa sul comportamento, ispezione medica sui

[101] AULETTA, *Riservatezza e tutela della personalità*, Milano, 1978, 42.
[102] CERRI, *Libertà negativa di manifestazione del pensiero e di comunicazione – diritto alla riservatezza:fondamento e limiti*, in *Giur. cost.*, 1974, 610; BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., 231.
[103] V.FROSINI, *La protezione della riservatezza nella società informatica*, cit., 37.
[104] CARNEVALE, *Autodeterminazione informativa e processo penale*, cit., 22.

dati clinici – , l'ambito semantico può essere esteso anche al procedimento conoscitivo di rilevazione ai fini di schedatura[105]. Non sarebbe improponibile il paragone tra l'arbitrio di chi detiene abusivamente una persona in prigionia e l'arbitrio di chi detiene, senza autorizzazione, la c.d. "identità informatica" della persona, cioè l'insieme dei dati che permettono di ricostruire l'immagine morale della sua personalità e che, raccolti ed elaborati elettronicamente, diventano immediatamente accessibili e idonei ad essere trasmessi o diffusi, a differenza dei dati inseriti in vecchi archivi cartacei[106].

Il riferimento all'art. 13 Cost. e al concetto di "ispezione personale" sembra più facilmente condivisibile quando si tratta della ricostruzione della personalità, delle preferenze, delle opinioni, delle abitudini del soggetto effettuata a sua insaputa attraverso l'aggregazione, l'elaborazione e l'analisi di una grande mole di dati eterogenei, singolarmente insignificanti, forniti dal soggetto per uno scopo specifico e diverso, o raccolti da una serie di fonti diverse o nell'utilizzazione di un sistema interattivo. In tal caso non si tratta di raccogliere informazioni già esistenti, ma piuttosto di analizzare il modo di essere del soggetto, di scavare e di svelare la sua intimità, *id est* di "ispezionare" la sua personalità.

Altri autori riconducono il diritto alla libertà informatica nel ventaglio delle tutele garantite dall'art. 15 della Cost., in particolare quando la banca dati costituisca il frutto di un processo di comunicazione interindividuale[107].

Generalmente l'articolo *de quo* viene invocato al fine di garantire sia la libertà sia la segretezza delle comunicazioni che avvengono attraverso i sistemi telematici, e quindi anche la riservatezza delle informazioni trasmesse dagli utenti di tali sistemi. Potrebbe però pensarsi che la norma costituzionale comprenda non soltanto la tutela della segretezza delle informazioni trasmesse nei confronti di terzi estranei alla comunicazione, ma anche quella della riservatezza dell'utente di una banca dati nei confronti del gestore di quest'ultima.

Si è già più volte rilevato, invero, che il pericolo per la libertà informatica e per la *privacy* viene non tanto, o non solo, dalla raccolta e poi dall'aggregazione

[105] V.FROSINI, *La protezione della riservatezza nella società informatica*, cit., 9.
[106] V.FROSINI, *La protezione della riservatezza nella società informatica*, cit., 12.
[107] Ad esempio quando la comunicazione di dati tra più soggetti determinati, avviene tramite sistemi di posta elettronica o di videotelefono. CERRI, *Libertà negativa di manifestazione del pensiero e di comunicazione*, cit., 358.

ed elaborazione di informazioni ricavate da altre fonti, ma proprio dalla raccolta e dall'analisi delle informazioni che lo stesso utente, di volta in volta, involontariamente fornisce al gestore della banca dati con l'effettuare richieste o trasmettere ordini[108]. E può trattarsi di un pericolo molto grave in quanto anche le richieste apparentemente innocue possono, se conservate ed elaborate a fini diversi da quelle per cui erano state fatte, portare o rivelare aspetti della personalità del soggetto molto delicati e altrimenti non conoscibili. Potrebbe quindi pensarsi che l'art. 15 Cost. tuteli anche il diritto dell'utente di una banca dati alla riservatezza di queste informazioni, inteso nel senso del diritto a che le stesse non siano utilizzate dal gestore della banca dati, o siano utilizzate esclusivamente per il limitato scopo per il quale era avvenuta la comunicazione, e siano conservate soltanto per il tempo strettamente necessario[109].

2.3) ***Orientamento della Corte costituzionale***

La Corte costituzionale si è orientata verso un cauto riconoscimento del diritto alla riservatezza tra i diritti inviolabili posti a tutela di tutti gli individui.

La Consulta ha per lo più risolto in modo positivo il nodo ermeneutico, risolvendo le questioni legate alla soluzione del caso prospettato fornendo una interpretazione del diritto alla riservatezza sul singolo caso, senza mai individuare regole o principi di carattere generale[110]. Quello che si evince dalla lettura delle tante pronunce della Corte in materia è senza dubbio una linea direttiva consolidatasi nel tempo, verso il riconoscimento di una forza maieutica alla singola disposizione della Carta costituzionale, sulla quale basare il giudizio di esistenza del diritto alla riservatezza. In altre parole la Corte costituzionale postula un principio, che si rifà a quelle teorie dottrinali che considerano la norma

[108] V.FROSINI, *La protezione della riservatezza nella società informatica*, cit., 25.
[109]PACE, *Nuove frontiere della libertà di comunicare riservatamente (o piuttosto del diritto alla riservatezza)?*, in *Giur. cost.*, 1993, 742.
[110] MORELLI, *La giurisprudenza costituzionale italiana tra diritto alla riservatezza e potere di controllo sulle informazioni personali*, in *Protezione dei dati personali e accertamento penale*, cit., 28.

generale fissata dall'articolo 2 come una clausola chiusa, incapace da sola a fondare un giudizio sul riconoscimento costituzionale della riservatezza[111].

Un esempio della linea seguita dai giudici del palazzo della Consulta, è offerto senza dubbio dalle due pronunce che hanno avuto ad oggetto i dati esteriori della comunicazione, i c.d. tabulati telefonici[112]. Questi ultimi possono essere considerati a tutti gli effetti dei dati personali, contenuti in banche organizzate e detenute dal gestore della compagnia telefonica presso il quale il soggetto indagato possiede un numero telefonico. La conoscibilità di tali informazioni costituisce pertanto un valido esempio sul quale ragionare in funzione dell'oggetto della presente ricerca.

La Consulta ha dovuto dirimere la questione legata ad un eventuale estensione delle garanzie previste per le intercettazioni telefoniche, in particolare per le comunicazioni intercorrenti tra due soggetti captate da un terzo, anche a quelle notizie indirettamente riconducibili alla comunicazione stessa, come l'ora, il luogo della telefonata e il numero dell'utenza chiamata[113]. In generale va ricordato come l'intera materia delle intercettazioni telefoniche rappresenti un giusto equilibrio con quanto affermato dal principio contenuto nell'articolo 15 della Costituzione sulla libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione. In quest'ottica un'intercettazione di conversazioni telefoniche o ambientali dovrà necessariamente concretizzare la duplice forma di garanzia di legge e di giurisdizione previste dalla norma costituzionale; dovrà fondarsi, cioè, sulla pronuncia di un decreto di autorizzazione da parte del giudice per le indagini preliminari – intervenuta in seguito della richiesta del pubblico ministero –, ed essere consentita solo se sussistono alcuni presupposti di carattere oggettivo, quali l'esistenza di gravi indizi di reato, l'assoluta indispensabilità per la prosecuzione delle indagini e che si tratti di alcune fattispecie criminose indicate dall'art. 266 c.p.p. . Le stesse garanzie vengono estese dal comma 2 di tale norma anche alle intercettazioni ambientali, con la precisazione che nel caso in cui queste si svolgano all'interno di un domicilio verranno consentite solo se si ha il fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

---

[111] MORELLI, *La giurisprudenza costituzionale italiana tra diritto alla riservatezza e potere di controllo sulle informazioni personali*, cit., 34.

[112] Corte cost., 11 marzo 1993, n. 81, in *Cass. pen.*, 1993, 2774; Corte cost., 7 luglio 1998, n. 281, in *Giust. pen.*, 1998, III, 353.

[113] MELILLO, *L'acquisizione dei tabulati relativi al traffico telefonico fra limiti normativi ed equivoci giurisprudenziali*, in *Cass. pen.*, 1999, 473.

Riconoscere all'acquisizione di un tabulato telefonico la stessa dignità di una comunicazione tra soggetti, significa estendere le garanzie previste dal nostro codice per le intercettazioni telefoniche, col conseguente rispetto di tutti quei parametri legislativi che sovrintendono all'iniziativa dell'autorità giudiziaria in situazioni siffatte. La Consulta ha risolto il nodo ermeneutico in modo positivo, riconoscendo la stessa protezione di rango costituzionale, prevista dall'articolo 15 Cost. alle intercettazioni telefoniche pure all'acquisizione dei dati esteriori della comunicazione[114]. Nel far ciò ha individuato anche un parametro minimo necessario per poter ottenere i tabulati dal gestore degli stessi, individuandolo nelle regole previste dall'art. 256 c.p.p. riguardante il dovere di esibizione che il codice di procedura penale impone ai pubblici ufficiali e agli incaricati di un pubblico servizio, giustificando questa differenza di garanzie, nella difformità delle lesioni della *privacy* esistenti nelle due situazioni[115], dato che, in quella derivante dalla conoscenza dei dati esterni si ha una diversa forma di intrusione nella sfera della riservatezza che si realizza mediante l'acquisizione dei tabulati relativi al traffico telefonico.

L'elemento importante da sottolineare è la conclusione alla quale sono arrivati i giudici della Corte, secondo i quali, nel corso del processo penale l'acquisizione dei tabulati relativi ai telefoni cellulari gode di una protezione costituzionale, in quanto le garanzie fissate dall'art.15 Cost. sono riferibili non solo alle intercettazioni del contenuto di conversazioni o comunicazioni, ma anche alle tecniche che consentono di identificare i soggetti colloquianti, il tempo e il luogo della comunicazione, che non possono essere utilizzati in difetto della preventiva autorizzazione dell'autorità giudiziaria[116].

[114] CAMON, *Sulla inutilizzabilità nel processo penale dei tabulati relativi al traffico telefonico degli apparecchi "cellulari", acquisiti dalla polizia senza autorizzazione dell'autorità giudiziaria*, in *Cass. pen.*, 1996, 3722.
[115] CAMON, *Sulla inutilizzabilità nel processo penale dei tabulati relativi al traffico telefonico*, cit., 3725.
[116] L'acquisizione dei tabulati telefonici è regolamentata dall'art. 132 del Testo unico sulla *privacy*, a tal proposito, Vedi cap. III, par. 2.

3) Il riconoscimento del diritto alla privacy nella Convenzione europea per la salvaguardia dei diritti dell'uomo

La Convenzione europea dei diritto dell'uomo comprende la vita privata tra i diritti fondamentali sanciti a tutela delle libertà individuali. L'art. 8 della CEDU, rubricato "diritto al rispetto della vita privata e familiare", allinea quest'ultimo a quello dell'inviolabilità del domicilio e della segretezza della corrispondenza, considerando la violazione della riservatezza come un elemento indispensabile – non a caso inserito come prima indicazione nel § 1 – per la realizzazione degli altri due.

Invero, la scelta di porre in successione le tre situazioni porta a considerare come la tutela della corrispondenza e del domicilio costituiscano di fatto una specificazione del generale riconoscimento del diritto individuale alla riservatezza. In particolare, la prima alla stregua di una forma particolare di tutela rivolta alla protezione della segretezza del rapporto epistolare intercorrente tra due o più soggetti, mentre il secondo come luogo specifico nel quale confinare il riserbo delle informazioni in esso rivelate.

Il paragrafo iniziale della norma *de qua*, rappresenta il diritto alla *privacy* come un "*right from*", ovvero alla stregua di una tutela da indebite intrusioni nella conoscenza di informazioni riconducili alla sfera privata personale, cioè di dominio del solo soggetto al quale le informazioni appartengono o ad una cerchia limitata di individui conosciuti. La segretezza delle informazioni personali, considerata in tal senso, assurge al ruolo di elemento essenziale nell'esistenza di una persona, nonostante lo stesso articolo preveda al secondo paragrafo una serie di interferenze all'esercizio del diritto riconosciuto, generando in tal modo un diritto di carattere relativo. Le ingerenze al diritto alla riservatezza da parte di una autorità pubblica, devono essere previste da una legge e perseguire uno scopo legittimo, volto cioè a garantire, in una società democratica, " […] la sicurezza pubblica, il benessere economico del paese, la difesa dell'ordine, la prevenzione dei reati, la protezione della salute e della morale, la protezione dei diritti e delle libertà degli altri".

Tali situazioni corrono il rischio di presentarsi come una sorta di "contenitore vuoto" che può essere riempito di volta in volta e senza troppi sforzi di carattere interpretativo, tramite una serie di giustificazioni giuridiche che rendono lecita l'interferenza dei pubblici poteri con l'esercizio individuale del

diritto alla riservatezza. Vale a dire che è sempre possibile motivare, nel caso concreto, una tale ingerenza nella "*privacy*" dei soggetti, appellandosi ad una di quelle situazioni legittimanti che possono - anche attraverso forzature interpretative - ricorrere sempre[117].

Il rischio appena accennato è il frutto di una tecnica redazionale seguita nella stesura dell'art. 8 non proprio ortodossa, caratterizzata dall'enunciazione di un principio generale e dal suo successivo parziale svuotamento, attraverso l'utilizzazione di formule – adoperate a fini delimitativi e restrittivi – caratterizzate da una potenziale onnicomprensività e da una eccessiva indeterminatezza. E' pur vero, tuttavia, che l'aggiunta alla formulazione di un principio generale di ulteriori disposizioni può sopperire all'esigenza di rendere in forma più concreta determinate implicazioni particolarmente importanti di quello stesso principio o di esprimere regole che, se non fossero direttamente formulate, potrebbero lasciare spazio a negative incertezze.

Ad ogni modo il secondo paragrafo dell'art. 8 pone uno strumento normativo a difesa dei rischi di ingerenza derivanti dalla previsione di quelle numerose eccezioni al divieto di interferenza che esso stesso prevede. Tale strumento è la riserva di legge: "non può esservi ingerenza della pubblica autorità [...] se non in quanto prevista dalla legge". Inoltre, fra le situazioni che legittimano l'interferenza della pubblica autorità rientra anche "la protezione dei diritti e delle libertà altrui".

Ancora una volta l'indeterminatezza della formulazione tende ad indebolire la portata del riconoscimento e della tutela del *right to privacy*. Sembra infatti emergere la prevalenza di non meglio specificati diritti e libertà altrui sul diritto alla riservatezza, predominio che ne legittima una limitazione da parte dell'autorità pubblica.

Il ricco *case law* della Corte europea dei diritti dell'uomo in materia di riservatezza, costituisce una fonte imprescindibile per intendere in modo corretto il significato dell'articolo 8 della Convenzione[118]. In un ottica di carattere generale si può osservare come i giudici di Strasburgo interpretano in modo ampio

[117] ALLEGREZZA, *Giustizia penale e diritto all'autodeterminazione dei dati personali nella regione Europa*, in *Protezione dei dati personali e accertamento penale*, cit., 60.
[118] BLASI, *La protezione dei dati personali nella giurisprudenza della Corte europea dei diritti dell'uomo*, in *Riv. int. dir. uomo*, 1999, 543; BONETTI, *Riservatezza e processo penale*, Milano, 2003, 112.

l'oggetto del diritto alla *privacy*, nel senso che vi fanno rientrare a tutti gli effetti i dati genetici, il nome, l'orientamento sessuale, le informazioni relative alla professione svolta o riconducibili alla sfera lavorativa[119]. Nell'esegesi autentica della lettera dell'articolo *de quo*, offerta dalle varie sentenze della Corte che si sono occupate di definire i contorni del diritto alla riservatezza, si rinviene altresì un riferimento esplicito alla protezione della vita privata sia come forma di particolare garanzia dell'integrità dell'identità personale e dello sviluppo di quest'ultima, sia come tutela coessenziale, e per certi versi preventiva, rispetto alla possibilità del singolo individuo di stabilire e intessere relazioni interpersonali col mondo circostante[120].

Interpretata in tal senso la protezione della sfera di informazioni intime, assume un ruolo dinamico, differente dalla percezione statica – che dovrebbe rappresentare in modo apparentemente più fedele il significato del mantenimento della segretezza delle informazioni di pertinenza soggettiva –, tutta riflessa sulla protezione del singolo contro l'esterno alla stregua di un baluardo inattaccabile. La Corte sottolinea giustamente in varie pronunce come la tutela della *privacy* costituisca il presupposto per una corretta vita di relazione del soggetto con gli altri, inserendo tra i dati posti sotto la tutela dell'articolo 8, le notizie riferibili alla interazione soggettiva e le informazioni appartenenti ai rapporti relazionali intrattenuti dal soggetto con persone diverse[121].

L'articolo *de quo*, come visto in precedenza, prevede una serie di deroghe all'esercizio del diritto alla riservatezza. In prima battuta la Convenzione indica in modo chiaro come queste ultime debbano essere previste da una espressa previsione legislativa.

A tal proposito, la Corte europea ha tracciato i confini dell'interpretazione da dare alla parola legge inserita nel contesto delle ingerenze sulla *privacy*. Il primo dato da sottolineare è senza ombra di dubbio la pretesa di "qualità" quale

---

[119] FACCHIN, *L'interpretazione giudiziaria della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali:guida alla giurisprudenza della Corte*, Padova, 1990, 46.

[120] Corte Eur. , Leander v. Svezia, 26 marzo 1987, in *www.ehcr.int – hudoc database -*

[121] Corte Eur. , P.G and J.H. v. Regno Unito, 25 settembre 2001, in *www.ehcr.int – hudoc database -* ; TAMIETTI, *L'utilizzazione di prove assunte in violazione di un diritto garantito dalla Convenzione non viola l'equo processo: riflessioni sul ruolo della Corte europea e sulla natura del sindacato da essa operato in margine alla sentenza P.j. e J.H. v. Regno Unito*, in *Cass. pen.* , 2002, 1827.

tratto caratteristico del provvedimento legislativo derogatorio[122]; invero tale parametro di valutazione costituisce di fatto il frutto di un orientamento ormai consolidato, di portata generale ed espresso in più occasioni nella giurisprudenza della Corte. I giudici di Strasburgo considerano una legge, alla stregua di un provvedimento di qualità, quando quest'ultima risulti chiara, prevedibile e facilmente accessibile[123]. In altre parole ogni singolo soggetto deve essere messo in grado di conoscere le potenziali azioni che l'autorità pubblica può porre in essere per limitare la propria sfera privata, attraverso un provvedimento che espliciti in modo lineare e comprensibile le situazioni eventuali in cui tale compressione può avvenire. In particolare, il requisito dal quale non può prescindere la legge è l'indicazione dello scopo fondamentale perseguito attraverso la previsione del limite alla riservatezza del soggetto. In pratica, non occorre che sia di pertinenza legislativa anche la concreta disciplina delle attività materialmente riconducibili alla limitazione del diritto soggettivo. Invero la regolamentazione di queste ultime può essere anche il frutto di provvedimenti di carattere amministrativo o derivare da prassi consolidate della pubblica amministrazione[124].

Peraltro, anche le attività investigative, svolte in segreto dall'autorità giudiziaria, – come le intercettazioni di comunicazioni – necessitano di una legge che ne individui le condizioni e le circostanze di attuazione[125]; in tal senso, si è pronunciata la Corte, nell'importante sentenza *Malone v. Regno unito*[126], relativa alla legittimità della pratica di captazione segreta frutto dell'attività del c.d. *metering* o – secondo la denominazione francese –, *comptage.* Tale operazione viene compiuta attraverso l'utilizzo di uno strumento d'intercettazione, una sorta di contatore, che connesso al telefono oggetto d'indagine può fornire tutte quelle informazioni, diverse dal contenuto della comunicazione utili nelle attività investigativa quali il numero delle utenze chiamate, il luogo e l'ora dell'avvenuta

[122] Corte Eur. , Peck v. Regno Unito, 28 gennaio 2003, in *www.ehcr.int – hudoc database-*
[123] Corte Eur. , L.L. v. Francia, 10 ottobre 2006, in *www.ehcr.int – hudoc database -* .
[124] ALLEGREZZA, *Giustizia penale e diritto all'autodeterminazione dei dati personali*, cit., 62.
[125] Corte Eur. , Peck v. Regno Unito, cit. .
[126] Corte Eur. , Malone v. Regno Unito, 2 agosto 1984, in *www.ehcr.int – hudoc database-* .

telefonata[127]. La lesione della vita privata prodotta dalle attività di *metering* costituisce una deroga atipica del diritto alla riservatezza; questa circostanza, in aperto contrasto con quanto previsto dal secondo paragrafo dell'art. 8 CEDU, sulle necessaria tipicità delle deroghe al diritto alla *privacy*, portò la Corte alla dichiarazione di illegittimità dello strumento di investigazione. Inoltre i giudici di Strasburgo valutarono la pratica summenzionata, lesiva del diritto alla riservatezza, in quanto " […] le operazioni di *metering* contengono informazioni, in particolare i numeri digitali, che sono parte integrante delle comunicazioni telefoniche. Di conseguenza, il rilascio di tali informazioni alla polizia senza il consenso dell'abbonato costituisce, una violazione del diritto garantito dall'art. 8"[128]. Questa pronuncia[129], che può essere definita come una sentenza pionieristica nel suo genere, anticipa di quasi un decennio la sentenza della nostra Corte costituzionale, nella quale si accoglie l'interpretazione estensiva, rispetto all'allargamento della protezione prevista dall'art. 15 Cost., anche per quelle attività investigative che hanno ad oggetto l'acquisizione dei dati esterni della comunicazione.

Le eccezioni al diritto alla riservatezza, oltre ad essere disciplinate da un provvedimento legislativo, devono perseguire uno scopo legittimo.

Tra i presupposti indicati per poter valutare la legittimità della deroga, il più volte menzionato art. 8 fa un riferimento generale alla tutela della sicurezza pubblica, al benessere economico del paese, alla difesa dell'ordine, alla prevenzione dei reati, alla protezione della salute e della morale, alla protezione dei diritti e delle libertà degli altri. In quest'ottica gli eventuali limiti stabiliti a danno del diritto alla riservatezza dovranno essere tali da garantire le necessità emergenti in "una società organizzata in modo democratico". Il requisito della "necessità" – richiamato esplicitamente nella lettera del secondo paragrafo dell'art. 8 –, implica che l'interferenza nel diritto alla *privacy* debba corrispondere ad una bisogno pressante della società, ed essere pertinente, sufficiente e proporzionata rispetto allo scopo legittimo che intende proteggere[130]. E' affermazione costante della Corte quella secondo cui le autorità nazionali godono

[127] BLASI, *La protezione dei dati personali nella giurisprudenza della Corte europea dei diritti dell'uomo*, cit. , 547.
[128] CAMON, *Sulla inutilizzabilità nel processo penale dei tabulati relativi al traffico telefonico*, cit., 3722.
[129] Corte Eur. , Malone v. Regno Unito, cit. .
[130] Corte Eur. , Amann v. Svizzera, 16 febbraio 2000, in *www.ehcr.int – hudoc database -*

di un margine discrezionale nell'individuare il punto di equilibrio fra obiettivi pubblici e interessi privati che entrino in collisione. Quest'ultima in numerose sentenze ha più volte ribadito come il requisito della "proporzionalità" della limitazione, rappresenti un parametro importante per definire la legittima interferenza nella vita privata di un soggetto, come dire che la gravità dell'ingerenza esercitata sul diritto alla riservatezza deve costituire una misura adeguata agli obiettivi da tutelare, indicati nella parte conclusiva del secondo comma dell'art.8[131].

3.1) ***La libertà informatica***

Il nuovo rapporto che si è venuto ad instaurare tra i cittadini, e fra questi e lo Stato, nella odierna società tecnologica, ha dato luogo – come visto nei precedenti paragrafi – al sorgere di una concezione dinamica del diritto alla *privacy* inteso come diritto al controllo dei dati personali inseriti in banche dati informatiche, spettante cioè al soggetto cui si riferiscono le informazioni. In quest'ottica tale diritto acquista un contenuto positivo, che può essere definito come un "contro limite" al potere informatico – esercitato dal soggetto pubblico o privato che forma e gestisce le banche dati – nell'affermazione della propria dignità e libertà[132].

Questo aspetto nuovo del diritto alla riservatezza viene anche denominato in dottrina come "libertà informatica", ossia diritto ad informarsi sui dati computerizzati di cui è in possesso il gestore di un elaboratore elettronico[133]. La "libertà informatica", va intesa come una concezione in chiave moderna del *right to privacy*, di fatto rappresenta una forma particolare della tradizionale libertà personale, considerato come essa configuri un diritto soggettivo, che può

[131] Corte Eur. , Halford v. Regno Unito, 27 maggio 1997, in *www.ehcr.int – hudoc database -*

[132] V.FROSINI, *La protezione della riservatezza nella società informatica*, cit. , 9; Secondo il quale la libertà informatica possiede due facce: una negativa consistente nel diritto di non rendere di dominio pubblico certe informazioni di carattere personale, privato o riservato; l'altra positiva, rappresentata dal diritto di esercitare un controllo sui dati concernenti la propria persona, che sono già fuoriusciti dalla cerchia della *privacy* per essere divenuti elementi di *input* di un programma elettronico

[133] V.FROSINI, *I diritti umani nella società tecnologica,* in *Riv. trim. dir. pubbl.*, 1981,1163.

diventare un diritto d'azione in sede giudiziaria e che richiede l'indicazione specifica di alcune garanzie giuridiche per realizzarsi: *id est* la previsione delle facoltà di accesso, controllo, rettifica, ed eventuale cancellazione di dati personali inseriti in una banca dati.

Inteso in tal senso, il diritto alla riservatezza, trova spazio in alcuni importanti provvedimenti europei come la Convenzione di Strasburgo n. 108 del 1981[134], la direttiva CE 95/46 c.d. (direttiva madre)[135], l'art. 8 della Carta di Nizza e la decisione quadro del Consiglio 2008/977/GAI sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale[136].

Questi ultimi insieme alla fondamentale sentenza del *bundesverfassunsgericht* tedesco del 15 dicembre 1983[137] rappresentano il *logos* del c.d. diritto alla autodeterminazione informativa, quantomeno del suo riconoscimento soggettivo.

Invero, nonostante le varie differenze legate alla genesi, al periodo storico, al contesto territoriale e alla tipologia di atto giuridico, è possibile leggere tra le

[134] Vedi par. 3.2 .

[135] Alla quale sono seguite le successive direttive sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni – direttiva 97/66 CE – , e nel settore delle comunicazioni elettroniche, direttiva 2002/58 CE .

[136] Vedi par. 3.4 .

[137] Con l'importante pronuncia del 1983 la Corte Costituzionale tedesca dichiarò l'esistenza di un "diritto all'autodecisione sui dati". Nello specifico venne riconosciuto al singolo cittadino il diritto al controllo sui propri dati, nei confronti dei metodi di elaborazione informatica. La Corte ha formulato il principio con estrema chiarezza enunciando come, attraverso le attuali possibilità offerte dall'elaborazione automatizzata delle informazioni personali e soprattutto dall'incrocio dei dati, non esista più un dato privo di importanza. In quest'ottica occorre determinare i requisiti leciti e gli scopi protetti attraverso le attività di catalogazione dei dati personali, anzitutto tutelando il segreto e garantendo l'anonimato nell'elaborazione, e il diritto di accesso al dato personale. Qualora questi requisiti non venissero rispettati, l'eventuale trasmissione dei dati, dal soggetto titolare al responsabile del trattamento, sarebbe lesiva del principio dell'autodecisione. In tal senso una completa registrazione e catalogazione della personalità mediante una raccolta combinata dei dati sui singoli aspetti della vita privata e della personalità che permetta una ricostruzione del profilo completo della personalità del cittadino non è ammessa neppure per i rilevamenti statistici soggetti all'anonimato anche se permette di costruire un quadro soltanto parziale della personalità del soggetto, a meno che, il legislatore non indichi dei metodi di rivelazione soggetti alla massima riservatezza, nel profondo rispetto del diritto all'autodecisione dei dati personali. In Italia il diritto all'autodeterminazione informativa è stato definito come una libertà informatica, nel quadro del generale diritto all'informazione sul dato personale. Per una approfondita analisi della sentenza del tribunale tedesco sul diritto all'autodecisione sui dati personali vedi; ADDIS, *Diritto all'autodeterminazione informativa e processo penale in Germania*, in *Protezione dei dati personali e accertamento penale*, cit., 90.

righe dei diversi provvedimenti una medesima *ratio,* da ricercare nell'individuazione del diritto alla protezione diretta del dato, operata in prima persona da parte del soggetto titolare dell'informazione, attraverso la partecipazione attiva al trattamento delle notizie.

Occorre sottolineare inoltre come la linea tracciata dal legislatore europeo sia stata seguita anche in Italia. Invero, prima con la legge sulla *privacy* n. 676 del 1996 e successivamente con l'approvazione del Testo unico in materia di riservatezza d.lg n. 196 del 2003, si è accolto il principio della protezione del dato catalogato in una banca dati, attraverso la predisposizione di quelle garanzie soggettive che dopo il riconoscimento ottenuto con la Convenzione di Strasburgo, sono diventati la base della tutela garantita alle persone in tema di catalogazione informatica di dati. D'altro canto negli ultimi anni la necessità di creare un argine normativo al libero trattamento dei dati personali, è divenuto sempre più pressante, in considerazione del fatto che non si può vivere oggi in quella che viene definita la "società dell'informazione" senza disporre di appropriati strumenti normativi che impediscano che la libera circolazione dei dati si attui a discapito del diritto alla *privacy*[138].

A tal proposito va rimarcato come, nel corso degli anni le varie disposizioni che hanno avuto ad oggetto lo specifico tema della tutela del dato personale, hanno disciplinato soprattutto il difficile rapporto esistente tra il diritto alla libera circolazione dei dati e quello sulla necessità di attribuire al titolare dell'informazione un ampio diritto di controllo circa l'uso e la diffusione dei suoi dati[139].

Da questo punto di vista possono essere identificati due approcci generali. Il primo - che trova realizzazione soprattutto negli Stati Uniti - è a carattere settoriale e si fonda sulla particolare regolamentazione delle specifiche modalità di trattamento dei dati. Il secondo, - che è prevalente invece in Europa - è quello che tende all'emanazione di leggi e convenzioni onnicomprensive di tutti gli aspetti caratteristici della tutela della *privacy* nella società dell'informatica, compresa la protezione dei dati ad opera di un autorità garante o del soggetto

[138] V.FROSINI, *La protezione della riservatezza nella società informatica*, cit., 8.
[139]GIANNANTONIO, *Il nuovo disegno di legge sulle banche di dati personali*, in *Riv. dir. informat. informaz.*, 1991, 80.

interessato, al quale appartengono i dati contenuti in un archivio elettronico[140]. La formula "protezione dei dati" fece la sua prima comparsa nella legge emanata dal *Land* dello *Hesse* (Assia) in Germania nel 1970[141], che può essere considerata in assoluto come la prima legge di una nazione europea sulla tutela dei dati. Sebbene tale formula sia stata criticata, poiché si riteneva che facesse riferimento più alla protezione dell'informazione in quanto tale piuttosto che a quella dei diritti del suo titolare, essa è stata largamente ripresa in leggi e convenzioni nazionali ed internazionali[142].

Peraltro, va rilevato come la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali riconosca anche il diritto di acquisire informazioni, che per certi versi può essere considerato di segno opposto rispetto all'esigenza di controllo e protezione dei dati personali[143]. Invero nell'articolo 10 della CEDU sono compresi, oltre al diritto alla libertà di espressione, "la libertà d'opinione, la libertà di ricevere e diffondere informazioni ed idee senza l'interferenza di pubbliche autorità e senza riguardo ai confini nazionali ".

Il Consiglio d'Europa si occupò per la prima volta di tale questione nel 1986, quando la sua Assemblea Parlamentare approvò la Raccomandazione R(86) 1037, sulla protezione dei dati e la libertà d'informazione in cui riaffermava il potenziale conflitto tra i due concetti e raccomandava che una Commissione di esperti sulla protezione dei dati fosse costituita "al fine di identificare criteri e principi in conformità ai quali la protezione dei dati e il diritto di accesso ad informazioni ufficiali possano essere conciliati". A tal proposito il principio del consenso informato al trattamento dei dati personali – previsto dall'art. 7 della direttiva 95/46 CE –, posto come condizione necessaria per la diffusione delle informazioni, rappresenta un buon compromesso tra i due diritti succitati, anche se la stessa direttiva prevede dei casi in cui può essere effettuato comunque un trattamento nonostante non ci sia il consenso dell'interessato[144], e lascia agli stati membri la previsione di particolari regole per il bilanciamento tra il diritto alla

[140] SERROTTI, *Libertà di informazione e libertà informatica:la tutela della riservatezza,* in *Inf. e dir.* , 1996, 84.
[141] ADDIS, *Diritto all'autodeterminazione informativa e processo penale in Germania*, cit., 100; MANNA, *I beni della personalità e limiti della protezione penale*, cit., 345.
[142] ADDIS, *Diritto all'autodeterminazione informativa e processo penale in Germania*, cit., 103.
[143] BLASI, *La protezione dei dati personali nella giurisprudenza della Corte europea dei diritti dell'uomo*, cit. , 545.
[144] Vedi par. 3.3 .

vita privata e le norme sulla libertà di espressione nel caso in cui il trattamento venga fatto esclusivamente a scopi giornalistici (art. 9).

I provvedimenti internazionali che hanno avuto ad oggetto lo specifico tema della protezione dei dati, si sono rivolti soprattutto verso l'individuazione di un livello minimo di tutela da garantire alle informazioni catalogate nelle banche dati informatiche. In quest'ottica, determinare uno standard omogeneo di difesa delle notizie personali appare necessario, ove si pensi alla facilità con la quale il singolo dato – in modo capillare – può essere trasmesso, oltre i confini statali, da una banca di raccolta ad un'altra.

Invero, attraverso l'utilizzazione delle normali reti di telecomunicazione, società specializzate nella elaborazione elettronica dei dati, che operano in paesi diversi, possono svolgere attività di elaborazione personali in un luogo ben preciso, differente rispetto al luogo nel quale i dati sono stati raccolti. In questo modo le informazioni dei cittadini di una nazione possono essere tranquillamente elaborate - senza nessun controllo - in un altro stato. Tale prassi, negli anni in cui mancavano regole uniformi volte a creare una situazione di garanzia omogenea rispetto al trattamento delle notizie personali, svuotava di contenuto ed effettività la legislazione sulla protezione dei dati della nazione di volta in volta interessata: come dire che eventuali regole approntate da questa sulla protezione dei dati personali potevano essere aggirate attraverso un uso strumentale della lacuna legislativa di un altro stato[145].

Inoltre, le carenze degli strumenti normativi transnazionali non davano adeguata risposta non solo alle problematiche relative ai diritti fondamentali degli individui rispetto al trattamento dei loro dati, ma nemmeno fornivano opportuna tutela agli interessi politici ed economici pure coinvolti nelle attività di elaborazione e trasmissione dei dati. Occorrevano dunque risposte normative di carattere internazionale più appropriate e da questa necessità prende corpo la Convenzione di Strasburgo del 1981.

[145] MARTINES, *La protezione degli individui rispetto al trattamento automatizzato dei dati nel diritto dell'U.E.*, in *Riv. it. dir. pubbl. com.* , 2000, 724.

3.2) ***La Convenzione 108/1981 sulla protezione degli individui rispetto al trattamento automatizzato dei dati personali***

La Convenzione di Strasburgo[146] nelle disposizioni generali sottolinea che il suo scopo è quello di garantire "ad ogni persona fisica […] il diritto alla vita privata in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano ("protezione dei dati")". A fronte dell'iniziale e solenne enunciazione di principio della disposizione relativa all'oggetto e allo scopo della Convenzione, l'art. 3, rubricato "campo d'applicazione", prevede una deroga importante; nel senso che, lo Stato aderente può escludere dall'ambito di applicazione "certe categorie di schedari automatizzati di dati a carattere personale dei quali sarà depositato un elenco". Peraltro l'applicazione della Convenzione può essere estesa anche a schedari di dati personali non automatizzati[147]: *id est* cartacei.

[146] La Convenzione di Strasburgo n. 108 del 1981 è stata ratificata dall'Italia con la legge n. 98 del 21 febbraio 1989. Il testo tradotto del provvedimento è disponibile nel repertorio normativo del sito *www.garanteprivacy.it* .

[147] In materia di protezione dei dati personali in ambito europeo va segnalata anche l'iniziativa dell'Organizzazione per la cooperazione e lo sviluppo economico, la quale con l'emanazione nel 1980 delle "Linee Direttrici concernenti la protezione della *privacy* e il flusso transfrontaliero dei dati" – testo integrale disponibile su *www.oecd.org/dataoecd/* --, ha offerto un importante strumento volto a rafforzare il ruolo del soggetto titolare dei dati personali nell'ottica di un controllo attivo degli stessi. Rispetto alla Convenzione di Strasburgo vi sono delle somiglianze, legate essenzialmente alla omogeneità degli argomenti trattati, ma anche delle differenze. Fra queste ultime la più rilevante è che la Raccomandazione dell'OCSE consiste in un "consiglio" e non in un "comando", è priva cioè di un potere vincolante fra le parti. Inoltre le finalità delle linee guida sembrano essere più ampie rispetto a quelle perseguite dalla Convenzione n° 108 del Consiglio d'Europa. Quest'ultima trova applicazione solo nel caso in cui i dati personali siano soggetti ad elaborazione automatizzata mentre le disposizioni della raccomandazione OCSE si "applicano ai dati personali, sia nel settore pubblico che in quello privato, i quali, a causa delle modalità di elaborazione o a causa della loro natura o del contesto nel quale sono utilizzati, mettono in pericolo la privacy e le libertà individuali". In merito alle assonanze tra i due provvedimenti va detto che con riferimento alle disposizioni più importanti c'è una grande similitudine tra la Convenzione e le "*Guidelines*", anche se le disposizioni delle linee guida dell'OCSE, sono quasi sempre tecnicamente meno accurate rispetto a quelle corrispondenti della Convenzione. Ad esempio, in relazione alla questione della trasparenza nell'elaborazione dei dati, la Convenzione prevede che "ogni persona dovrà essere messa in grado […] di stabilire l'esistenza di un archivio automatizzato di dati personali che la riguardano direttamente, i suoi scopi principali, l'identità e la residenza abituale o il luogo primario dell'attività del gestore dell'archivio". Le "*Guidelines*" - invece - dispongono semplicemente che "ci

Tra le varie innovazioni inserite nella Convenzione approvata dal Consiglio d'Europa, merita sicuramente di essere segnalata quella prevista dall'articolo 2, che contiene le definizioni dei nuovi termini giuridici derivanti dal progresso tecnologico in campo di banche dati. Nella norma *de qua* si fa riferimento al "responsabile dello schedario", novità questa di rilevante conseguenza per le responsabilità civili e penali, che identifica in una "persona fisica o giuridica", il gestore dell'archivio elettronico. Si tratta di un'indicazione che può inquadrarsi nelle recenti tendenze volte ad individuare il responsabile di un procedimento amministrativo, orientamenti accolti peraltro anche nella legislazione italiana successiva alla Convenzione.

Il Capitolo II tratta dei principi fondamentali della protezione dei dati, l'art. 5, individua le linee direttive alle quali i gestori di banche dati si devono uniformare; *id est* i principi di liceità, proporzionalità e di scopo[148]. La disposizione internazionale dà anche una dettagliata definizione dei dati "sensibili"; essi sono indicati come quelli relativi all' "origine razziale, alle opinioni politiche, alle convinzioni religiose o altre convinzioni, alla salute ed alla vita sessuale ed a condanne penali", per il trattamento di tale categoria di dati si richiedono "garanzie appropriate" (art. 6) .

La Convenzione prevede inoltre delle deroghe al diritto alla protezione dei dati personali. In tal senso l'art. 9 indica alcune eccezioni ai diritti riconosciuti al titolare delle informazioni contenute in una banca dati. Con tale previsione il Consiglio ha riprodotto fedelmente quanto già previsto dal secondo paragrafo dell'art. 8 CEDU per il diritto alla riservatezza[149]. Infatti anche nella Convenzione di Strasburgo, l'eccezione al diritto dovrà realizzare una misura necessaria in una società democratica per la protezione della sicurezza dello Stato, per la sicurezza pubblica, per gli interessi monetari, per la repressione dei reati,

---

dovrebbe essere una generale politica di apertura circa gli sviluppi, le attività e le politiche relative al trattamento dei dati personali. In tal senso dovrebbero essere predisposti prontamente strumenti per stabilire l'esistenza e la natura di dati personali, le principali finalità della loro utilizzazione, l'identità e la residenza abituale del gestore"; MISSORICI, *Banche dati e tutela della riservatezza*, in *Riv. int. dir. uomo* , 1996, 54.

[148] L'art. 5 indica precise prescrizioni per i responsabili del trattamento dei dati in particolare: devono essere acquisiti ed elaborati lealmente e legalmente, registrati per fini determinati e legittimi, devono essere esatti ed aggiornati, devono essere conservati sotto una forma che permetta l'identificazione delle persone interessate per un periodo non superiore a quello necessario per i fini per i quali essi sono stati registrati, e, infine, devono essere adeguatamente protetti.

[149] Vedi, par. 3.

per la protezione della persona interessata e dei diritti e libertà di altri. In dottrina, le deroghe al diritto alla protezione dei dati personali di stampo puramente pubblicistico, vengono considerate come una vera e propria "contro regola", posta a tutela dell'arbitrio dello Stato; mentre quelle previste genericamente "a protezione […] dei diritti e delle libertà di altrui" sono valutate alla stregua di una clausola di salvaguardia, volte a garantire la libertà di stampa[150].

Peraltro le deroghe su elencate riguardano nello specifico le disposizioni previste dagli artt. 5, 6, 8 della Convenzione. In particolare l'articolo 8 enuncia le garanzie per la persona interessata, che, nell'ottica della definizione la c.d. "libertà informatica" in senso soggettivo, costruiscono l'aspetto forse più importante del provvedimento. Invero va rimarcato come in molti casi le banche dati rappresentino uno strumento di creazione di nuove informazioni prima sconosciute al gestore dell'archivio e - quel che è più importante - spesso ignote anche a terzi e talvolta allo stesso soggetto cui si riferiscono.

L'elaborazione informatica, infatti, si caratterizza, come più volte sottolineato, soprattutto per la sua capacità di trasformare informazioni disperse in una informazione organizzata e aggregata, che consente di risalire così dagli atti più banali dell'individuo ai suoi più intimi segreti[151]. Basti pensare, a questo proposito, ai sistemi interattivi e alla possibilità che ha il loro gestore di sottoporre ad aggregazione e ad analisi migliaia di dati di per sé insignificanti – relativi, ad esempio, alla scelta di un programma televisivo o all'acquisto di certi prodotti o alla lettura di certe notizie o alla richiesta di date informazioni e così via – e di ricavarne, all'insaputa dell'interessato, un profilo della personalità, delle opinioni, delle tendenze, dei gusti dell'utente del tutto nuovo e non rinvenibile da altre fonti.

Per porre un limite giuridico a queste derive incontrollate della catalogazione informatica, la norma fissa il diritto di conoscenza e accesso agli schedari automatizzati con la contestuale possibilità di richiedere la rettifica e la cancellazione dei dati nel caso in cui questi ultimi fossero errati, fino ad arrivare alla previsione di un ricorso contro la violazione del diritto personale di "*habeas data*", ossia di controllo sui propri dati personali, nell'ipotesi in cui " non venga

[150] MISSORICI, *Banche dati e tutela della riservatezza*, cit., 55.
[151] SERROTTI, *Libertà di informazione e libertà informatica:la tutela della riservatezza*, cit., 86.

dato seguito ad una richiesta di conferma e, a seconda del caso, di comunicazione, rettifica, o cancellazione del dato personale " .[152]

L'idea di dare risposte ai nuovi fenomeni tecnologici introdotti in campo informatico, si ritrova anche nelle disposizioni che la Convenzione pone come argine alla pratica della trasmissione simultanea, e a qualunque distanza, dei dati. Invero la possibilità di "esportare" le informazioni personali al di là dei confini di uno stato – e di sottrarsi in tal modo agli obblighi e ai controlli vigenti in un dato paese in materia di tutela della *privacy* – ha portato alla genesi di un fenomeno che in dottrina è stato ribattezzato, come la ricerca dei c.d. "paradisi informatici", in analogia con i c.d. "paradisi fiscali" [153].

E' necessaria dunque che ci sia una disciplina omogenea per evitare abusi a danno degli interessati, senza però chiudere le frontiere, salvo che nei confronti di quegli Stati nei quali proprio la libertà di circolazione dei dati - di tutti i dati, sensibili e no - crea pericolosi inconvenienti. Si può dire, con formula paradossale, che non può sussistere la libertà di scambio di dati con quegli Stati in cui vige la piena libertà di circolazione degli stessi.

Il Capitolo III della Convenzione disciplina questo particolare aspetto, legato alla mobilità dei dati, attraverso un esplicito accenno ai flussi di informazioni, che possono verificarsi da uno stato all'altro, al fine di assicurare la cooperazione fra questi e la libera circolazione delle notizie "indipendentemente dalle frontiere". L'art. 12 stabilisce la regola della libertà di flusso transfrontaliero dei dati fra le parti contraenti, ma insieme enuncia due eccezioni: la prima è quella che sanziona il principio di equivalenza, ovvero di come si può vietare l'esportazione di quei dati per i quali non sia prevista una protezione equivalente nel paese importatore; la seconda eccezione è intesa ad evitare vantaggi a favore dei "paradisi informatici": come dire che non si possono trasferire dati ad un altro Stato non contraente la Convenzione, che è perciò sottratto ai suoi obblighi. Il capitolo IV concerne l'assistenza reciproca; nell'ambito di quest'ultimo l'art. 14 evidenzia l'importanza del principio secondo cui "ciascuna parte presta assistenza a tutte le persone residenti all'estero per l'esercizio dei diritti previsti dalle sue

[152] V.FROSINI, *La protezione della riservatezza nella società informatica*, cit., 10.
[153] Il richiamo ai c.d. "paradisi", fiscali o informatici, tende a sottolineare la similitudine tra situazioni in cui si va alla ricerca di un posto nel quale ci sia un *deficit* di garanzie soggettive o di regole. MISSORICI, *Banche dati e tutela della riservatezza*, cit., 57.

norme interne che danno attuazione" alle garanzie riconosciute del diritto di accesso, rettifica e ricorso. Si garantisce, inoltre l'obbligo della segretezza delle informazioni di cui in tal modo si viene a conoscenza e si vieta alle autorità di un Paese "di presentare una richiesta di assistenza a nome di una persona interessata residente all'estero di sua propria iniziativa e senza l'esplicito consenso di tale persona" (art.16) .

3.3)***Diritto comunitario e trattamento dei dati personali: la direttiva 95/46 CE***

L'Unione Europea ha emanato la direttiva 95/46, relativa alla "Tutela delle persone fisiche rispetto al trattamento automatizzato dei dati" ed alla "tutela della libera circolazione di tali dati", con l'obiettivo di armonizzare le legislazioni nazionali di settore ai sensi dell'articolo 100 A del Trattato CE relativo al "ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno"[154]. La necessità di una disciplina interstatale organica in materia, è stata avvertita dal legislatore comunitario per una serie di fattori come il sempre più frequente ricorso al trattamento di dati personali nei vari settori economici e sociali favorito dai progressi registrati nelle tecnologie dell'informazione, dal fatto che il rafforzamento della cooperazione scientifica e tecnica e la messa in opera di nuove reti di telecomunicazione nella Comunità che facilita il flusso transfrontaliero dei dati personali, e dalla necessità di colmare il divario esistente tra le legislazioni nazionali sotto il profilo del grado di protezione della riservatezza dei dati[155].

Soprattutto in considerazione dell'ultimo fattore, la direttiva 95/46 CE stabilisce un "principio di equivalenza" – già contenuto nella Convenzione si Strasburgo – relativamente al livello di tutela dei diritti e delle libertà delle

[154] A tal proposito il primo "considerando" della direttiva colloca la materia della tutela delle persone fisiche con riguardo al trattamento dei dati personali, nell'ambito dei diritti fondamentali dell'individuo. Si fa infatti riferimento alla "necessità di eliminare le barriere che dividono l'Europa" basandosi "sui diritti fondamentali sanciti dalle Costituzioni e dalle leggi degli stati membri, nonché dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali".

[155] MARTINES, *La protezione degli individui rispetto al trattamento automatizzato dei dati nel diritto dell'U.E.*, cit., 724.

persone coinvolte nel trattamento dei loro dati[156]. Lo strumento per attuare una "protezione equivalente" tra i diversi stati dell'U.E. è stato individuato dalla direttiva – nel considerando n. 9 – nell'opera di ravvicinamento delle diverse legislazioni nazionali, che dovranno dare attuazione ai principi fondanti del provvedimento *de quo*. Per contro, gli Stati membri avranno "un margine di manovra" di cui potranno valersi nell'applicazione della direttiva, precisando le condizioni generali di liceità dei trattamenti. Tuttavia tale libertà non deve avere come effetto quello di "indebolire la tutela approntata dalle leggi" ma deve anzi "mirare a garantire un elevato grado di tutela nella Comunità".

Scopo della direttiva è inoltre quello di ampliare e precisare la tutela del diritto alla riservatezza predisposta dalla Convenzione di Strasburgo 108 del 1981 con riguardo al trattamento automatizzato dei dati personali. D'altra parte nei quindici anni di distanza che intercorrono tra le due disposizioni le tecnologie dell'informazione sono progredite in maniera rilevante ponendo problemi giuridici nuovi – comunicazioni telefoniche su reti cellulari, telecomunicazioni satellitari che richiedevano, nel momento in cui è stata emanata la direttiva, nuovi diversi approcci e soluzioni.

Invero, il legislatore comunitario ribadisce che le grandi potenzialità dell'informatica e della telematica devono essere poste al servizio dell'uomo, e non il contrario, in modo tale da promuovere il rispetto delle libertà, il diritto alla vita privata e il benessere degli individui. Proprio in considerazione dei progressi delle tecnologie dell'informazione, la direttiva, nel considerando n. 14, indica come quest'ultima "dovrebbe applicarsi al trattamento dei dati in forma di suoni e immagini relativi a persone fisiche, vista la notevole evoluzione in corso nella società dell'informazione delle tecniche per captare, comunicare, conservare siffatti dati".

Nel solco delle considerazioni fatte fin'ora, e nell'ottica delle conclusioni alle quali si vuole arrivare attraverso l'analisi della direttiva 95/46 CE, pare interessante notare come tra le disposizioni di ordine generale, l'atto comunitario fornisca le definizioni, specificandone l'accezione, di alcuni concetti fondamentali nell'ambito della protezione dei dati personali, partendo proprio dal significato da attribuire a questi ultimi . In quest'ottica per "dato personale" s'intende qualsiasi

[156] ACCIAI, *Privacy e banche dati pubbliche. Il trattamento dei dati personali nelle pubbliche amministrazioni*, Padova, 2001, 10.

informazione concernente una persona fisica – non giuridica – identificata, o identificabile, sulla base di uno o più elementi specifici caratteristici. Inoltre le attività riconducibili al "trattamento" vengono definite come "qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicati a dati personali", mentre "l'archivio di dati personali" viene interpretato come "insieme strutturato di dati personali accessibili secondo criteri determinati". Sulla base di quest'ultima indicazione si può considerare come l'ambito di applicazione della direttiva non è limitato agli archivi informatizzati, ma ricomprenda tutte le unioni organizzate di informazioni, *id est* anche quelli cartacei.

Tra le definizioni riportate nell'art. 2 della disposizione *de qua*, assume particolare rilievo la distinzione – già prevista anche dalla Convenzione di Strasburgo – tra il "responsabile del trattamento" e "l'incaricato del trattamento". Il primo è la persona fisica o giuridica, l'autorità pubblica, il servizio o qualunque altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento; il secondo è la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati per conto del responsabile del trattamento[157]. La nozione di "terzo" si ricava poi negativamente, nel senso che è "terzo" la persona fisica, giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia responsabile del trattamento, incaricato del trattamento o persona interessata.

La direttiva introduce altresì il principio del "Consenso informato" come requisito generale di liceità del trattamento. Invero si considera come tale qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento[158]. Da sottolineare altresì come l'art. 3 individui il campo di

[157] MISSORICI, *Banche dati e tutela della riservatezza*, cit., 58.

[158] L'art. 7 della direttiva 95/46 CE prevede che uno stato membro possa autorizzare il trattamento di dati personali solo quando: " a) la persona interessata ha manifestato il proprio consenso in maniera inequivocabile, b) è necessario all'esecuzione del contratto concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta di tale persona, c) è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento, d) è necessario per la salvaguardia dell'interesse vitale della persona interessata, e) p necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati, f) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le

applicazione delle disposizioni contenute nel provvedimento comunitario. Queste ultime si applicano al trattamento di dati personali interamente o parzialmente automatizzati, nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi. Viceversa sono esclusi dal suddetto ambito i trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico e quelli che non rientrano nel campo di applicazione del diritto comunitario[159].

Inoltre va detto che il considerando n. 13 prevede che le attività previste dai titoli V e VI del trattato sull'Unione Europea attinente alle materie del c.d. "terzo pilastro", non rientrano nel campo di applicazione del diritto comunitario[160]. Particolare importanza riveste il riferimento fatto alle legislazioni nazionali, per la determinazione delle condizioni alle quali i trattamenti dei dati personali sono leciti. A tal proposito la direttiva fornisce i principi generali in materia, richiamando implicitamente quanto aveva stabilito a tal fine l'art. 5 della Convenzione di Strasburgo. In relazione alla qualità dei dati – previsti nello specifico dall'art. 6 – la direttiva prevede che questi ultimi devono essere trattati lealmente e lecitamente, raccolti per finalità determinate, espliciti, legittimi, adeguati, pertinenti, esatti, aggiornati. L'articolo *de quo* specifica inoltre che laddove fossero inesatti o incompleti rispetto alle finalità della raccolta, i dati dovranno essere cancellati o rettificati; prevede inoltre la possibilità di conservare le informazioni solo per il tempo necessario al conseguimento dello scopo della catalogazione, concretizzando di fatto anche in sede comunitaria il c.d. diritto all'oblio del dato personale. Il rispetto di queste disposizioni - che riguardano più precisamente non solo la qualità dei dati ma anche quella della raccolta, del trattamento e della conservazione degli stessi - deve essere garantito da parte del responsabile del trattamento.

Molto importante nell'ambito della nostra ricerca sulle caratteristiche dei tratti distintivi del diritto alla libertà informatica, risulta essere la previsione contenuta nella sezione IV della Direttiva, composta da due articoli che disciplinano "l'informazione della persona interessata", regolando i casi della

---

libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1".

[159] ROSSETTI, *Commento alla direttiva 95/46*, in *Dir. industr*., 1997, n.3, 246.

[160] ALLEGREZZA, *Giustizia penale e diritto all'autodeterminazione dei dati personali*, cit., 65.

"informazione in caso di raccolta dei dati presso la persona interessata" e della "informazione in caso di dati non raccolti presso la persona interessata".

Nella prima ipotesi l'articolo 10 considera l'informazione fornita alla persona presso la quale il responsabile del trattamento o un suo responsabile effettua la raccolta di dati che la riguardano, come una condizione fondamentale il cui rispetto è necessario per un "trattamento leale". L'elenco del tipo di informazioni da fornire non è da considerarsi esaustivo: la stessa norma che lo prevede afferma che devono essere fornite almeno le informazioni elencate. Il che vuol dire che la norma fissa una piattaforma informativa minima avente ad oggetto l'identità del responsabile del trattamento ed eventualmente del suo rappresentante e le finalità del trattamento medesimo[161].

Altre informazioni che devono essere fornite alla persona interessata "quando siano necessarie per effettuare un trattamento leale" riguardano: i destinatari dei dati, se esistono diritti di accesso e di rettifica dei propri dati, se rispondere alle domande è obbligatorio o volontario nonché le possibili conseguenze di una mancata risposta. Peraltro occorre segnalare come l'articolo *de quo* si applica solo se la persona non è già informata.

L'articolo 11 presenta una struttura quasi identica a quella dell'articolo precedente con la differenza che in tale caso il responsabile del trattamento - quando i dati non vengono raccolti presso la persona interessata - deve informare il titolare dei dati al più tardi al momento della registrazione, o della comunicazione a terzi se prevista, indicando altresì le categorie di dati interessati. Altra differenza riguarda una serie di deroghe all'obbligo informativo che non deve essere adempiuto se l'informazione della persona interessata si rivela impossibile e richiede sforzi sproporzionati o la registrazione o la comunicazione sono previsti dalla legge. Ad ogni modo gli Stati membri sono comunque tenuti a fornire le opportune garanzie.[162]

Nell'ottica del diritto alla protezione del dato personale, così come nella Convenzione di Strasburgo, la Sezione V disciplina in un unico articolo – art. 12 – il diritto di accesso ai dati da parte della persona interessata. Tale diritto, così

[161] ALPA, *La direttiva comunitaria sul trattamento dei dati personali*, in www.jei.it .
[162] MARTINES, *La protezione degli individui rispetto al trattamento automatizzato dei dati nel diritto dell'U.E.*, cit., 730.

come disciplinato dalla direttiva, deve essere libero e senza costrizione esercitato a intervalli ragionevoli, senza ritardi o spese eccessive.

Il titolare del dato deve essere messo in grado di conoscere l'esistenza di un trattamento in corso, delle finalità perseguite dall'attività posta in essere, le categorie di dati trattati, i destinatari cui essi sono comunicati, le informazioni sull'origine dei dati,nonché, infine, la logica utilizzata se il trattamento è svolto in forma automatizzata. Inoltre, se il trattamento non è conforme alle disposizioni della direttiva, il titolare dei dati - specie se inesatti o incompleti - può chiederne la rettifica, la cancellazione o il congelamento e può ottenere che tali operazioni siano notificate ai terzi destinatari delle comunicazioni, quando ciò non comporti sforzi irragionevoli. Peraltro è necessario precisare come le deroghe al diritto di accesso ai dati sono soggette al rispetto di due restrizioni: devono costituire una misura necessaria di salvaguardia di particolari intessi pubblici o privati, possono riguardare solo i diritti e gli obblighi di cui agli artt. 6, primo paragrafo, 10, 11, primo paragrafo, 12 e 21: *id est* qualità dei dati, diritti di informazione, diritto di accesso, pubblicità dei trattamenti.

Va infine segnalata l'importanza dei meccanismi di controllo individuati dalla direttiva in relazione alla creazione di banche dati. Si tratta in particolare dell'obbligo di notificazione circa l'esistenza di un archivio elettronico di raccolta di dati e del controllo preventivo sulle caratteristiche tecniche di quest'ultimo. Il primo adempimento è generalizzato: riguarda, cioè, tutti i trattamenti di dati interamente o parzialmente automatizzati destinati al conseguimento di una o più finalità correlate, deve rivolgersi ad un organismo di controllo centralizzato unico per tutti gli stati membri dell'U.E. e grava sul responsabile del trattamento o sul suo rappresentante. Destinatario della notificazione è il "Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali" istituito dall'articolo 29 della direttiva, come autorità comunitaria di controllo[163].

Il secondo parametro da soddisfare ogni qual volta si istituisce una banca dati di raccolta è il controllo preliminare, *id est* una verifica prima della loro attivazione ad opera di una autorità garante di controllo, istituita presso ogni Stato membro.

[163] MISSORICI, *Banche dati e tutela della riservatezza*, cit., 61.

3.4) ***(segue) La decisione quadro 2008/977/GAI del Consiglio, sulla protezione dei dati personali nelle materie del c.d. terzo pilastro***

Come visto nel precedente paragrafo, la protezione delle materie rientranti nel c.d. terzo pilastro, relative alla cooperazione giudiziaria in materia penale, non godevano della protezione garantita dalla direttiva 95/46 CE, in quanto escluse dall'ambito di applicazione del provvedimento comunitario. La collaborazione tra nazioni in materia giudiziaria è stata, per quanto riguarda lo scambio di dati personali, caratterizzata dalla progressiva – e piuttosto lenta – attuazione delle indicazioni contenute nel programma dell'Aia relative all'attuazione del principio di disponibilità[164]. In tal senso sono nate nel corso degli anni una serie di banche dati di matrice europea, che di fatto rappresentavano – fino all'adozione della decisione quadro 2008/977/GAI – le uniche fonti normative in grado di tutelare lo scambio di informazioni tra stati in ambito giudiziario[165]. La decisione *de quo* prevede una serie di regole generali, indirizzate verso tutte quelle situazioni in cui la collaborazione tra Stati riguardi la trasmissione di dati o la disponibilità di informazioni di carattere giudiziale, tanto che la decisone quadro del Consiglio colma una lacuna di sistema; visto e considerato come le precedenti regole, poste a tutela della cooperazione informativa tra stati, erano confinate allo scambio di informazioni nell'ambito delle c.d. "banche dati europee di terzo pilastro"[166].

La decisione *de qua* ribadisce l'importanza dei principi di proporzionalità, finalità e di scopo che devono sovrintendere alla creazione di una banca dati organizzata. Stabilisce inoltre un dovere di controllo in capo agli Stati membri relativo alla verifica della correttezza dei dati trasmessi e un obbligo – che può essere sollecitato anche dal titolare dei dati – alla cancellazione dei dati personali nel caso in cui questi risultino non più necessari per le finalità per le quali sono stati legalmente raccolti, ovvero alla loro rettifica qualora fossero non corretti. A tal proposito lo Stato che ha l'onere di trasmissione dovrà procedere al blocco

[164] CIAMPI, *Principio di disponibilità e protezione dei dati personali nel terzo pilastro dell'Unione europea*, in *Cooperazione informativa e giustizia penale nell'Unione europea*, a cura di PERONI – GIALUZ, Trieste, 2009, 34.
[165] DECLI – MARANDO, *Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia*, in *Cooperazione informativa e processo penale*, cit., 101.
[166] Rientrano in quest'elenco: la banca dati SIS, il sistema informativo doganale SID, la base di dati TECS di Europol ed EPOC III di Eurojust.

delle informazioni personali "se vi sono motivi ragionevoli di ritenere che la cancellazione possa compromettere gli interessi legittimi della persona interessata".

I doveri statali arrivano fino a coprire un controllo sulle garanzie offerte dallo stato richiedente sulla tutela dei dati personali e, a tal fine si dovrà procedere all'accertamento del livello di protezione e di trattamento dei dati. Peraltro il livello di verifica è innalzato nel caso in cui il trasferimento riguardi dati sensibili o particolarmente delicati; in tali ipotesi"il trattamento di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale è ammesso soltanto se strettamente necessario e se la legislazione nazionale prevede adeguate garanzie". Inoltre la decisione quadro rappresenta, un provvedimento che può essere qualificato come un *genus* in materia di cooperazione informativa. Tale impostazione è ribadita nelle premesse dello stesso provvedimento, segnatamente nel "considerando" n. 39 che fa un esplicito riferimento a tutte le disposizioni in materia che nel dettaglio si occupano di materie riconducibili alla protezione dei dati personali, ma che lo fanno in settori specifici ed in relazione a particolari materie. La decisione menziona a tal proposito le disposizioni che disciplinano il funzionamento "dell'Europol, di Eurojust, del sistema informativo Schengen del sistema informativo doganale SID e di quelle che introducono l'accesso diretto delle autorità degli Stati membri a taluni sistemi di dati di altri Stati membri. Lo stesso vale per quanto riguarda le disposizioni di protezione dei dati che disciplinano il trasferimento automatizzato tra Stati membri di profili di dna, dati dattiloscopici e dati nazionali di immatricolazione dei veicoli a norma della decisione 2008/615/GAI del Consiglio del 23 giugno 2008 sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità organizzata".

Ai fini dello studio che si conduce, occorre mettere in luce un dato importante: la decisione quadro individua il diritto di accesso ai dati personali, e l'informativa al soggetto titolare quali momenti caratterizzanti del diritto all'autodeterminazione informativa. Il fatto rilevante, a parer di chi scrive, è che tale provvedimento ribadisce l'importanza della libertà informatica, strutturato sulla scorta di quanto previsto da precedenti provvedimenti – in particolare la Convenzione di Strasburgo e la direttiva 95/46 CE –, anche in materie che

idealmente sarebbero poco inclini a tutelare il diritto del soggetto ad interagire con l'autorità giudiziaria nell'ambito di un indagine a carico. Invero, con tutte le dovute cautele del caso, occorre notare come alla luce della decisone *de qua*, un soggetto del quale vengano richieste notizie da una autorità giudiziaria straniera gode di più garanzie – in campo informativo – rispetto ad un soggetto sottoposto ad indagine all'interno del nostro paese dall'autorità giudiziaria italiana[167]: come dire che lo stesso diritto garantito nel caso di individui coinvolti in indagini penali all'estero non è assicurato in ambito nazionale[168].

Peraltro tale considerazione rappresenta il risultato dell'analisi delle fonti che si è fin qui condotta allo scopo di ricercare dei riferimenti esterni ai quali ancorare le conclusioni del presente lavoro; costituisce altresì il dato di partenza sul quale riflettere in relazione al rapporto, ad oggi inesistente, tra diritto all'autodeterminazione informativa e il processo penale.

[167] La legge sulla *privacy* prevede un regime di trattamento speciale dei dati personali, nel caso in cui questi siano effettuati in ambito giudiziario. In relazione a questo specifico utilizzo è inibito qualsiasi intervento del soggetto interessato rivolto ad esercitare un controllo su informazioni personali contenute in banche dati criminalistiche, impiegate dall'autorità giudiziaria nel corso di un procedimento penale.

[168] CIAMPI, *Principio di disponibilità e protezione dei dati personali nel terzo pilastro,* cit., 74.

CAPITOLO TERZO

PROFILI PROBLEMATICI

1) La regolamentazione delle banche dati nel d.lg. n. 196 del 2003

Il d.lg. n. 196 del 2003 – Testo Unico in materia di protezione dei dati personali – contiene una disciplina organica in materia di tutela della riservatezza pienamente in linea con gli obiettivi indicati in sede europea dalla relativa Convenzione di Strasburgo e dalla direttiva 95/46 CE[169]. In particolare anche in Italia, viene affermato il diritto alla corretta identità informatica, corrispondente all'interesse collettivo[170] ad avere trattamenti di dati personali rispettosi dei principi di proporzionalità, correttezza e finalità[171]. Per questo motivo – in base all'articolo 11 del Testo unico – nel nostro paese non possono essere create banche dati che mantengano le informazioni oltre il tempo necessario per il raggiungimento dello scopo[172], rechino al loro interno notizie non corrette, non rispecchino in modo fedele la realtà delle situazione alle quali si riferiscono,

[169] Vedi cap. II, par. 3 e 3.2

[170] "La controversa natura giuridica della "*privacy* informatica", si direbbe sospesa fra vero e proprio diritto soggettivo e semplice interesse, non impedisce di rilevare che si è in presenza di un interesse collettivo […] sembrerebbe che l'evoluzione del concetto di vita privata, dal "segreto" al "controllo" da una dimensione, cioè, puramente individuale ad una collettiva, corrisponda – grosso modo – al fenomeno degli "interessi diffusi", i quali sono scomponibili, a differenza dell' "interesse generale", in una serie di situazioni giuridiche soggettive singole". MANNA, *Tutela penale della personalità*, Bologna, 1993, 139.

[171] L'art. 6 della direttiva 95/46 CE e l'art. 5 della Convenzione di Strasburgo sulla protezione dei dati personali, contengono entrambe l'elencazione dei principi generali posti a fondamento delle attività di raccolta dei dati personali, del tutto uguale a quella contenuta nell'art. 11 del Testo unico sulla *privacy*.

[172] In Italia non sono consentite raccolte di dati illimitate, non soggette cioè alla fissazione di tempi di riferimento che ne cristallizzino il limite temporale per l'impiego. Per questo motivo l'informazione personale deve essere distrutta allo scadere del termine, onde evitare un utilizzazione all'infinito della stessa, in modo tale da veder realizzato il diritto all'oblio del dato.

cataloghino dati personali selezionati in modo illecito o approssimativo, raccolgano dati per fini differenti da quelli per i quali sono state istituite[173].

Ciò premesso, pare importante focalizzare l'attenzione su alcuni punti del Testo unico sulla *privacy*, così da poter affrontare in modo accurato l'analisi delle norme dedicate alle attività di trattamento dei dati personali effettuate dalle forze di polizia, o in ambito giudiziario per ragioni di giustizia.

Il codice di protezione dei dati definisce all'art. 4, tra i principi generali, il novero delle attività rientranti nella nozione generale di "trattamento". A tal proposito sono compresi tra le operazioni *de quibus* tutte quelle elaborazioni o complesso di elaborazioni effettuate anche senza l'ausilio di strumenti elettronici e concernenti "la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati". Tale indicazione appare molto significativa, in quanto definisce l'ambito di applicazione delle regole contenute nel codice sulla *privacy*. Nell'elencazione offerta dalla lett. a, dell'articolo 4 emerge un coacervo di situazioni, che vanno dalla semplice raccolta, fino ad arrivare alla "disgregazione informativa": ovvero a tutte quelle circostanze in cui il dato perde la sua integrità e diventa un informazione complessa – come avviene ad esempio nel caso delle operazioni di modificazione o elaborazione – in virtù della scomposizione o aggregazione insieme ad altre.

Peraltro, il Testo unico classifica i dati personali[174] in identificativi – attraverso i quali si arriva all'identificazione diretta dell'interessato –, sensibili[175],

[173] In particolare l'art. 11 afferma che "I dati personali oggetto di trattamento sono trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi, esatti e, se necessario, aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati".

[174] Viene considerato dato personale "qualunque informazione relativa ad una persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente mediante il riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"

[175] Sono dati sensibili "i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti politici, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale"

"quasi sensibili"[176] e giudiziari[177]. Questa distinzione incide direttamente sulla disciplina del trattamento prevista per la singola informazione, dato che, le norme di carattere speciale che si occupano di regolamentare forme particolari di elaborazione di informazioni, e le regole stabilite per il trattamento effettuato da soggetti pubblici o privati, aumentano o affievoliscono il livello di tutela del dato catalogato, a seconda che questo sia sensibile, quasi sensibile o giudiziario. Oltre a ciò, va detto che la difesa dei dati viene garantita attraverso un sistema di tutele integrato, dal momento che la lesione delle disposizioni previste dal Testo unico in materia di *privacy* legittima il soggetto che la subisce a rivolgersi sia all'autorità amministrativa garante per la *privacy* che al giudice competente[178]. Peraltro, il controllo sulle attività di elaborazione può essere effettuato direttamente dall'interessato allo scopo di acquisire indicazioni precise sulla natura dell'elaborazione e sulle finalità ad essa collegate, oppure per ottenere la rettifica o la cancellazione delle informazioni raccolte in modo illecito[179]. Tali diritti possono essere esercitati presso il titolare del trattamento delle notizie, e rientrano nell'ambito del diritto di accesso ai dati personali garantito dall'art. 7 del

[176] L'art. 17 definisce come "quasi sensibili" tutti quei dati diversi da quelli sensibili e giudiziari il cui trattamento "presenta dei rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare"

[177] Nel gruppo dei dati giudiziari sono ricompresi "i dati personali idonei a rivelare provvedimenti di cui all'articolo 3 comma 1 , lettere da a) a o) e da r) a u), del d.p.r. 14 novembre 2002, n.313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale" .

[178] Il codice di protezione dei dati personali prevede due forme di tutela, una di carattere amministrativo l'altra di stampo giurisdizionale. L'autorità garante è competente per tutte le violazioni rilevanti delle norme previste dal Testo unico sulla *privacy*, e può essere investita della questione attraverso la proposizione di un reclamo, di una segnalazione, e, nel caso di lesione di un diritto rientrante tra quelli previsti dall'art. 7 sul diritto d'accesso, con la proposizione di un ricorso. In particolare il Testo unico definisce quest'ultimo caso, come una tutela alternativa a quella giurisdizionale, in quanto i diritti previsti dall'art. 7 possono essere fatti valere dinanzi all'autorità giudiziaria o al garante; nel senso che l'intervento di uno esclude l'altro. Pertanto la presentazione del ricorso al garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto. Tuttavia il giudice – tribunale collegiale del luogo in cui ha sede il soggetto titolare del trattamento – è competente per tutte le controversie che riguardano il codice della *privacy*, comprese quelle inerenti ai provvedimenti del garante in materia di protezione dei dati personali o alla loro mancata adozione. RESTA, *Le sanzioni amministrative e la modulazione dell'interesse punitivo*, in CARDARELLI – SICA – ZENO-ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 65.

[179] MESSINA, *I diritti dell'interessato*, in CARDARELLI – SICA – ZENO-ZENCOVICH, *Il codice dei dati personali*, cit., 65.

Testo unico[180]. Per quanto riguarda quest'ultimo aspetto, va evidenziato come le garanzie soggettive siano parametrate al settore speciale nel quale si dà origine alla raccolta delle informazioni riservate; in tal senso, il Testo Unico sulla *privacy* regola l'esercizio di alcuni diritti spettanti al soggetto interessato in relazione agli obiettivi per cui si realizza l'archiviazione delle notizie private.

In particolare per il trattamento dei dati personali che avviene in ambito giudiziario e da parte delle forze di polizia, – espressamente disciplinati dal Testo unico sulla *privacy* dagli artt. 46 - 49 e 53 – 57 –, la legge stabilisce un'incompatibilità oggettiva con i principi incorporati nelle disposizioni generali, relative alla protezione dei dati esercitabile in prima persona da parte di colui cui si riferiscono le notizie contenute in un *database*[181]. Questa impostazione costituisce il frutto del bilanciamento operato dallo stesso compilatore del codice di protezione dei dati tra le norme poste a tutela della *privacy* e le esigenze legate alle attività di carattere giudiziario[182]. In tal senso deve essere letto il sacrificio di diritti importantissimi come il diritto d'accesso[183], il consenso al trattamento, l'applicazione del diritto all'informativa sul trattamento dei dati e dei poteri spettanti all'autorità di garanzia in materia di tutela delle notizie riservate, dal momento che sia l'obbligo di comunicare al garante i trattamenti di dati idonei a rivelare lo stato di salute dell'interessato[184], che la possibilità di presentare il

[180] Il diritto all'informazione sulle modalità d'uso dei dati personali (art.13), e la necessità del consenso informato (art. 23) – nei casi in cui è previsto come presupposto per poter attivare il trattamento –, sebbene siano collocati nel titolo relativo alle regole generali per il trattamento dei dati, costituiscono una parte integrante dei diritti riconosciuti alla persona fisica, alla persona giuridica, l'ente o l'associazione cui si riferiscono le notizie catalogate.

[181] BUTTARELLI, *Banche dati e tutela della riservatezza. La* privacy *nella società dell'informazione*, Milano, 1997, 201; C. FILIPPI, *Il trattamento dei dati personali per finalità di giustizia*, in *La tutela della riservatezza*, a cura di LOIODICE – SANTANIELLO, Padova, 2000, 311; MAIETTA, *I trattamenti in ambito giudiziario, da parte delle forze di polizia e per la difesa dello Stato*, in CARDARELLI – SICA – ZENO-ZENCOVICH, *Il codice dei dati personali*, cit., 166; PERRI, Privacy, *diritto e sicurezza informatica*, Milano, 2007, 55.

[182] FRATUCELLO, *La protezione dei dati personali come limite all'accertamento penale nel codice della* privacy, in, *Protezione dei dati personali e accertamento penale*, cit., 118.

[183] Il diritto d'accesso ai dati personali è limitato anche nel caso in cui le informazioni siano raccolte da un avvocato difensore, limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive. Vedi art. 8 lett. e) Testo unico.

[184] L'art. 55 prevede un'eccezione per l'obbligo di comunicazione al garante – previsto dall'art. 39 –, nel caso in cui la polizia giudiziaria effettui un trattamento di dati

ricorso contro il trattamento illegittimo di dati[185], risultino inconciliabili con i trattamenti d'informazioni personali effettuati dalla polizia o dall'autorità giudiziaria.

Tuttavia, la tendenziale non applicabilità dei principi posti nel Testo unico a tutela della *privacy,* incontra un limite negli artt. 11 e 3. L'art. 3 fissa il principio di necessità: vale a dire che il trattamento dei dati riservati segua ad una valutazione sulle esigenze reali del caso concreto in cui deve essere effettuato. In quest'ottica il *database* dovrà rispondere ad una logica di urgenza e, laddove possibile, utilizzare "dati anonimi o modalità che permettano di identificare l'interessato solo in caso di necessità." Come visto in precedenza, l'art. 11, richiama i parametri fondamentali che sovrintendono al trattamento dei dati privati, quando questi vengono raccolti ed elaborati presso archivi elettronici.

Per quanto riguarda i casi di passaggio d'informazioni da una banca dati esterna, pubblica o privata, a *database* gestiti direttamente dalla polizia o dall'autorità giudiziaria, gli artt. 48 e 54 del Testo unico prevedono che questo avvenga nel rispetto delle leggi e dai regolamenti posti a tutela della riservatezza dei cittadini[186].

1.1)(segue) Il Centro elaborazione dati presso il dipartimento della pubblica sicurezza del ministero degli interni

La legge n.121 del 1981 – che ha istituito il centro di elaborazione dati presso il dipartimento della pubblica sicurezza del ministero degli interni – si pone in connessione diretta con quanto appena accennato a proposito delle banche dati utilizzate dalle forze di polizia nel corso dell'attività investigativa. Tale legge può

---

personali "quasi sensibili" previsti dall'art. 17, con "banche dati basate su particolari tecniche di elaborazione delle informazioni e con l'uso di particolari tecnologie" .

[185]Il soggetto interessato può sempre presentare al garante segnalazioni o reclami, sia per i trattamenti effettuati dalle forze di polizia che per quelli realizzati in ambito giudiziario. Vedi cap. IV, par. 3.3.

[186] L'art. 54 del Testo unico , prevede che le informazioni personali raccolte da banche dati esterne devono essere strutturate "in conformità alle vigenti disposizioni di legge o di regolamento"; allo stesso modo la stipula di eventuali accordi, volti ad agevolare la consultazione di tali archivi elettronici, deve rispettare come riferimento minimo "i principi di cui agli artt. 3 e 11" del Testo unico sulla *privacy*.

essere considerata come in un rapporto di *genus - species* col Testo unico sulla *privacy*, visto che quest'ultimo traccia i limiti del trattamento dei dati personali nell'ambito delle attività di prevenzione, accertamento e repressione dei reati, mentre la legge n. 121 del 1981 indica regole determinate, relative alla conservazione e all'utilizzo dei dati raccolti negli archivi elettronici a disposizione della polizia. L'intreccio tra le due discipline è evidenziato dal rimando chiaro contenuto nella lettera del Testo unico, oltreché dalla modulazione delle garanzie sostanziali previste per la banca dati del C.E.D. in linea con quanto disposto in materia dalla legge sulla protezione dei dati personali[187].

Il profilo che preme rimarcare in questa sede, è l'esplicita previsione – già contenuta nella stesura originaria della norma, in anni in cui nel nostro ordinamento giuridico mancava una disciplina organica in materia di *privacy*[188] – di norme preposte alla regolamentazione del rapporto tra protezione delle informazioni personali e *database* utilizzati dalla polizia giudiziaria. In linea con questo principio la legge *de qua* prevede un controllo sulla banca dati da parte dell'autorità garante per la *privacy*, oltre alla tutela del diritto alla cancellazione dei dati erronei, incompleti o illegittimi.

La banca dati del C.E.D. provvede alla raccolta, ripartizione e custodia di informazioni e dati, forniti, in particolare, dalle forze di polizia in materia di tutela dell'ordine, della sicurezza pubblica e repressione della criminalità. In quest'ottica la finalità principale del *database* è individuabile, nell'esigenza di avere un polo

[187] Alla banca dati del C.E.D. si applicano le regole del codice di protezione dei dati personali previste per le banche dati effettuati in ambito giudiziario. Vedi par. 1.

[188] La versione primigenia della legge del 1981, può essere considerata a tutti gli effetti come una disposizione antesignana – quantomeno della *ratio* – dell'art. 11 del Testo unico sulla protezione dei dati personali e diritto di accesso agli stessi. Secondo l'originaria elaborazione del comma 5 dell'articolo 10, chiunque venisse a conoscenza, dagli atti o nel corso di un procedimento giurisdizionale o amministrativo, dell'esistenza di dati che lo riguardavano da lui ritenuti erronei o incompleti o illegittimamente raccolti, poteva avanzare istanza al tribunale penale – nel cui circondario era pendente il procedimento medesimo – per la cancellazione dei dati erronei e illegittimamente raccolti o per l'integrazione di quelli incompleti. In tali situazioni il soggetto interessato tutelava – con la mediazione del tribunale penale – il proprio diritto all'autodeterminazione informativa. CAROTA, *Prime ipotesi applicative della normativa sulle banche dati contro la criminalità*, in *Foro it.* , 1986, II, 138; DINACCI, *Elaborazione elettronica dei dati presso il ministero dell'interno ed orientamenti giurisprudenziali in tema di procedure di correzione*, in *Giust. pen.*, 1987, III, 398; GIANNANTONIO, *Le banche dati contro la criminalità*, in *Cass. pen.*, 1985, 1254.

centralizzato di notizie personali al quale fare riferimento nel caso di indagini giudiziarie svolte per la prevenzione e l'accertamento dei reati[189].

Il complesso sistema informativo a disposizione delle forze di polizia dislocate sul territorio nazionale, è caratterizzato da una struttura articolata, integrata da informazioni provenienti, sia dall'attività operativa svolta nel corso delle indagini, che da banche dati esterne interfacciate con quella del C.E.D. E' necessario evidenziare come la possibilità di ottenere notizie derivanti da documenti conservati da soggetti pubblici o privati estranei alle forze di polizia, faciliti enormemente la canalizzazione dei dati utili verso gli organi preposti al compimento delle attività di repressione e accertamento dei reati, recando senza dubbio un beneficio importante per la celere esecuzione delle operazioni di indagine[190]. Tale patrimonio di dati può essere definito come un "*network* informativo complesso", costruito da "notizie risultanti da documenti […] conservati dalla pubblica amministrazione o da enti pubblici, o risultanti da sentenze o provvedimenti dell'autorità giudiziaria o da atti concernenti l'istruzione penale o da indagini di polizia" (art. 7) . Tutte le informazioni relative alle operazione d'indagine, unite a quelle delle banche dati esterne collegate, costituiscono un polo esclusivo di riferimento, di assoluto interesse investigativo, che, grazie alla possibilità di mettere in relazione tra loro dati eterogenei[191], permette all'utente di svolgere particolari ricerche integrate.

Il sistema nel suo insieme viene comunemente indicato con la sigla S.D.I. (sistema d'indagine), in quanto permette di avere a disposizione in un unica banca dati, vari tipi di informazioni, consultabili da parte di tutti gli organi investigativi

[189] La lett. a dell'art. 6, riconosce nella "classificazione, nell'analisi e nella valutazione delle informazioni e dei dati" l'obiettivo principale dell'istituzione del centro di raccolta.
[190] La possibilità di disporre di notizie provenienti da banche dati esterne alle forze di polizia è regolamentata dall'art. 54 comma 1 del Testo unico sulla *privacy*, che prevede l'ingresso di informazioni di questo tipo a fronte di convenzioni o accordi speciali che tengano conto dei principi stabiliti dagli artt. 3 e 11dello stesso Testo unico . In particolare possono essere attivate connessioni dirette tra C.E.D. ed altri centri di elaborazione pubblici e privati come ad esempio: le banche dati delle camere di commercio, l'anagrafe nazionale dei protesti, le imprese Italiane operanti con l'estero, il C.E.D della suprema Corte di Cassazione, il pubblico registro automobilistico (PRA - ACI), l'anagrafe tributaria, INPS, la banca dati della motorizzazione civile, la banca dati dell'amministrazione penitenziaria, la banca dati dell'Italgas, nonché gli elenchi di tutti gli abbonati e gli acquirenti del traffico prepagato della telefonia mobile secondo quanto previsto dall'art. 55 del d.lg. n.259, 2003, codice delle comunicazioni elettroniche.
[191] Vedi cap. I, par. 1.

appartenenti alle forze di polizia[192]. Il contenuto a disposizione degli utenti può essere ricondotto a due categorie fondamentali: i fatti, e i provvedimenti, cioè atti formali emessi dalle autorità competenti nei confronti di soggetti od oggetti coinvolti in uno specifico reato od evento[193]. Per quanto riguarda i fatti, il presupposto per l'inserimento di un informazione nell'archivio elettronico non è dato necessariamente da un reato o dalla denuncia di un reato, bensì dal c.d. "fatto S.D.I.", vale a dire un accadimento che si riferisce globalmente a qualsiasi avvenimento di interesse per le forze di polizia[194].

Inoltre all'interno dell'archivio elettronico possono confluire le informazioni e i dati in possesso delle polizie degli Stati appartenenti alla Comunità economica europea, nonché di ogni altro Stato con il quale siano raggiunte specifiche intese. Tuttavia, in certi casi la natura del dato può costituire un limite alla raccolta, in quanto non possono essere collezionate notizie su cittadini per il solo fatto della loro razza, fede religiosa od opinione politica o della loro adesione ai principi di movimenti sindacali cooperativi, assistenziali e culturali[195].

A ben vedere, la condivisione di informazioni tra le forze di polizia dislocate sul territorio nazionale – attivata grazie alla banca dati centralizzata del C.E.D. – costituisce un supporto importante nella lotta al crimine di stampo nazionale e transazionale, considerata la facilità con la quale i moderni *software* di catalogazione riescono a registrare ed irradiare a distanza le notizie personali utili

[192] Le informazioni dello S.D.I., sono esaminabili da parte: della polizia di Stato, dei carabinieri, della guardia di finanza, della polizia penitenziaria, della direzione investigativa antimafia, del corpo forestale dello Stato, delle capitanerie di porto e, indirettamente, dai corpi di polizia locali. FRATUCELLO, *La protezione dei dati personali come limite all'accertamento penale nel codice della* privacy, cit., 137.

[193] SERROTTI, *Libertà di informazione e libertà informatica:la tutela della riservatezza*, cit., 87.

[194] Tale informazione può riguardare: il luogo in cui è accaduto il fatto, la città, la via, il numero civico, l'ubicazione, l'ora. Per quanto riguarda gli individui coinvolti nel "fatto S.D.I.", possono essere inseriti nella banca dati in qualità di: denuncianti, vittime, autori di reati o persone denunciate in quanto presunti autori. Inoltre sulle persone vengono raccolte informazioni relative a caratteristiche socio demografiche, e altre di interesse investigativo, come le particolarità biometriche necessarie per l'identificazione personale degli indagati o eventuali precedenti penali, o ancora provvedimenti emessi dalle autorità competenti. Anche per gli oggetti rinvenuti nel corso delle indagine è possibile una raccolta di notizie dettagliate; così può suscitare l'interesse degli investigatori: la cilindrata, la marca, il modello , la targa di un automobile o la matricola e il tipo dell'arma utilizzata per commettere il reato.

[195] FERRARO, *C.E.D. del ministero dell'interno e tutela del cittadino*, in *Cass. pen.*, 1991, 826.

alle indagini. Per questo motivo, nell'ambito delle forze di polizia l'accesso ai repertori informativi viene consentito solo ed unicamente a particolari soggetti, impegnati specificamente nell'esercizio delle funzioni di cui all'art. 56 c.p.p. o posti in una posizione gerarchica di particolare responsabilità come gli ufficiali di polizia giudiziaria, e quelli di pubblica sicurezza, i funzionari dei servizi di sicurezza, nonché agli agenti di polizia giudiziaria debitamente autorizzati. Peraltro anche l'autorità giudiziaria può consultare il contenuto del C.E.D. , per effettuare gli accertamenti necessari allo svolgimento dei procedimenti in corso e nei limiti stabiliti dal codice di rito[196].

Oltre a precisare l'ampia portata delle informazioni che convergono all'interno dell'archivio informatico, la legge istitutiva del C.E.D. prevede altresì una serie di tutele e garanzie per i dati in esso contenuti. A tal proposito l'art.10, determina la modalità di acquisizione delle informazioni personali nel corso di un procedimento penale, precisando come questa possa avvenire solo attraverso le fonti originarie dei dati contenuti nella banca di raccolta. Per di più, il legislatore indica alcune forme di controllo e modalità di organizzazione dei repertori informativi, in modo tale da garantirne la genuinità e la correttezza nel caso di una utilizzazione nel corso di procedimento giudiziario. In quest'ottica, prevede la possibilità dell'intervento del garante per la protezione dei dati personali – attraverso i meccanismi previsti dal Testo unico – ed istituisce una commissione tecnica, – presso il dipartimento di pubblica sicurezza – competente per l'attuazione dei principi stabiliti dalla legge *de qua*. In particolare tra i compiti assegnati alla commissione, c'è la predisposizione del limite massimo di conservazione dei dati; tale valutazione dovrà tener conto delle esigenze del procedimento al quale si riferisce la catalogazione dell'informazione, in modo tale da far coincidere la realizzazione dello scopo con la scadenza del termine.

Inoltre, per quanto riguarda il rapporto tra banca dati e soggetto interessato, la legge prevede in capo a quest'ultimo la possibilità di sollecitare chiarimenti sui dati personali contenuti nel C.E.D. Invero qualora intenda solo chiedere informazioni, l'interessato dal trattamento potrà rivolgersi direttamente alla direzione centrale della polizia anticrimine per verificare se ed in che modo,

[196] A.A.DALIA, *Il controllo giurisdizionale sulla banca dati del ministero dell'interno*, in *Dir. inf.*, 1986, 577.

all'interno della banca dati, risultino notizie che lo riguardano[197]; nel caso in cui scopra, tra i dati ad esso riferiti, delle imprecisioni, o gli estremi di una raccolta effettuata in modo illegittimo, potrà rivolgersi al tribunale del circondario presso il quale esercita le proprie funzioni il titolare del trattamento per chiedere che il dato venga corretto, integrato o cancellato. Peraltro, il riferimento alla legittimità delle informazioni contenute nel C.E.D., va direttamente collegato al principio di finalità che sovrintende alla creazione della banca dati. In quest'ottica tutte le informazioni dovranno essere catalogate solo per far fronte agli scopi precisi indicati dalla legge istitutiva, per contro, tutte le notizie diverse, cioè che non rispondano alle caratteristiche previste, potranno essere dichiarate illegittime, e quindi, cancellate.

L'articolo *de quo* contiene pure un riferimento al possibile esercizio, da parte di "chiunque venga a conoscenza dell'esistenza di dati personali che lo riguardano", della richiesta di rettifica, integrazione, cancellazione o trasformazione delle informazioni, che si ritengono essere erronee, incomplete o illegittime; in tal caso l'istanza potrà essere fatta direttamente al tribunale del luogo ove risiede il titolare del trattamento, anche senza la presentazione preliminare della richiesta di informazioni sul contenuto della banca dati alla direzione centrale della polizia anticrimine.

2) Identità informatica e processo penale: scenari di una convivenza possibile

L'indicazione che si trae dall'analisi sistematica delle norme contenute negli artt. 46 - 49 e 53 - 57, dedicati dal Testo unico al trattamento de dati personali effettuato in ambito giudiziario, e dalle forze di polizia, è piuttosto chiara. Per tali situazioni il legislatore ha limitato l'operatività di alcune garanzie

[197] La risposta del C.E.D. interviene entro venti giorni dalla richiesta di informazioni, "può non essere data nel caso in cui ciò pregiudichi azioni od operazioni a tutela dell'ordine o della sicurezza pubblica; in tal caso deve esserne data comunicazione al garante. Tale norma si spiega con l'esigenza, per le forze di polizia, di evitare un utilizzo pretestuoso del diritto d'accesso, magari da parte di chi sia oggetto di indagine; la previsione di un termine più ampio rispetto ai cinque giorni fissato in via generale per l'esercizio di tale diritto, nei confronti di tutti gli altri trattamenti, si giustifica proprio con la necessità di esperire i necessari accertamenti anche nei confronti del richiedente". ACCIAI, *Privacy e banche dati pubbliche*, cit., 242.

connesse al controllo diretto delle informazioni da parte del soggetto interessato, assicurando così, al diritto alla *privacy*, solo un livello minimo di protezione[198]. In particolare, sono fatti salvi i principi contenuti nell'art. 11 del Testo unico, relativi alle modalità di trattamento e ai requisiti fondamentali dei dati sottoposti a processi di archiviazione.

Tale regola, inserita come prima disposizione tra le quelle generali applicabili a tutti i tipi di trattamento, costituisce la base normativa di riferimento per ogni forma di elaborazione delle informazioni riservate. Invero, l'art. 11 indica in termini di principio, i presupposti fondamentali per realizzare una forma di utilizzazione garantita delle notizie personali; focalizzando nell'elencazione dei principi di finalità, correttezza, e liceità i tre capisaldi irrinunciabili nelle operazioni di trattamento dei dati. La formulazione adottata dal legislatore nazionale riporta alla mente lo stile già adoperato, in sede europea, dalla Convenzione di Strasburgo e dalla direttiva 95/46 CE, per individuare il livello qualitativo minimo dei dati da sottoporre ad elaborazione automatizzata. Come indicato dalle disposizione transazionali, anche l'articolo del Testo unico collega la realizzazione di quanto previsto in via generale alla pronuncia di regole successive d'attuazione; dato che la concretizzazione dei parametri determinati dalla cornice normativa "in bianco", contenuta nell'elencazione effettuata dal primo comma dell'articolo, si riflette nelle norme peculiari stabilite dal legislatore, per disciplinare nello specifico ciascun tipo di trattamento di notizie individuali[199].

La frase "in ambito giudiziario" utilizzata dal Testo unico per identificare le regole applicabili a tali trattamenti è da intendere in senso ampio[200], inclusiva perciò anche delle attività di archiviazione di informazioni personali effettuate nel corso del processo penale[201] dalle forze di polizia o dall'autorità giudiziaria allo scopo di raccogliere e catalogare i dati necessari per prevenire, reprimere o accertare reati. Pertanto anche in tali situazioni, l'attuazione dei principi contenuti nell'art.11, avviene grazie alla pronuncia di norme particolari dirette a garantire la tutela della *privacy* dei dati raccolti in archivi elettronici nel corso del

[198] MAIETTA, *I trattamenti in ambito giudiziario*,cit., 168.
[199] FRATUCELLO, *La protezione dei dati personali come limite all'accertamento penale nel codice della* privacy, cit., 124.
[200] MAIETTA, *I trattamenti in ambito giudiziario*,cit., 167.
[201] Anche per l'elaborazione di informazioni connesse allo svolgimento del procedimento penale sono attuabili i principi generali fissati dall'art. 11 del Testo unico.

procedimento. In questi termini si è espressa la Corte Costituzionale, che in una recente sentenza ha osservato come " la pressante esigenza di dare al diritto fondamentale alla riservatezza una tutela più intensa, rispetto a quella rivelatasi insufficiente, del recente passato, induce a ritenere non irragionevoli particolari modalità di trattamento del materiale probatorio, che riescano a contemperare tutti i diritti e principi fondamentali coinvolti in questa delicata materia. Le modalità di bilanciamento tra i suddetti diritti e principi sono molteplici e non spetta alla Corte Costituzionale, ma al legislatore individuare possibili soluzioni nell'ambito della disciplina del processo penale"[202].

A tal proposito, occorre sottolineare come le varie fasi processuali siano caratterizzate dalla raccolta continua di informazioni personali, attraverso azioni, che a più livelli e con differente intensità, limitano la riservatezza dei cittadini; cosicché, appare piuttosto difficile individuare un punto di equilibrio tra esigenze procedimentali e tutela garantita al diritto alla riservatezza, soprattutto in relazione all'uso dei dati personali contenuti in banche dati. D'altro canto, non va dimenticato che il legislatore in questi anni ha regolamentato l'acquisizione di dati personali provenienti da banche di raccolta criminalistiche o esterne[203], attraverso l'individuazione di regole poste a garanzia del diritto alla *privacy*. Costituiscono un esempio di questo impegno legislativo la recente introduzione della legge istitutiva della banca dati del dna[204], la legge n.121 del 1981 istitutiva del C.E.D[205], la modifica dell'art. 240 comma 2 c.p.p. relativa all'inutilizzabilità delle intercettazioni illegali e dei documenti formati attraverso la raccolta illegale d'informazioni[206], e l'art. 132 del Testo unico, che fissa le regole di acquisizione dei dati esterni delle comunicazioni telefoniche o telematiche nel corso del procedimento penale. A ben vedere, il filo conduttore che collega tutti questi interventi normativi pare rintracciabile nell'attuazione degli "obblighi di

[202] Corte cost., 22 aprile 2009 n.173, in *G.U., serie spec.*, I, 2009, n. 24, 11; TONINI, *Manuale di procedura penale,* X ed., Milano, 2009, 351.
[203] Le autorità inquirenti possono trarre informazioni utili allo sviluppo del procedimento anche da banche dati esterne. Invero i dati utilizzabili possono arrivare all'autorità giudiziaria o alle forze di polizia, attraverso la consultazione di altri *database* già esistenti, gestiti da soggetti pubblici o privati estranei allo svolgimento delle indagini preliminari.
[204] Vedi cap. IV.
[205] Vedi par. 1.1.
[206] Vedi par. 2.2.

condotta"[207] stabiliti dall'art. 11 Testo unico sulla *privacy*. Pertanto, in quest'ottica dovrebbe essere interpretata anche la regolamentazione del flusso d'informazioni provenienti dai tabulati delle comunicazioni telefoniche e telematiche. Invero, il legislatore, per disciplinare queste situazioni, ha istituito un termine di conservazione dei dati *ad hoc*, strutturato in base ai tempi e alle dirette esigenze del procedimento; in tal modo, ha tutelato l'integrità di informazioni potenzialmente impiegabili per le attività di accertamento del fatto reato, attraverso la "messa in sicurezza" di un dato che diversamente il titolare del trattamento avrebbe potuto cancellare in tempi più rapidi; inoltre, così facendo ha riconosciuto il diritto soggettivo alla conservazione a termine dell'informazione personale, – il diritto all'oblio – anche nel caso in cui questa debba essere utilizzata nel corso di un procedimento penale.

In queste ipotesi il titolare del trattamento deve conservare le informazioni relative al traffico telefonico – numero delle utenze, ora e durata della chiamata e i dati relativi alle chiamate senza risposta[208] – per un tempo massimo di quarantotto mesi, e mantenere quelle attinenti al traffico telematico per dodici mesi.

Per i primi ventiquattro mesi, nel caso di dati relativi al traffico telefonico, o sei mesi, nel caso di informazioni attinenti alle comunicazioni telematiche, l'acquisizione dei dati deve essere preceduta dalla pronuncia di un decreto motivato del pubblico ministero, che può essere emesso anche in seguito ad un'istanza presentata dall'imputato, dalla persona offesa o dalle altre parti private. Inoltre in questo lasso di tempo il difensore dell'imputato è legittimato a presentare una richiesta di acquisizione diretta al titolare del trattamento; in tal caso però dovrà limitare l'istanza ai soli dati delle chiamate in uscita, relative all'utenza del proprio assistito. Per quanto riguarda un eventuale indagine sui dati in entrata, questa potrà essere condotta a condizione che il difensore dimostri che l'acquisizione delle notizie *de quibus* sia necessaria per svolgere le indagini difensive[209]. Nei mesi successivi di conservazione – ulteriori ventiquattro per i dati del traffico telefonico o sei per le comunicazioni avvenute telematicamente –

[207] In questi termini MAIETTA, *I trattamenti in ambito giudiziario*,cit., 167.
[208] Le chiamate senza risposta hanno una valenza investigativa fondamentale per alcune tipologie di indagine, come ad esempio in tutti quei casi in cui con una semplice chiamata si può inviare un segnale concordato o addirittura attivare a distanza un ordigno esplosivo.
[209] L. FILIPPI, sub *art. 266 c.p.p.*, in *Codice di procedura penale commentato*, a cura di GIARDA – SPANGHER, Milano, 2007, 1910.

l'acquisizione dei dati potrà avvenire solo su istanza presentata al giudice competente per fase ed è condizionata alla sussistenza di sufficienti indizi sull'esistenza dei reati previsti dall'art. 407 comma 2 lett. a c.p.p. nonché dei delitti commessi in danno di sistemi informatici o telematici. Peraltro è prevista una procedura d'urgenza per tutte quelle situazioni in cui è necessario acquisire immediatamente i dati, e non si possa attendere il provvedimento del giudice; in tali casi il pubblico ministero può "disporre l'acquisizione dei dati relativi al traffico telefonico con decreto motivato che è comunicato immediatamente, e comunque non oltre ventiquattro ore, al giudice competente per i rilascio dell'autorizzazione in via ordinaria. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del p.m. non è convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati"[210].

In tutti i casi elencati l'assunzione delle informazioni detenute dal gestore titolare dei dati relativi alle comunicazioni telefoniche e telematiche avviene nel rispetto dei principi generali previsti per il trattamento delle informazioni personali. In tali situazioni il legislatore ha garantito la custodia del dato personale attraverso l'individuazione di un tempo limite di mantenimento, in ossequio a quanto previsto dall'art. 11 del Testo unico sulla fissazione di un termine massimo per la durata del trattamento delle notizie riservate. In altre parole si può dire che la previsione di una scadenza speciale per la conservazione dei tabulati telefonici o telematici, scaturisca dalla necessità di avere dei tempi calibrati rispetto al fine per cui tali dati devono essere utilizzati; *id est* per le attività connesse all'accertamento dei reati.

Le considerazioni fatte fin'ora spingono a porre in termini più generali la questione relativa ai rapporti tra l'art. 11 del Testo unico, e le attività procedimentali, legate all'acquisizione di dati personali provenienti da archivi elettronici. Il nodo ermeneutico da risolvere può essere riassunto in un quesito fondamentale: può essere utilizzato nel corso del processo penale, un dato proveniente da una banca dati che non rispetti i principi stabiliti dall'art. 11 del Testo unico sulla *privacy*?

[210] L. FILIPPI, sub *art. 266 c.p.p.*, in *Codice di procedura penale commentato*, a cura di GIARDA – SPANGHER, cit., 1911.

2.2)(segue) Riflessioni sull'art. 240 comma 2 c.p.p.

Prima di rispondere all'interrogativo posto in precedenza, vale la pena precisare come l'ingerenza dell'autorità giudiziaria nel vissuto dei cittadini – espresso sotto forma di dati contenuti in elaboratori elettronici – sembri un'attività necessaria per garantire la sicurezza collettiva. Allo stesso modo, tuttavia, non si nutrono dubbi sul fatto che occorra determinare in modo chiaro dei parametri per stabilire quale sia il "requisito minimo" che deve avere una banca di raccolta di informazioni personali per essere identificata come un "*database* produttore" di dati utilizzabili[211] in dibattimento.

Come visto in precedenza l'art. 240 c.p.p., impedisce l'ingresso nel processo penale di documenti, supporti e degli atti concernenti intercettazioni telefoniche o telematiche illegali e documenti formati attraverso la raccolta illegale di informazioni. In tali situazioni il pubblico ministero chiede al giudice per le indagini preliminari la distruzione dei dati, dei quali inoltre non può essere utilizzato il contenuto ed "è vietato effettuare copia in qualunque forma e in qualunque fase del procedimento".

Uno degli elementi che ha suscitato maggiori perplessità in dottrina[212] sull'interpretazione della norma *de qua* è legato al corretto significato da attribuire alla parola "illegale", usata per identificare i documenti e le intercettazioni inutilizzabili da sottoporre a sequestro e successiva distruzione. Secondo alcuni autori tale termine è stato impiegato in modo atecnico e confuso col concetto di illiceità: "la verità è che il legislatore ha scritto qualcosa di diverso da ciò che intendeva dire: ha scritto illegale ma intendeva illecito e ciò è grave per chi legifera"[213]. L'errore di valutazione non è di poco conto, considerato che il

[211] Vedi par. 3.

[212] CONTI, *Le intercettazioni illegali:* lapsus linguae *o nuova categoria sanzionatoria?*, in *Dir. pen. proc.*, 2007, 163; L.FILIPPI, *Distruzione dei documenti e illecita divulgazione di intercettazioni: lacune ed occasioni perse di una legge nata già vecchia*, ivi, 2007, 152.

[213] Lo sbaglio del legislatore è stato quello di porre l'accento solo sugli effetti da evitare senza considerare i possibili riflessi che la dichiarazione di inutilizzabilità rafforzata dalla distruzione dei dati raccolti poteva produrre sullo svolgimento del processo penale. Invero l'eliminazione dell'informazione unita alla rinuncia a qualsiasi notizia derivante dal dato illecito rispondono solo ad esigenze direttamente connesse alla tutela della

significato del vocabolo illegale abbraccia in modo ampio il riferimento a tutti i comportamenti *contra ius*, comprendendo sia il concetto di illiceità – violazione delle norme del codice penale sostanziale – , che quello di illegittimità inteso come inosservanza delle norme processuali[214]. Pertanto una interpretazione estensiva della norma porterebbe a considerare come presupposti oggettivi per la dichiarazione di inutilizzabilità tutte quelle situazioni che infrangono una norma qualsiasi di carattere sostanziale o processuale. Cosicché, in teoria, tutte le regole previste dal Testo unico sulla *privacy* e relative alle specifiche modalità di trattamento in ambiti particolari, potrebbero rappresentare una causa di "illegalità-illiceità" tale da portare alla dichiarazione di inutilizzabilità del dato[215]. Per evitare l'allargamento incontrollato della fattispecie, la dottrina maggioritaria[216] ha interpretato in senso restrittivo la lettera dell'art. 240 comma 2 c.p.p., circoscrivendo il riferimento alla documentazione e alle intercettazioni illegali, solo ai casi in cui tali attività concretizzino dei reati.

Peraltro è stata oggetto di discussione[217] anche la scelta di affidarsi al procedimento in camera di consiglio la verifica dell'illegalità dei dati personali, dato che le regole generali previste dall'art. 127 c.p.p. , sembrano del tutto inadatte all'acquisizione di una prova[218]. Invero il modello indicato dalla norma *de qua* non garantisce il contraddittorio, in quanto non sono contemplati eventuali rinvii del procedimento camerale dovuti ad un legittimo impedimento delle parti[219], che peraltro sono sentite dal giudice solo se compaiono o ne fanno esplicita richiesta[220].

---

riservatezza. L.FILIPPI, *Distruzione dei documenti e illecita divulgazione di intercettazioni: lacune ed occasioni perse di una legge nata già vecchia*, cit., 152.

[214] CONTI, *Le intercettazioni illegali*, cit., 163.

[215] CONTI, *Le intercettazioni illegali*, cit., 159.

[216] BRICHETTI – PISTORELLI, *La distruzione immediata della prova rischia di ledere i diritti dell'imputato*, in *Guida dir.*, 2006, n.32, 22; CHIAVARIO, *Passi avanti sulle intercettazioni illegali ma c'è bisogno di un ampio ripensamento*, ivi, 2006, n.39, 13; CONTI, *Le intercettazioni illegali*, cit., 160; L. FILIPPI, *Distruzione dei documenti e illecita divulgazione di intercettazioni*, cit., 152; FRIGO, *Ridotti gli spazi della tutela penale*, in *Guida dir.*, 2006, n.47, 27.

[217] BRICHETTI – PISTORELLI, *La distruzione immediata della prova rischia di ledere i diritti dell'imputato*, cit., 25.

[218] CHIAVARIO, *Passi avanti sulle intercettazioni illegali*, cit., 41.

[219] ROCCA, sub *art. 127 c.p.p.*, in *Codice di procedura penale commentato*, a cura di GIARDA – SPANGHER, cit., 885.

[220] Buona parte di tali imprecisioni, paiono attribuibili al clima emergenziale che ha preceduto l'approvazione dell'articolo, poiché la norma è nata col preciso scopo di porre rimedio ad alcune situazioni di particolare allarme sociale, verificatesi negli ultimi

Il procedimento per l'eliminazione dei dati personali è scandito da tempi ben precisi, ed è preceduto dalla conservazione dei *dossier* illeciti, effettuata dal pubblico ministero in un luogo sicuro e in assoluta segretezza, dato che i dati devono essere conosciuti dalla sola autorità giudiziaria, e non possano essere mostrati né ai soggetti interessati, né al giudice per le indagini preliminari. Sebbene tale accorgimento, voluto dal legislatore, tenda ad evitare che le notizie personali possano essere divulgate all'esterno, la contromisura individuata pare piuttosto forte, in quanto l'opposizione indiscriminata del segreto limita il diritto di difesa esercitabile dalle persone interessate. Invero queste ultime possono avere una diretta conoscenza delle notizie che li riguardano solo nel corso del procedimento in camera di consiglio necessario per poter procedere all'eliminare definitiva dei dati illeciti[221]. Occorre evidenziare, infatti, come il momento successivo al congelamento di tali notizie, coinvolga direttamente il g.i.p, che entro quarantotto ore, calcolate a partire da quando il p.m. ha acquisito le informazioni, dovrà ricevere la richiesta necessaria ad aprire la fase camerale, prodromica alla pronuncia del provvedimento di distruzione dei dati[222]. L'eventuale cancellazione, risulterà da un verbale nel quale dovranno essere indicate tutte le attività svolte nel corso del procedimento, ma che non dovrà recare alcuna traccia del contenuto delle notizie personali eliminate. Esso costituisce pertanto un atto surrogatorio del dato illecito, visto che l'esistenza di questo verrà provato attraverso la documentazione della procedura di eliminazione posta in essere nel corso del procedimento in camera di consiglio[223]; inoltre dovrà

---

periodi, e relative ad attività illecite di intercettazione e dossieraggio di informazioni personali. In particolare lo scandalo Telecom – Sismi relativo alle intercettazioni illegali effettuate da alcuni responsabili della sicurezza Telecom Italia scoppiato nel settembre 2006, con ventuno arresti di vari dipendenti Telecom, di poliziotti e di militari dei carabinieri e della guardia di finanza.

[221] L. FILIPPI, *Distruzione dei documenti e illecita divulgazione di intercettazioni*, cit., 156.

[222] La procedura di distruzione del dato illecito non fa salva la prova dell'avvenuta condotta illecita, e nemmeno quella dell'innocenza dell'imputato, tanto che " sembra logicamente inconcepibile e oltretutto incostituzionale che la prova dell'innocenza debba andare distrutta e che si debba pronunciare consapevolmente la condanna di un innocente solo per l'altrui comportamento illegittimo. Pertanto […] ogni qual volta dai documenti illeciti emergesse la prova dell'innocenza dell'imputato, non vi può essere dubbio che un ordinamento processuale degno di questo nome non può condannare un imputato che risulta innocente, sia pure tramite una prova viziata". In tal senso, vedi L.FILIPPI, *Distruzione dei documenti e illecita divulgazione di intercettazioni*, cit., 154.

[223] TONINI, *Manuale di procedura penale*, cit., 354.

essere letto in dibattimento, in modo tale da verificare l'effettiva provenienza illecita dei dati contenuti nel documento distrutto[224].

Peraltro i ritmi serrati della procedura di distruzione delle informazioni – il giudice deve decidere entro quarantotto ore dalla richiesta – sembrano impedire una discussione sui contenuti dei dati secretati, pregiudicando, nel caso in cui il dato illecito venga immediatamente distrutto all'esito del procedimento, la concreta operatività di un ricorso in cassazione presentato da un soggetto legittimato[225]. In relazione a quest'ultimo punto, un eventuale sentenza della Corte di cassazione che dovesse riconoscere l'illegittimità del provvedimento conclusivo del procedimento in camera di consiglio, sarebbe del tutto inutile vista l'impossibilità di ripristinare la situazione preesistente a causa dell'irrimediabile eliminazione del dato.

D'altra parte anche la Corte costituzionale, in una recente sentenza[226], ha rilevato la palese inidoneità del procedimento indicato dall'art. 240 c.p.p. I giudici – riprendendo i rilievi sollevati dalla dottrina – hanno sottolineato alcune imperfezioni nella formulazione della norma, legate essenzialmente all'insufficienza delle informazioni contenute nel verbale di eliminazione dei dati illeciti, e all'inadeguatezza della disciplina generale prevista dall'art. 127 c.p.p. per i procedimenti in camera di consiglio, a garantire il contraddittorio nelle attività di acquisizione probatoria. La Corte ha individuato nella sentenza, una serie di correttivi in grado di assicurare il rispetto dei principi costituzionali stabiliti dall'art. 111, anche per le operazioni connesse alla distruzione dei documenti illeciti. A tal fine, i giudici della Consulta hanno affermato l'applicabilità al procedimento, *ex* art. 240 comma 2 c.p.p., delle regole previste per l'udienza dell'incidente probatorio, dal momento che "all'intenzione di dettare una normativa mirata alla formazione della prova anticipata rispetto alle successive fasi del processo, consegue il necessario rispetto dei principi del giusto processo, del diritto di difesa e di azione e dell'effettivo esercizio dell'azione

[224] L'art. 512 comma 1- *bis*, prevede "la lettura dei verbali relativi all'acquisizione ed alle operazioni di distruzione degli atti di cui all'art. 240 c.p.p.".
[225] L. FILIPPI, *Distruzione dei documenti e illecita divulgazione di intercettazioni*, cit., 156.
[226] Corte cost., 22 aprile 2009 n.173, cit., 11 .

penale, che si concretizzano in una rigorosa prescrizione del contraddittorio tra le parti, come quella contenuta nell'art. 401 commi 1 e 2 c.p.p."[227].

Inoltre secondo la Corte, il ruolo di prova sostitutiva del corpo del reato esercitato dal verbale conclusivo della fase camerale, "impone che lo stesso non si limiti a contenere i dati relativi alle modalità e ai mezzi usati ed ai soggetti interessati, ma debba altresì contenere tutte le indicazioni utili ad informare il giudice e le parti del successivo giudizio in merito alle circostanze da cui si possano trarre elementi di valutazione circa l'asserita illiceità dell'attività contestata agli imputati"[228]. In altre parole la Corte puntualizza come l'allargamento del contenuto del verbale sia l'unico modo per poter garantire alle parti, nel corso del processo, gli elementi obiettivi necessari per sostenere le rispettive posizioni, difensive o accusatorie; a tal fine risulterà decisiva l'inclusione nello stesso di tutte le circostanze che hanno caratterizzato le operazioni di intercettazione, detenzione ed acquisizione del materiale per il quale il pubblico ministero ha chiesto l'avvio del procedimento di distruzione, come " i dati conoscitivi sulla natura e sulle caratteristiche formali dei documenti, supporti ed atti (con esclusione, ai sensi del comma 6, di ogni riferimento alle informazioni in essi contenute), da cui, in correlazione alle circostanze di luogo, di tempo, e di contesto della loro acquisizione, si possono trarre elementi di giudizio sulla liceità dei comportamenti degli imputati"[229].

3)L'informazione personale proveniente da una banca dati illecita

L'art. 11 del Testo unico sulla *privacy* contiene una serie di principi generali validi per tutte le banche dati, anche per quelle in cui il grado di applicazione delle disposizioni contenute nel codice di protezione dei dati personali raggiunge livelli minimi; pertanto i dati contenuti in un archivio elettronico dovranno essere sempre il frutto di una raccolta lecita, corretta, rispettosa di un fine prestabilito, e a termine. L'idea che l'informazione personale debba necessariamente provenire da un *database* così strutturato è rafforzata dalla

[227] Corte cost., 22 aprile 2009 n.173, cit., 15.
[228] Corte cost., 22 aprile 2009 n.173, cit., 15.
[229] Corte cost., 22 aprile 2009 n.173, cit., 15.

lettera del secondo comma dello stesso articolo, in base al quale le notizie "trattate in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzate". A ben vedere, tale valutazione potrebbe rappresentare la premessa maggiore di un ragionamento logico deduttivo, in base al quale, se si considerano le caratteristiche su elencate come i requisiti indispensabili per poter individuare una banca dati di raccolta, si deve necessariamente concludere che, le informazioni personali generate da archivi elettronici non in linea con tali principi siano da considerare *tanquam non esset* [230].

Il risultato di tale sillogismo offre lo spunto per ragionare sui riflessi – principalmente in prospettiva *de iure condendo* – che i parametri contenuti nell'articolo *de quo* potrebbero avere sull'inutilizzabilità delle informazioni personali provenienti dai *database* impiegati nel corso di un procedimento penale. Va detto subito, in modo da non creare confusione, che la parola "utilizzabilità" contenuta nel secondo comma dell'articolo *de quo*, non può interpretatarsi in termini processuali, nel senso che la norma non produce un divieto probatorio *ex se*, poiché il legislatore impiega il termine al solo scopo di sottolineare l'importanza della regola generale[231].

Indicate le premesse, occorre sottolineare come tale ragionamento su esposto sia inevitabilmente condizionato da quanto la giurisprudenza costituzionale e la dottrina hanno affermato in questi ultimi anni in materia di prove illecite; in particolare rispetto alla possibilità di rintracciare l'esistenza di un divieto probatorio anche nella violazione di norme differenti da quelle contenute nel codice di rito. La dottrina già sotto la vigenza del codice rocco, aveva classificato i vizi patologici relativi alle prove in due specie. Si parla di "prove illecite" quando sia stata violata una norma penale sostanziale, o meglio quando la commissione di un reato si inserisca nell'*iter* che permette l'ammissione di una

[230] MAIETTA, *I trattamenti in ambito giudiziario,*cit., 176; MORASSUTO, *La difficile convivenza tra garante e magistrato penale*, in *Protezione dei dati personali e accertamento penale*, cit., 157.

[231] Il codice di protezione dei dati personali sceglie una strada "neutra" rispetto alla definizione dell'utilizzabilità in sede processuale dei dati acquisiti indebitamente, rinviando alle fattispecie processuali l'indicazione dei casi specifici. In particolare l'art. 160 comma 6 del T.U. stabilisce che "la validità, l'efficacia e l'inutilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale". MAIETTA, *I trattamenti in ambito giudiziario,*cit., 175.

prova nel processo; sono invece definite "prove illegittime" quelle che presentano un vizio tale per cui nel procedimento di ammissione della prova sia identificabile una violazione di una norma processuale[232].

In assenza di espressa indicazione normativa, nel codice abrogato, vi fu un acceso dibattito che ha visto contrapposti i sostenitori delle due teorie. Da un lato secondo un impostazione dominante, l'ammissibilità delle prove doveva essere giudicata in base alla legge processuale[233]. Si sosteneva infatti, che "per quanto la si cerchi riuscirà impossibile rintracciare nel nostro codice una norma che imponga d'escludere, e in ogni caso d'ignorare, le prove ottenute con un azione illecita: le qualifiche d'ammissibilità e rilevanza appaiono formulate in base a criteri autonomi, endoprocessuali, fuori d'ogni riferimento ai paradigmi del diritto sostanziale"[234].

Ancora secondo questa tesi, tali qualifiche non potevano essere dedotte dai principi costituzionali poiché le norme della Costituzione rappresentano il metro per valutare la validità delle leggi comuni, ma spetta alle leggi comuni del processo stabilire l'ammissibilità o meno delle prove[235]. In conclusione si sosteneva che per decidere sulla validità dell'acquisizione probatoria bisognasse riferirsi al "potere di apprensione coattiva dell'organo giudiziario", come dire che, in una ipotesi di sequestro probatorio eseguito all'esito di una perquisizione illegittima " la chiave sta nel vedere se il giudice avrebbe potuto ordinare il sequestro ; nell'ipotesi affermativa la prova è ammissibile, perché, di fatto, l'esito non eccede la misura del legittimamente conseguibile; e se invece il potere del sequestro non compete neppure al giudice, vale la conclusione opposta […]. Ammesso che l'ausiliare si sia impossessato illegittimamente della prova, l'acquisizione da parte del giudice – che avrebbe potuto disporre il sequestro – interrompe la sequela: l'atto del funzionario era e resta illecito, ma il giudice può disporre validamente della prova perché, nell'acquisirla, agisce secondo la misura dei suoi poteri: il qual concetto affiora immaginosamente dalla formula *male captum bene retentum*"[236].

[232] CORDERO, *Prove illecite*, in *Tre studi sulle prove penali*, Milano, 1963, 147.
[233] CORDERO, *Dialogo sulle prove*, in *Jus,* 1964, 35.
[234] CORDERO, *Prove illecite,* cit., 49
[235] CORDERO, *Prove illecite,* cit., 153.
[236] CORDERO, *Procedura penale,* IX ed. , 1987, 926.

D'altra parte vi fu chi criticò radicalmente tale ricostruzione esegetica, sostenendo che " il principio del libero convincimento del giudice non è vincolato ad un sistema di prove legali […] ma non significa principio per cui il giudice non è vincolato alla legalità nella scelta delle prove e nella loro assunzione […]. Qualora si debba riconoscere che una prova è stata illecitamente ottenuta dall'organo di giustizia […] questa deve considerarsi illegale: e se è illegale non può essere utilizzata"[237].

Un ulteriore profilo volto ad impedire l'ingresso nel processo delle prove illecite è stato desunto dall'art. 13 Cost., a norma del quale gli atti lesivi delle libertà personale, oltre a venire revocati di diritto, restano privi di ogni effetto. Da questa espressione si è, così, tratta la conclusione che la norma configuri un vero e proprio divieto di attribuire rilevanza agli elementi di prova ottenuti con i mezzi illeciti[238].

Negli anni immediatamente successivi, la stessa giurisprudenza costituzionale intervenne sulla questione della rilevanza delle prove illecite nel processo penale.

La Corte, pur dichiarando infondata la questione di legittimità costituzionale – in relazione agli artt. 15 e 24 Cost. – dell'art. 226 comma 4 c.p.p. abr., in tema di intercettazioni telefoniche assunte senza previa autorizzazione dell'autorità giudiziaria, aveva posto in evidenza come "il principio enunciato dal comma 1 dell'art. 15 Cost. sarebbe gravemente compromesso se a carico dell'interessato potessero valere, come indizi o prove, intercettazioni telefoniche assunte illegittimamente senza previa motivata autorizzazione dell'autorità giudiziaria. Se ciò avvenisse, un diritto riconosciuto e garantito come inviolabile dalla Costituzione sarebbe davvero esposto a gravissima menomazione"[239].

Partendo dal presupposto che, in casi simili, si avrebbe non solo un contrasto con la legge penale, ma anche la lesione di un bene costituzionalmente garantito, la Corte costituzionale aveva enunciato un principio di carattere più generale in merito alla problematica delle prove illecite. Si era pertanto stabilito che "le attività compiute in dispregio dei fondamentali diritti del cittadino non

[237] NUVOLONE, *Le prove vietate nel processo penale nei paesi di diritto latino*, in *Riv. dir. proc*., 1966, 448 e 473.
[238] CAPPELLETTI, *Processo e ideologie*, Bologna, 1969, 112; VIGORITI, *Prove illecite e Costituzione*, in *Riv. dir. proc*., 1968, 71.
[239] Corte Cost., 6 aprile 1973, n. 34, in *Giur. cost*., 1973, 316.

possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito"[240].

Attraverso la deduzione dall'art. 15 Cost. di uno specifico divieto di utilizzazione, è stata elaborata la categoria delle cosiddette "prove incostituzionali", cioè di quegli elementi ricavati attraverso un'attività intrapresa in dispregio dei fondamentali diritti dei cittadini, garantiti dalla Costituzione. Ciò equivale a dire che nella categoria delle prove vietate dalla legge debbano in primo luogo rientrare tutte le prove la cui acquisizione comporti la lesione di disposizioni costituzionali inerenti ai diritti di libertà individuale. Peraltro, tale teoria parte da una logica assolutamente condivisibile, se si pensa al fatto che alla norma fondamentale spetta il ruolo di base portante dell'ordinamento giuridico, rispetto al quale tutte le fonti del diritto si devono necessariamente uniformare.

Una simile impostazione avrebbe conseguenze rilevanti nello sviluppo della nostra analisi sul rapporto tra banche dati e processo penale. A ben vedere, l'affermata esistenza di un sistema di "prove incostituzionali" unita al fatto che la dottrina maggioritaria riconosce al diritto alla riservatezza una dignità costituzionale, potrebbe portare dei riflessi dirompenti sul processo penale[241], considerata la tendenziale incompatibilità della tutela del diritto alla *privacy* con le indagini preliminari effettuate sui dati personali.

Peraltro, il dibattito dottrinale, così come l'apporto della giurisprudenza costituzionale, hanno indubbiamente avuto una notevole influenza sull'emanazione delle disposizioni inerenti l'inutilizzabilità nel nuovo codice di rito. La novità di quest'ultimo consiste proprio nell'aver inserito, all'intero del libro terzo dedicato alle prove, l'art. 191 che contempla espressamente l'inutilizzabilità delle prove acquisite in violazione dei divieti stabiliti dalla legge[242].

La previsione di una categoria espressa di invalidità rivolte a sanzionare le irregolarità "tipiche" del procedimento probatorio, ad ogni modo, non ha di certo

[240] Corte Cost., 6 aprile 1973, cit., 338.

[241] E' da considerare incostituzionale anche la norma che contraddice i principi stabiliti dalla C.E.D.U., in virtù del principio della c.d. incostituzionalità derivata, tratto dalla lettera dell'art. 117 Cost., in base al quale " La potestà legislativa è esercitata dallo Stato e dalle regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali."

[242] MENCARELLI, *L'inutilizzabilità e l'acquisizione delle prove nel nuovo sistema processuale*, in *Giust. pen.*, 1989, III, 84.

circoscritto i dubbi e le incertezze circa i confini di applicazione della norma. Posto che per inutilizzabilità si debba intendere una sorta di principio della legalità della prova inteso in senso negativo atto a limitare il principio del libero convincimento del giudice[243], essa ha ad origine l'esigenza di limitare la conoscenza da parte dell'organo giudicante di prove ottenute in dispregio dei diritti fondamentali sanciti nella prima parte della Costituzione[244]. Tuttavia, acquisisce una fondamentale importanza per la materia *de qua*, l'orientamento giurisprudenziale e dottrinario che ammette l'utilizzabilità di prove illegittime in *favorem rei*, salvo si tratti di violazioni di divieti stabiliti a tutela dell'attendibilità dell'accertamento[245].

L'aspetto sul quale si è maggiormente dibattuto concerne, senza dubbio, l'interpretazione dell'espressione "divieti stabiliti dalla legge" contenuta nel primo comma dell' art. 191 c.p.p. .

Una parte della dottrina, rimasta fedele all'interpretazione tradizionale ha ritenuto che la disposizione possa riferirsi esclusivamente "ad ogni ipotesi di inosservanza di un divieto stabilito dalla legge processuale" anche alla luce della stessa rubrica dell'articolo che utilizza la terminologia "prove illegittimamente acquisite"[246].

Altri autori hanno ritenuto, all'opposto, di poter dedurre dall'ampiezza della formula usata dal legislatore della norma una volontà legislativa tesa a non limitare la fonte del divieto alla legge processuale, bensì ad estenderla sino a ricomprendere le violazioni della legge penale sostanziale. A tale conclusione si dovrebbe giungere in ragione della genericità del termine "legge": la pluralità di interpretazioni cui può dar luogo, rende non decisiva anche la stessa portata della rubrica dell'art. 191 c.p.p. [247].

Questa ricostruzione esegetica, sebbene elaborata al fine di ottenere una certa coerenza sistematica interna all'ordinamento, poggia su una debole premessa. Essa si fonda essenzialmente sull'ampiezza del termine legge impiegato

[243] UBERTIS, *La conoscenza del fatto nel processo penale,* cit., 27.
[244] RUGGIERI, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001, 57.
[245] Cass., sez. I, 20 dicembre 1996, in *Giust. Pen.*, 1998, III, 409; in dottrina GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Padova, 1992, 703.
[246] VOENA, *"Atti"*, in *Profili del nuovo codice di procedura penale*, a cura di CONSO – GREVI, Padova, 1990, 156.
[247] NOBILI, sub. *art. 191 c.p.p.* , in *Commento al nuovo codice di procedura penale*, a cura di CHIAVARIO, Vol. II, Torino, 1989, 413.

dal legislatore, ma si espone all'evidente critica per cui, stando così le cose, il divieto ricomprenderebbe tutti i tipi di legge, dalla cui violazione deriverebbero limiti all'utilizzo della prova. Peraltro, la stessa genericità del termine, in mancanza di uno specifico riferimento alla sola legge penale sostanziale, comporterebbe anche l'applicazione dei divieti stabiliti da leggi civili, amministrative o quant'altre previste come tali nel nostro ordinamento, come ad esempio il Testo unico sulla *privacy*.

Pertanto, non sembrano sussistere argomentazioni tali da far ritenere superata l'impostazione tradizionale, ancorché sviluppatasi sotto la vigenza del codice Rocco. Se ne deve dedurre che per definire la portata del divieto di cui all'art. 191 c.p.p. , ancora oggi , è necessario riferirsi esclusivamente alle norme ed ai limiti derivanti dalla legge processuale; così risultano quanto mai attuali le conclusioni cui pervenne un'autorevole dottrina in materia di perquisizioni intrapresa fuori dai casi consentiti dalla legge: "in parole povere, il legislatore punisce l'autore di una perquisizione illecitamente eseguita, ma non ripudia le prove che ne rappresentano il compendio […]. Soluzione di compromesso, si dirà, ma non tanto illogica quanto potrebbe apparire, nel conflitto tra gli interessi dei privati e le esigenze del processo, il punto di equilibrio si può trovare in una reazione penalistica opportunamente dosata all'illecito del funzionario: bandire la prova è rimedio estremo, il cui costo vi è da temere che eccede la misura dell'utile"[248].

3.1)(Segue) L'articolo 11 del Testo unico sulla privacy: alla ricerca del dato inutilizzabile

L'idea che un bilanciamento tra l'utilizzazione delle informazioni personali provenienti da banche dati illecite e processo penale, possa essere ricercato nelle pieghe dell'articolo 11 del Testo unico, prende corpo se si analizza come tale norma cristallizzi i requisiti minimi stabiliti per legge, richiesti ad un *database* per essere considerato come tale. Essi potrebbero rappresentare il paradigma del "*database* utilizzabile", condizionando in modo negativo il

[248] CORDERO, *Prove illecite,* cit., 158.

giudizio su tutte quelle banche dati che forniscono alle autorità inquirenti notizie personali utili per la ricostruzione di un fatto reato, e che non rispettino i parametri stabiliti. Come visto nel paragrafo precedente l'attuazione dei principi *ex* art. 11 passa attraverso la pronuncia di leggi di raccordo indispensabili per calibrare il senso della norma allo specifico trattamento effettuato. In tal senso, anche un eventuale la trasposizione delle regole *de quibus* in divieti probatori, necessiterebbe di un intervento normativo in grado di individuare il livello di lesione della *privacy* capace di condizionare l'utilizzabilità dei dati personali nel corso del processo

In base a quanto affermato, per quanto riguarda le banche dati esterne – quelle create da soggetti estranei al procedimento penale –, si potrebbe ricercare un bilanciamento che tenga conto delle esigenze legate alla protezione della *privacy* dei cittadini e delle necessità connesse all'accertamento del fatto reato, utilizzando i principi contenuti nella lettera dell'articolo 11 come "filtro" delle notizie in entrata verso il processo penale. A tal proposito, si ritiene che le regole elencate dall'articolo *de quo* potrebbero rappresentare la base normativa per identificare un divieto probatorio, che blocchi l'uso dei dati gravemente lesivi del diritto alla riservatezza, provenienti da archivi elettronici: illeciti, clandestini, nati con l'inganno o all'insaputa dell'imputato. Allo stesso modo possono essere considerate anche le banche dati che non garantiscono il diritto soggettivo alla cessazione del trattamento, oppure che non attuano la distruzione delle notizie una volta che il termine per la loro conservazione risulta esaurito.

Peraltro, l'inutilizzabilità rafforzata dalla distruzione dei dati provenienti da *dossier* "illegali", introdotta dalla recente integrazione dell'art. 240 c.p.p., conferma per certi versi il ragionamento su esposto. Il legislatore attraverso questa modifica ha creato un vero e proprio "schermo" al materiale ingresso nella dinamica processuale dei dati personali prodotti dall'attività di *dossieraggio* illegale, in modo tale da proteggere la riservatezza dei cittadini da indebite diffusioni di notizie raccolte in conseguenza di comportamenti illeciti. Poste le premesse, si può considerare come l'impostazione generale data dalla norma, potrebbe rappresentare la soluzione rispetto a quanto appena detto, visto che la previsione di un divieto probatorio per tutti i dati raccolti e trattati in modo illecito sembra voler realizzare un ostacolo all'ingresso nel processo penale di dati personali trattati contro i principi stabiliti dall'art. 11 del Testo unico sulla

privacy. Tuttavia occorre prendere atto di come la costruzione della fattispecie *de qua* risulti alquanto lacunosa da un punto di vista sistematico, poiché – come accennato nei precedenti paragrafi[249] – il fatto di non aver precisato con puntuali riferimenti l'ambito di applicabilità ne condiziona inevitabilmente il senso.

In quest'ottica, alla luce dei rilievi avanzati dalla dottrina e dalla recente sentenza della Corte costituzionale[250], sarebbe auspicabile pensare ad una riscrittura dell'articolo che precisi meglio i punti critici segnalati. A tal proposito si potrebbe chiarire in modo definitivo il concetto di illegalità, impropriamente utilizzato dal legislatore, in modo tale da sostituirlo col riferimento ai soli casi in cui il trattamento di dati personali realizzi una delle norme penali sostanziali che tutelano la riservatezza – artt. 615 *bis* ss c.p. – e dagli artt. 167 ss. del codice della *privacy*, con la relativa esclusione di altre illiceità derivanti dalla violazione di norme sostanziali non penalmente sanzionate, come gli illeciti civili, amministrativi, o i trattamenti definiti illeciti da norme del codice della *privacy* ma non richiamate dagli artt. 167 ss. del Testo unico, pertanto resterebbero "fuori dalla portata sanzionatoria dell'art. 240 comma 2 c.p.p. tutti quei documenti che […] non siano stati formati attraverso quel trattamento di dati personali che è definito illecito dagli artt. 167 ss. del codice della *privacy*. Così ad esempio i documenti contenenti informazioni che non siano dati personali (fotografia di un luogo che venga rubata) e i documenti contenenti dati personali trattati in violazione di norme del codice della *privacy* diverse da quelle espressamente richiamate dagli artt. 167 ss dello stesso Testo unico […] saranno utilizzabili nel processo penale"[251]. Peraltro l'idea di salvaguardare la *privacy*, attraverso il meccanismo della radicale eliminazione delle informazioni, e la realizzazione di un verbale sostitutivo delle informazioni personali distrutte, sembra – anche alla luce delle correzioni apportate al senso della norma da parte di una recente sentenza della Consulta – un procedimento quanto mai efficace, e pertanto una delle cose da salvare pensando ad un eventuale futura modifica della norma.

Il riferimento ai parametri generali stabiliti dal'art. 11 del Testo unico, condiziona inevitabilmente anche l'istituzione delle banche dati interne alle forze di polizia o all'autorità giudiziaria, nate per far fronte a particolari esigenze connesse alle attività investigative. Queste ultime devono essere strutturate in

[249] Vedi par. 2.2.
[250] Corte cost., 22 aprile 2009 n.173, cit., 15.
[251] CONTI, *Le intercettazioni illegali*, cit., 158.

modo tale da assicurare una tutela della *privacy* in linea con quanto previsto dal codice in materia di protezione dei dati personali.

A tal proposito la recente introduzione della banca dati del dna costituisce un modello d'azione condivisibile, dato che ha delineato i tratti della cornice normativa di tutela del dato biologico catalogato nel corso di un procedimento penale[252]. L'archivio dei profili del dna introdotto nel nostro paese, prevede un sistema di controlli articolato, volto a verificare la validità scientifica delle attività di raccolta e conservazione del materiale genetico utilizzato per l'indagine biologica con l'ausilio del dna *database*, in modo tale da ridurre al minimo eventuali errori nell'identificazione di un soggetto sospettato della commissione di un reato. Inoltre, individua in modo chiaro: lo scopo perseguito, le autorità preposte all'accertamento di eventuali lesioni del diritto alla *privacy*, i tempi per la concretizzazione del diritto all'oblio del profilo identificativo e del materiale biologico utilizzato per la tipizzazione[253].

La banca dati contiene un numero limitato di profili identificativi, poiché prevede la possibilità di inserire solo informazioni genetiche provenienti da alcuni soggetti privati della libertà personale – gravemente indiziati della commissione di un reato sottoposti a custodia cautelare in carcere, arrestati in flagranza o condannati per la commissione di reati determinati[254] –, o repertate nel corso del procedimento penale[255]. Peraltro tale selezione si differenzia notevolmente da quella utilizzata dal dna *database* a scopo identificativo, istituito, in campo di indagini criminali, nel Regno Unito. Invero lo strumento impiegato dalla polizia inglese, muove dal presupposto – diametralmente opposto a quello sul quale si fonda il *database* italiano – che la catalogazione massiccia di profili identificativi del dna, costituisca la base per poter assicurare maggior sicurezza ai cittadini[256]. A ben vedere, questo discorso portato agli estremi, ha una sua logica aritmetica, tutta legata ai numeri del raffronto; nel senso che un maggior quantità di individui schedati attraverso il profilo identificativo del dna produce un aumento, secondo

[252] Vedi cap. IV.
[253] FELICIONI, *L'acquisizione di materiale biologico a fini identificativi o di ricostruzione del fatto*, in *Prelievo del DNA e banca dati nazionale*, a cura di SCARCELLA, Padova, 2009, 191.
[254] Vedi cap. IV.
[255] FELICIONI, *L'acquisizione di materiale biologico a fini identificativi o di ricostruzione del fatto*, cit., 197.
[256] FANUELE, *Banche dati genetiche: modelli stranieri e peculiarità italiane*, in *Prelievo del DNA e banca dati nazionale*, cit., 303.

le leggi della statistica, della probabilità d'individuazione dei colpevoli della commissione di certi reati. [257]

3.2)(segue) Il tempo di conservazione del dato personale e il diritto all'oblio

Il diritto all'oblio dei dati personali – contenuto tra i principi elencati dall'art. 11 del Testo unico – costituisce una garanzia molto importante nella dinamica del rapporto esistente tra titolare dell'archivio elettronico e soggetto interessato dalla catalogazione, in quanto esclude qualsiasi possibilità di conservazione illimitata dei dati. Pertanto le informazioni personali dovranno essere cancellate dalla banca che le raccoglie, al venir meno delle ragioni che ne hanno giustificato la scelta, o nel caso in cui scada il termine stabilito per la durata del trattamento. In queste situazioni l'effetto prodotto – distruzione dell'informazione catalogata – potrebbe avere riflessi negativi sul processo penale; si pensi a tutti quei casi in cui i termini ordinari di conservazione di un

[257] Ad onor del vero, occorre sottolineare come in questi anni la cronache d'oltre manica sulla banca dati del dna abbiano riportato successi investigativi sulla repressione di alcune particolari tipologie di delitti, oltreché il racconto di numerosi riconoscimenti erronei; non ultimo il fallimento investigativo registrato in relazione ad un indagine genetica richiesta a *Scotland Yard* dalla nostra polizia scientifica nell'ambito di una collaborazione investigativa per la soluzione di un caso di omicidio. Il reparto del R.I.S. di Parma aveva trasmesso il profilo genetico repertato sulla luogo del delitto – nelle campagne della grossetano – presso le polizie europee che potevano disporre all'epoca di una banca dati del dna per il riconoscimento delle persone. Tale trasmissione seguì alla testimonianza di una delle vittime dell'aggressione che aveva percepito un accento straniero nel sentire la parlata dell'aggressore. Il soggetto sospettato di aver commesso il reato – un ragazzo inglese nativo di Liverpool – e stato prosciolto da ogni accusa, dopo essere stato indagato a causa della corrispondenza del proprio profilo del dna, contenuto nella banca dati inglese, con quello repertato sulla scena del crimine in Italia. In questo caso specifico l'evidenza scientifica si è dovuta arrendere di fronte all'altrettanto indubitabile risultato della prova d'alibi; invero dall'esame di ben venti testimoni a discarico, è emerso che nel giorno e all'ora del delitto il presunto colpevole beveva tranquillamente in un bar di Liverpool. Ciò che lascia perplessi in questa vicenda è la totale corrispondenza dei profili confrontati in un primo momento dalle forze di polizia; tanto che le cronache dei giorni successivi all'avvenuto confronto sul dna, registrano l'assoluta certezza della bontà dell'indagine genetica effettuata, e l'enorme soddisfazione per la positiva risoluzione del caso di omicidio. Vedi, BOLOGNI, *E' un inglese il killer della pineta, smascherato dalla banca dati del DNA*, in *La repubblica*, 15 febbraio 2003, 26; BOLOGNI, *Omicidio Vicentini, il secondo* test *del DNA scagiona il barista inglese*, in *La repubblica*, 10 marzo 2003, 2; GIUSI, *Dna, processo ai test, troppi errori non ci sono certezze. Londra riapre duecento indagini*, in *Corriere della sera*, 23 febbraio 2007, 29.

dato – calibrati in modo tale da far fronte alle esigenze relative al trattamento effettuato in specifici settori – producano l'eliminazione dell'informazione prima che questa possa essere utilizzata nel corso del procedimento. In particolare, alla cessazione del trattamento, si potrebbero verificare due situazioni differenti sulla sorte del dato; *id est*, l'eliminazione, o viceversa la conservazione nonostante la scadenza del temine massimo.

Nel primo caso il dato eliminato, anche qualora recasse delle informazioni importanti per la definizione della regiudicanda, sarebbe irrimediabilmente perduto. A ben vedere, l'unico modo per porre rimedio a questo avvenimento negativo, pare l'intervento del legislatore – seguendo l'esempio offerto dalla legge sull'acquisizione dei tabulati relativi alle comunicazioni telefoniche o telematiche –, che attraverso l'indicazione di termini speciali per la conservazione del dato, potrebbe garantire l'integrità dello stesso per un tempo congruo all'accertamento del fatto reato. Una simile soluzione rappresenterebbe pienamente il caleidoscopico mondo delle banche dati, per natura poco incline alla formulazione di regole di principio "valide per tutti". Invero il numero elevato di campi in cui vengono utilizzati e catalogate notizie personali, impone una ricerca delle soluzione di tipo "settoriale", che, nella fissazione di un tempo dedicato alla custodia dei dati archiviati, tenga conto, tanto delle necessità del procedimento penale, quanto della natura dell'informazione catalogata.

Una questione di particolare importanza che accomuna le informazioni personali provenienti da una banca dati comune o criminalistica, riguarda l'utilizzazione del dato mantenuto nel *database* oltre il termine stabilito dalla legge per i rispettivi trattamenti. Questa eventualità si realizza in tutti quei casi in cui il titolare dell'archivio di raccolta non distrugga il dato catalogato una volta che si esaurisca il termine stabilito per la conservazione. Come sottolineato nel paragrafo precedente, in tali casi il dato sarà utilizzabile, a meno che non ci sia una norma processuale che dica il contrario. Viceversa, qualora esista una legge che fissi una determinata scadenza per la conservazione dei dati – calibrata sui tempi del processo –, l'eventuale informazione ancora disponibile oltre il termine massimo indicato per il mantenimento, sarà da considerare come inutilizzabile.

Tale ricostruzione esegetica pare la soluzione migliore per interpretare l'indicazione relativa ai termini finali per la custodia delle informazioni genetiche,

contenuta nella legge n. 85 del 2009[258]. Invero la disposizione *de qua* sembra rappresentare il risultato di valutazioni fatte dal legislatore per far fronte ad esigenze proprie dell'indagine genetica; dal momento che, a tal fine individua, in quarant'anni il limite massimo di protezione per il profilo identificativo del dna e in vent'anni il tempo di conservazione del materiale genetico, utilizzato per le operazioni di tipizzazione del dato inserito nel *database*. Inoltre la legge prevede che allo scadere di tali periodi le informazioni contenute nella banca dati vengano cancellate, e la distruzione del materiale biologico conservato presso il laboratorio centrale del dna. Pertanto, i dati soggetti ad eliminazione, comunque mantenuti nella banca oltre il tempo limite stabilito *ex lege*, saranno inutilizzabili, per qualsiasi attività di identificazione genetica soggettiva, svolta dal pubblico ministero o dalla polizia giudiziaria. Ciò non significa, una rinuncia assoluta all'informazione, in quanto l'autorità giudiziaria potrebbe trarre dal dato inutilizzabile lo spunto per effettuare nuove indagini o, nel caso fosse possibile, operare una nuova acquisizione della stessa notizia. Considerazioni, queste ultime, che sembrano estendibili anche alle banche dati che conservano i dati esterni relativi alle comunicazioni telefoniche e telematiche[259].

[258] Vedi cap. IV.

[259] "I fornitori possono tenere i dati sul traffico telefonico soltanto per quarantotto mesi; viene allora spontaneo pensare che il giudice, investito d'una richiesta d'acquisizione, debba anche verificare che tale periodo non sia già decorso; anche se le norme non autorizzano tale deduzione. L'art. 132 commi2 e 5 lettera d , laddove stabilisce che la custodia non possa durare più di quarantotto mesi, si rivolge appunto ai fornitori, non al giudice. Pur con molte perplessità, la conclusione più plausibile è che un eventuale sforamento dei quarantotto mesi possa rilevare ad altri fini (ad esempio un'azione di responsabilità verso il fornitore del servizio) ma non impedisca al giudice di concedere l'autorizzazione e non intacchi la validità processuale delle prove raccolte". In questi termini, CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005,624.

CAPITOLO QUARTO

DALLA TRACCIA BIOLOGICA AL DNA *DATABASE*

1) *I modelli di banche dati del dna*

Le scoperte fatte in biologia molecolare negli ultimi venti anni hanno avuto un riflesso diretto anche sul processo penale. La possibilità di arrivare ad una identificazione indiscussa del colpevole attraverso l'utilizzo del dna – così come accaduto per le impronte digitali e per le indagini biometriche in passato – , ha suscitato da subito l'interesse degli investigatori. La prima polizia al mondo ad utilizzare la genetica come mezzo per il riconoscimento di soggetti colpevoli della commissione di reati fu nel 1986 *Scotland Yard* , che nella risoluzione del caso relativo all'individuazione dell'assassino di due ragazzine nelle *Midlands* inglesi sperimentò con successo le immense potenzialità di questo particolare e innovativo strumento scientifico nelle aule di tribunale[260].

[260] L'esperienza del Regno Unito in relazione alla regolamentazione di tutte le fasi caratteristiche dell'indagine genetica può essere considerata come antesignana rispetto all'evoluzione che altri stati – come l'Italia ad esempio – hanno avuto solo di recente. La distinzione tra atti invasivi e non, in base alla quale stabilire il limite rispetto ad un intervento coercitivo dell'autorità giudiziaria per l'apprensione del campione biologico, è stata affrontata dal legislatore inglese già nel 1984 con la pubblicazione del *Police and Criminal Evidence Act*. Tale provvedimento prevedeva il consenso dell'indiziato come elemento discriminante tra le due tipologie di atti investigativi; nel senso che tutta una serie di azioni particolarmente limitative della libertà individuale non potevano svolgersi senza il consenso necessario dell'individuo indagato c.d. *intimate sample*; viceversa alcune attività d'indagine meno invasive, c.d. *non intimate sample*, legittimavano la polizia giudiziaria ad iniziative di carattere coercitivo, ovvero senza il necessario *placet* del soggetto passivo. Peraltro occorre segnalare come nel corso degli anni si sia assistito alla pubblicazione di una serie di norme caratterizzate da un progressivo restringimento del riferimento agli atti non invasivi contenute nella primigenia regolamentazione del 1984, nel solco di un maggiore permissivismo dell'attività di prelievo del materiale biologico da parte della polizia giudiziaria. Sul punto FANUELE, *L'indagine genetica nell'esperienza italiana ed in quella inglese*, in *Riv. it. dir. proc. pen.*, 2006, 732; FELICIONI, *Accertamenti personali e coattivi nel processo penale: linee di riforma*, in *Dir. pen. proc.*, 2005, 621; SCAFFARDI, *Le banche dati genetiche personali per fini giudiziari e i diritti della persona*, in www.forumcostituzionale.it, 2008, 7.

Tuttavia il paradigma dell'indagine genetica forense, si deve alla fondamentale scoperta del genetista inglese Alec Jeffreys, che nel 1985 individuò per la prima volta la mappatura completa del genoma umano, dando inizio all'uso del *dna profiling* per l'identificazione personale[261] in ambito penale, "più precisamente, l'oggetto dell'analisi comparativa è il polimorfismo del dna, ossia la parte "intronica" di tale molecola[262]: attraverso il relativo *test* è possibile confrontare le caratteristiche del dna ricavate dalle tracce biologiche rilevate sul luogo del delitto con quelle dell'indagato e, quindi, ricostruire la dinamica dell'evento"[263]. Nel corso degli anni si è amplificato il ruolo della biologia nell'esercizio dell'indagine identificativa, soprattutto con l'utilizzo della banca dati del dna[264], dato che grazie a tale strumento aumentano le possibilità di confronto e, di riflesso, la probabilità d'individuare il soggetto colpevole della commissione di un reato

I dati statistici rivelano come, nei paesi in cui le operazioni di raffronto dei profili genetici acquisiti nel corso delle indagini vengono effettuate con l'ausilio di banche dati elettroniche, si sia assistito ad un progressivo miglioramento dell'attività di *intelligence*. In particolare le notizie riportate da un recente studio[265] sul dna *database* inglese relativo all'utilizzo di quest'ultimo nell' individuazione di soggetti autori di reati, denota in modo chiaro le potenzialità dell'indagine genetica realizzata con l'ausilio di siffatti strumenti di investigazione, con percentuali altissime di soluzione dei casi rispetto al grado di utilizzazione[266]. Sulla scorta di queste valutazioni, negli ultimi quindici anni, molti paesi europei hanno introdotto nei loro ordinamenti una legislazione

[261] JEFFREYS – WILSON – THEIN, *Individual- Specific "Fingerprints" of Human DNA*, in *Nature*, 1985, 76.
[262] Vedi cap. I, par. 3.
[263] FANUELE, *L'indagine genetica nell'esperienza italiana ed in quella inglese*, cit., 733.
[264] MIRAGLIA, *La ricerca della verità per condannare ed assolvere: il test del DNA e l'esperienza statunitense*, in *Dir.pen.proc*., 2003, 1555.
[265] *Expansion program 2000 – 2005, Reporting Achievement*, in *UK Home Office*
[266] Tuttavia occorre sottolineare come, la maggior parte di delitti risolti grazie allo strumento della banca dati del dna rientra nei c.d. *volume crime* o crimini di non particolare gravità, come furto o rapina, rispetto a delitti molto più gravi come per esempio omicidio. In relazione a questo dato statistico e in prospettiva *de iure condendo* – in vista del futuro potenziamento nel nostro paese di tale strumento investigativo – occorrerebbe operare una scelta – considerati i costi di gestione necessari per l'implementazione del *database* – di politica criminale, rivolta più alle reali possibilità dimostrate in questi anni dalla banca dati di profili genetici, che alla eventuale soluzione – statisticamente molto più rara – di delitti gravi ma potenzialmente meno adatti all'identificazione biologica come forma di indagine.

speciale sulla banca dati del dna. L'organizzazione di tali *databases* ricalca in linea di massima il modello importato dal *codis* nordamericano – il *software* utilizzato dalla polizia federale statunitense – sia per quanto riguarda la forma della catalogazione, che per l'individuazione dei dati genetici oggetto dell'archiviazione. Tuttavia, pare interessante notare come cambi da paese a paese lo specifico approccio sostanziale adottato da ogni stato nella regolamentazione delle banche dati[267]. A tal fine, fatti i doverosi distinguo legati alla diversità dei sistemi giuridici, all'organizzazione del processo penale e delle forze di polizia giudiziaria, è possibile operare un parallelo – tra alcune delle banche dati implementate nei maggiori stati dell'Europa occidentale – articolato su tre "macro livelli": oggetto della catalogazione, conservazione del materiale biologico utilizzato per determinare la tipizzazione del profilo genetico, tempo di conservazione di tale dato.

Per quanto riguarda il primo punto, la conservazione dei profili identificativi di soggetti che hanno subito una sentenza di condanna irrevocabile costituisce un dato costante e generalizzato in tutti i paesi europei in cui è stato introdotto un *database* centralizzato per l' archiviazione del dna. A tal proposito si può osservare come la catalogazione del profilo genetico del condannato abbia quasi una valenza paradigmatica, in quanto concretizza di fatto gli obiettivi di prevenzione generale e speciale, caratteristici della custodia di profili biologici identificativi all' interno di banche dati del dna. Invero, l'obiettivo principale di questa forma di controllo, è quello di agevolare – come più volte rimarcato – l'opera degli inquirenti nelle indagini penali per reati ad alto tasso di recidiva attraverso l'attività di confronto *ex post* operata sui profili genetici identificativi conservati. Al riguardo merita sottolineare come l'unico motivo di differenza tra i vari paesi in cui è stata implementata una banca dati, consista nella selezione delle fattispecie, accertate in via definitiva da una sentenza di condanna, dalle quali far dipendere la catalogazione.

Molto più complessa risulta la situazione del soggetto sottoposto ad indagini penali. Invero, le soluzioni impiegate per risolvere la questione connessa ad una eventuale conservazione del profilo genetico in una fase precedente alla conclusione del processo, appaiono alquanto eterogenee. Non in tutti i paesi,

[267] MENDELLA, *Banca dati del DNA: l'arma anticrimine. Nel resto d'Europa funziona così*, in *Dir. giust.*, 2005, n.25, 21.

infatti, è stato utilizzato lo stesso criterio per stabilire quali siano i soggetti passivi della registrazione del dna nel *database* nazionale.

Prendendo come esempio portante della nostra trattazione l'esperienza del Regno Unito – che per certi versi rappresenta la realtà dove la banca dati del dna ha avuto un maggiore utilizzo[268] – possiamo osservare, come la tipologia di catalogazione ivi utilizzata prescinda da qualsiasi considerazione sulla tipologia o sul grado di accertamento del fatto reato, in quanto il dna del sospettato può essere repertato dalla polizia giudiziaria in modo coercitivo in conseguenza di un semplice arresto – non è infatti necessaria nessuna pronuncia giurisdizionale ancorché revocabile, che accerti una effettiva colpevolezza del soggetto – , come dire che il solo sospetto d'aver commesso un reato ricompreso nella tipologia dei c.d. *recordable offences*,[269] legittima l'inserimento nella banca dati del dna dell'indagato. Invero, la registrazione del dato genetico avviene in un'unica banca dati nazionale, NDNAD, che riceve – insieme ai profili di imputati condannati con sentenza passata in giudicato – quelli di soggetti gravati da indizi di colpevolezza o semplicemente sospettati della commissione di un reato, quelli relativi al materiale repertato sulla scena del crimine, c.d. *open records* – nel quale si ricomprende il dna proveniente dalla vittima del reato e quello lasciato da soggetti ignoti sul luogo del delitto –, e di soggetti che contribuiscono volontariamente il proprio profilo genetico[270].

Ognuno di questi insiemi di dati costituisce di fatto l'oggetto dell' indagine induttiva che dovrebbe portare all'identificazione del colpevole di un reato, attraverso il confronto e la ricerca della corrispondenza con gli eventuali elementi a disposizione degli inquirenti.

---

[268] Il database inglese contiene secondo dati ufficiali circa tre milioni e quattrocentomila profili identificativi tipizzati e catalogati. *Parliamentary Office of Science and Technology, Report 2006,* n. 258, 2006, 1.

[269] Letteralmente "*recordable offence*" significa "reato registrabile", di fatto rappresenta una effetto sanzionatorio accessorio, di carattere special preventivo, che in Inghilterra accomuna pressoché tutti gli illeciti penali. Una fattispecie si può definire come registrabile quando – dopo l'inizio di un indagine a carico la formulazione di una imputazione (*charge*) – è possibile prelevare un campione di materiale biologico dal quale tipizzare il profilo identificativo da inserire nella banca dati del dna.

[270] Qualsiasi cittadino inglese può spontaneamente donare il proprio profilo genetico identificativo da inserire nella banca dati del dna, ciò avviene grazie ad un consenso rilasciato per iscritto all'autorità procedente dal donatore. FANUELE, *Un archivio centrale per I profili del DNA nella prospettiva di un diritto comune europeo,* in *Dir. pen. proc*., 2007, 386.

Alcuni autori hanno rimarcato come simili catalogazioni di massa realizzino delle vere e proprie forme di controllo sociale, una sorta di "biosorveglianza"[271]. Tale definizione esplica in modo chiaro la *ratio* di *database* genetici così invasivi, che si traduce nell'idea che una più agevole individuazione dei colpevoli dei reati passi attraverso la mera schedatura genetica di quanti più cittadini sia possibile effettuare. Peraltro occorre sottolineare come il dna *database* inglese è il più grande esistente in Europa, con più di tre milioni di profili registrati. Questo profluvio di informazioni è dovuto al sistema di prelievo e catalogazione adottato, improntato verso una logica di conservazione – la cancellazione dei dati avviene dopo cento anni dall'inserimento – degli elementi genetici raccolti. L'eccesso di questa filosofia del controllo, è rappresentato in modo chiaro da una recente proposta avanzata dal dipartimento delle scienze forensi di *Scotland Yard*, in base alla quale si chiede l'inserimento nella banca dati nazionale inglese del dna di profili genetici di scolari con età inferiore a dieci anni che nel corso del normale svolgimento dell'attività didattica hanno dato adito a comportamenti antisociali a rischio di commissione di reati[272].

La vastità di dati a disposizione degli investigatori d'oltremanica sembra in realtà trascendere l'effettiva esigenza connessa alla raccolta e successiva catalogazione dei profili del dna nel corso delle indagini: l'accumulazione di dati nel *database* appare infatti decisamente sproporzionato rispetto alle reali necessità legate alle attività di identificazione genetica[273]. Non va dimenticato inoltre che questa mole di dati necessita di un adeguato limite alla illegittima intrusione o utilizzazione degli stessi, ed il modello inglese negli anni ha dato invero, una cattiva prova di resistenza relativa allo specifico settore della gestione dei dati[274].

---

[271] WILLIAMS – JOHNSON, *Forensic DNA Databasing: a European Perspective, interim report*, Durham, 2005, 11.

[272] CARBONI, *Scotland yard vuole il DNA dei bambini, l'idea di schedare il patrimonio genetico dei piccoli con comportamenti "sospetti"*, in *Corriere della sera*, 17 marzo 2008, 35.

[273] La banca dati del Regno Unito è attualmente la più grande al mondo; secondo i dati forniti dal *parliamentary office of science and tecnology*, a dicembre 2005, il numero totale di campioni di DNA inseriti nel NDNAD era di circa 3.450.000. Nello specifico, pare interessante rilevare come 139.463 campioni identificativi appartengano a individui mai accusati di alcun crimine e 685.748 a ragazzi di età compresa tra i 10 e i 17 anni; *Parliamentary Office of Science and Technology, the National DNA Database*, cit. .

[274] WILLIAMS – JOHNSON, *Genetic Policing the Use of DNA in Criminal Investigations*, London, 2008, 46; vedi inoltre i *report* pubblicati sul sito *www.innocentproject.org/press*

Esistono altresì anche tipi di banche dati meno intrusivi rispetto al prototipo "universale inglese"[275] . In particolare la dottrina ha circoscritto i modelli alternativi a quello anglosassone in due filoni: le banche dati di tipo emergenziale – ne costituisce un esempio quella francese – e quelle intermedie quali, secondo un'usuale definizione, l'archivio genetico tedesco [276].

I *database* del primo tipo non prevedono "inserimenti automatici" – nel corso delle indagini – del profilo genetico del soggetto gravato dal mero sospetto di aver commesso un reato[277]. La catalogazione del dato ha luogo solo nel caso in cui un soggetto venga indagato per gravi reati o qualora – in fase antecedenti alla conclusione del processo – sussistano a suo carico gravi indizi di colpevolezza. In tali situazioni la conservazione del dato genetico nella banca dati nazionale del dna è condizionato dalla presenza di un elemento di prova qualificato, dal quale si possa desumere in modo indiscutibile la responsabilità del soggetto sottoposto alle indagini, nella commissione di una serie di reati precisi individuati *ex lege*. In altre parole la catalogazione del profilo biologico, consegue solo ed esclusivamente al riscontro di una evidenza oggettiva grave, nel caso in cui le indagini riguardino una serie ristretta di fattispecie indicate preventivamente dal legislatore[278].

Altri stati hanno adottato una soluzione mediana rispetto a quelle testé indicate. A tal proposito il limite alla catalogazione del profilo genetico nel *database* nazionale nel corso delle indagini è rappresentato da una valutazione prognostica operata dall' organo giudicante, sulla pericolosità sociale del soggetto sottoposto alle indagini, intesa come il rischio che quest' ultimo possa commettere nuovi reati[279]. Ciò avviene per esempio in Germania[280], laddove il fattore discriminante rispetto ad una eventuale conservazione del dna dell'indagato è

---

[275] STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Padova, 2008, 171.

[276] PICOTTI, *Trattamento dei dati genetici, violazioni della* privacy *e tutela dei diritti fondamentali,* in *Dir. dell' inf. e dell' inform*., 2003, 722.

[277] FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Milano, 2007, 193.

[278] In Francia l'inserimento nella banca dati avviene su richiesta della polizia o direttamente *ex officio* da parte dell'autorità giudiziaria solo per la commissione di gravi reati quali: omicidio volontario di un minore con violenza sessuale, tortura, violenza sessuale, corruzione di minorenni, molestie sessuali senza violenza,

[279] STEFANINI, *Dati genetici e diritti fondamentali,* cit. , 178.

[280] ORLANDI – PAPPALARDO, *L'indagine genetica nel processo penale germanico: osservazioni su una recente riforma*, in *Dir. pen. proc.*, 1999, 762.

rappresentata dall' apprezzamento operato dall'organo giudicante, al di là quindi di qualsiasi valutazione *ex ante* realizzata per legge attraverso la selezione di situazioni oggettive qualificate dalle quali far discendere un obbligo diretto alla introduzione del profilo genetico nel *database* nazionale del dna.

Nelle banche dati di tipo emergenziale e in quelle intermedie il profilo biologico dell'indiziato o del sospettato della commissione di determinati reati, viene mantenuto fintanto che su quest'ultimo gravano degli indizi di colpevolezza[281] ed eliminato non appena questi vengano meno, concretizzando di fatto il c.d. diritto all'oblio in campo genetico[282] .

Risulta inoltre piuttosto omogenea tra gli stati dell'Unione europea che afferiscono ai modelli di *database* differenti da quello inglese, l'indicazione dei reati per i quali è consentito procedere all'inserimento nella banca dati del dna del profilo genetico dell'indiziato, del sospettato, o del condannato[283]. La selezione dei crimini segue criteri di carattere sostanziale attraverso l'indicazione specifica delle tipologie di reato – in genere tutti i reati per i quali è considerato un alto livello di recidiva –, e parametri prettamente formali legati ai limiti edittali di pena. Peraltro è necessario ricordare come il profilo genetico rinvenuto sulla scena del crimine e appartenente a soggetti ignoti, ipoteticamente collegabili alla commissione del reato, è inserito in una specifica sezione della banca dati del dna e utilizzabile quindi per ricerche e confronti incrociati con i dati di imputati condannati o – a seconda della nazione – sospettati per altri reati, ovvero con elementi rinvenuti su altre scene del crimine e appartenenti a soggetti sconosciuti. Tale attività ha una *ratio* esplorativa, e costituisce la base sulla quale si fonda l'azione di *intelligence* dell'investigatore chiamato alla soluzione del caso di cui si conoscono solo le "notizie biologiche" rinvenute sul luogo delitto che è poi la ragione principale per cui consulta la banca dati del dna nazionale o chiede la collaborazione di quelle di altri stati.

---

[281] La cancellazione del profilo identificativo dal *database* del dna costituisce una prassi comune a tutti i paesi in cui è stata introdotta la banca dati genetica, con l'unica eccezione dell'Inghilterra dove non esiste un tale diritto. Pertanto, il profilo genetico del sospettato viene conservato nella banca dati nazionale, indipendentemente da eventuali pronunce di proscioglimento e successive all'inserimento.

[282] Il diritto alla cancellazione del dato genetico nei casi in cui non sia più necessario per le finalità per i quali è stato legalmente raccolto, costituisce un principio ormai affermato a livello europeo, ed è stato recentemente ribadito dall' art. 4 della Decisione Quadro del Consiglio 2008/977/GAI., in *G.U.U.E.*, 19 dicembre 2008, L 350/60.

[283] D'ANTONIO, *I dati genetici,* in CARDARELLI– SICA – ZENO-ZENCOVICH, *Il codice dei dati personali*, cit., 382; PICOTTI, *Trattamento dei dati genetici,* cit., 715.

Ulteriore aspetto critico è rappresentato dalla potenziale conservazione del materiale biologico utilizzato per individuare il profilo genetico da catalogare nella banca dati. Invero mentre il dato da archiviare si riduce ad una sequenza alfanumerica che dice ben poco su informazioni fenotipiche riconducibili al soggetto, il materiale biologico contiene informazioni utili per ricostruire l'intera catena polinucleotidica del dna individuale. A tal proposito alcuni stati non ne consentono la conservazione, prevedendo una distruzione nel momento successivo alla determinazione del profilo genetico, mentre altri ne autorizzano la custodia in luoghi differenti rispetto alla sede della banca dati dei profili – solitamente presso il laboratorio che ha condotto le operazione di estrazione del dato genetico da inserire in banca dati – , per periodi inferiori rispetto a quelli di detenzione di questi ultimi[284].

In ultima analisi, occorre sottolineare come i tempi di conservazione, dei profili identificativi tipizzati dal materiale biologico, si distinguano a seconda del modello di banca dati utilizzato dallo stato di riferimento. In linea di massima si può affermare che – escluso il Regno Unito dove, come ricordato in precedenza, il dato viene mantenuto per un tempo indefinito – , nei paesi che impiegano banche dati di tipo emergenziale, la custodia delle informazioni viene calibrata sui termini di prescrizione del reato o dell'esecuzione della pena; mentre in quelli che utilizzano modelli intermedi i tempi di conservazione risultano ampliati rispetto ai primi ma entro limiti temporali non eccessivamente dilatati come quelli della raccolta universale inglese[285] . Inoltre, il dato genetico catalogato nel corso delle indagini, deve essere eliminato dalla banca dati, nel momento in cui l'indagine si conclude in modo positivo per l'indagato, *id est* attraverso la pronuncia di un proscioglimento[286].

[284]MENDELLA, *Banca dati del DNA: l'arma anticrimine*, cit.,11; FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, cit., 195.

[285] FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico,* cit., 192.

[286] La Corte Europea dei diritti dell'uomo, nella sentenza S. and Marper v Regno Unito, ha sancito il diritto del soggetto indagato, nei confronti del quale intervenga un provvedimento di proscioglimento, alla cancellazione del dato genetico precedentemente catalogato nella banca dati del dna. Corte Eur. , S. and Marper v Regno Unito, 4 dicembre 2008, in *www.ehcr.coe.int – hudoc database -* .

2) ***Il* "co.d.i.s" *nordamericano***

L'archetipo della catalogazione elettronica in campo genetico è costituito dal modello di archiviazione utilizzato negli U.S.A. . Si può asserire come l'idea stessa d'identificazione genetica forense nasca sulla scorta di quanto teorizzato dai biologi americani all'atto della creazione della prima banca dati del dna. Invero, l'affermare che l'individuazione di tredici zone del genoma umano altamente polimorfiche, dislocate su diverse zone della catena polinucleotidica e caratterizzate dal fatto di essere non codificanti e sequenze di nucleotidi ripetute in tandem – STR[287] –, potesse portare all'identificazione di un soggetto con assoluta certezza, ha schiuso le porte ad un nuovo tipo d'indagine. Non pare dunque esagerato , parlare di questo sistema come di una invenzione rivoluzionaria che ha di fatto modificato l'atteggiamento e l'approccio degli investigatori del ventesimo secolo.

Il sistema di identificazione adottato dal *codis* rappresenta a tutt'oggi un modello di organizzazione, trattamento e consultazione dei dati *id est* un punto di riferimento importante per la creazione delle banche dati del dna a livello mondiale[288]. Il *codis* fu istituito in via sperimentale nel 1990 e usato inizialmente solo da quattordici stati e da laboratori locali; successivamente, nel 1994, il *Dna Identification Act* autorizzò formalmente l' FBI a creare un sistema nazionale di *Databanking* del dna che divenne definitivamente operativo nel 1998[289].

---

[287] Vedi, cap. I, par. 3.

[288] Il gruppo ENFSI (*European Network of Forensic Science Institute*), che raccoglie principalmente i laboratori europei delle forze dell'ordine, raccomanda l'uso di almeno sette sezioni del DNA umano quale parametro minimo da utilizzare per validare l'identificazione genetica soggettiva. Allo stesso modo anche il protocollo consigliato dall'INTERPOL – *Issol (Interpol standard set of loci)* a tutti i laboratori forensi suggerisce l'impiego di un modello identificativo simile a quello stabilito dall' ENFSI. Il sistema di identificazione usato dall' FBI americana, il CODIS, è costituito da un numero di marcatori considerevolmente superiore, poiché comprende tredici marcatori STR ovvero i sette previsti dall' ENFSI più altri sei. Ciò allo scopo di garantire l'acquisizione di profili individuali che risultino praticamente unici nelle popolazioni di riferimento. Recentemente, dopo un meeting tenutosi il 4 – 5 aprile del 2005 a Glasgow, è stata stabilita da parte dell' ENFSI l'introduzione di tre ulteriori marcatori STR, in modo tale che verrà aumentato il numero dei *loci* utilizzati in precedenza dallo standard delle indagini identificative genetiche in ambito europeo, portandolo da sette a dieci, nel solco di quanto già accade in America. In argomento cfr. RICCI – PREVIDERÈ – FATTORINI - CORRADI, *La prova del DNA per la ricerca della verità,* cit., 410.

[289] FANUELE, *Dati genetici e procedimento penale*, cit., 217.

Il *database* genetico contiene solo porzioni del genoma umano non codificante ed è costituito da due indici o sezioni contenenti i profili genetici di soggetti condannati per crimini particolarmente gravi quali violenza sessuale o omicidio – *convicted index* [290]– e quelli rinvenuti sulla scena del crimine e appartenenti a individui sconosciuti o alla vittima *offender index* [291] .

Oltre a questi indici classici, che hanno accompagnato il modello primigenio del *codis,* nel corso del tempo sono state introdotte altre raccolte di dati genetici attinenti in particolare, ai profili soggettivi dei parenti di individui scomparsi. Tali informazioni sono utili in tutte quelle indagini che riguardano il riconoscimento di resti umani ritrovati, dei quali non si conosce l'identità. Infatti l'indagine biologica relativa alla ricerca del rapporto di prossimità genetica tra dna dei resti individuati e quello dei potenziali parenti può concretamente consentire l'identificazione positiva del soggetto.

Il *codis* è un *database* strutturato in modo gerarchico, nel senso che il suo contenuto rappresenta il frutto della raccolta di dati confluenti da archivi di carattere statale e locale. Al vertice della piramide così organizzata sta la raccolta denominata NDIS (*National dna index system*) che ricomprende tutte le informazione raccolte dalle banche dati che rappresentano la dimensione statale dell'archivio nazionale del dna le SDIS (*State dna index system*), queste ultime infine contengono i profili genetici prodotti dai laboratori autorizzati all'interno di ogni singolo stato LDIS (*local dna index system*)[292] . Siffatto sistema consente lo scambio e la comparazione di profili genetici, ai vari livelli, allo scopo di poter correlare eventi delittuosi avvenuti in luoghi e tempi differenti. Inoltre tale suddivisione è funzionale rispetto al grado di utilizzo dei repertori contenuti negli archivi genetici da parte delle forze di polizia. Nella fattispecie solo gli organi di

[290] Negli Stati Uniti d'America la selezione delle fattispecie che legittimano la polizia statale ad operare i prelievi di materiale biologico dal quale tipizzare il profilo identificativo di un soggetto, da inserire nel database, cambia da stato a stato; come dire che, non c'è omogeneità tra i reati indicati come presupposto oggettivo all'inserimento nell'archivio genetico di ogni singolo stato (SDIS) e di riflesso in quello governativo generale (NDIS): "dal 1999 cinquanta stati possiedono una banca dati del dna dove vengono conservati i campioni acquisiti da persone condannate per un reato di natura sessuale. Ventisette di tali archivi contengono i profili di criminali violenti; quattordici quelli di colpevoli per furto. Solo sei *databases* conservano i profili degli autori di un qualsiasi illecito penale". FANUELE, *Dati genetici e procedimento penale*, cit., 219.

[291]RICCI – PREVIDERÈ – FATTORINI - CORRADI, *La prova del DNA per la ricerca della verità*, cit., 409.

[292]MIRAGLIA, *La ricerca della verità per condannare ed assolvere*, cit. , 1557.

polizia federale avranno accesso e potranno consultare l'intero indice genetico interstatale, mentre alle polizie locali tale accesso rimane precluso[293].

Il *software* è in grado di contestualizzare il riscontro richiesto dall'operatore, elaborando i dati in relazione a determinati parametri oggettivi, che possono condurre prima possibile all'eventuale risultato positivo c.d. *match.* Nello specifico è possibile effettuare ricerche sulla base delle caratteristiche del reato commesso e di conseguenza confrontare il profilo rinvenuto sul luogo del crimine con dati appartenenti a soggetti condannati per un reato determinato affine a quello per il quale si svolgono le indagini, oppure confrontare il dna del sospettato con quello rinvenuto su altre scene del crimine riconducibili a quelle oggetto dell'indagine *a quo,* in modo da verificare l'eventuale coinvolgimento dell'indagato in quest'ultime. Peraltro a questo proposito va indicato come la scelta dei reati oggetto della condanna da inserire nella raccolta dei profili genetici, viene stabilita autonomamente da ogni singolo stato.

Come visto in precedenza, l'utilizzo della banca dati accompagna l'attività d'identificazione genetica e si può considerare a tutti gli effetti come un elemento importante per una migliore riuscita di questa. Invero, appare indubitabile come una comparazione di profili fatta su un numero limitato di campioni abbia una possibilità di successo nettamente inferiore rispetto alla stessa operazione posta in essere su un quantitativo di dati superiore. Questo perché – fermo restando che l'inserimento nella banca dati del dna del profilo genetico di un soggetto non da alcuna certezza sull'eventuale individuazione futura del colpevole di un reato – la probabilità di riscontrare una coincidenza all'esito del confronto, è direttamente proporzionale al numero di tentativi che si possono fare con la ricerca. Tale considerazione ha un valore assoluto in teoria, ma ad avviso di chi scrive perde di significato non appena si operano una serie di valutazioni oggettive sulla reale potenzialità della banca dati come strumento d'indagine. In particolare l'inserimento massiccio di dati schiude le porte ad ulteriori problemi di ordine organizzativo, come la conservazione e la tutela del dato genetico. Infatti, l'applicazione pratica della legge dei grandi numeri in campo di catalogazione genetica, laddove è stata usata in modo scientifico, ha prodotto dei grossissimi *deficit* sul fronte delle tutele individuali.

[293] Per una definizione più specifica del ruolo e delle competenze delle forze di polizia americane in materia si veda il sito *www.fbi.gov/hq/lab./codis.*

In quest'ottica, anche il sistema americano non ha dato prova di assoluta inviolabilità; infatti la mole di notizie archiviate – considerato che si parla di un sistema che raccoglie tutti i dati catalogati negli Stati Uniti d'America e soggetta ad un progressivo aumento nel tempo – si è rivelata difficilmente gestibile[294], talché negli anni si sono verificati diversi casi di dispersione di dati e confusione di questi.

Al di là di tali eventi, tragicamente normali quando si parla di archivi di questa portata, il giudizio sul modello investigativo *tout court* non può che essere positivo. Il riferimento alla tutela della *privacy* ad ogni modo, non va trascurato e posto in secondo piano come pegno da scontare in nome della sicurezza dei cittadini. In quest'ottica l'indagine genetica necessita di regole precise e di ferree forme di controllo, per consentire un uso di quest'ottimo mezzo scientifico in ossequio alle norme primarie rivolte alla tutela della personalità individuale.

3) *L' indagine genetica in Italia*

L'importanza del riconoscimento della colpevolezza dell'imputato al di là di ogni ragionevole dubbio ha spinto l'interesse della dottrina nel corso degli anni verso tutte quelle "nuove evidenze" che hanno alla base un grado di persuasività tale da rappresentare in modo compiuto la concretizzazione empirica del contenuto dell'art. 533 c.p.p.[295].

In tal senso negli ultimi vent'anni, – a far data cioè dalla storica scoperta del biologo Alec Jeffreys [296] –, l'attenzione degli studiosi del settore si è concentrata sulle potenzialità identificative della genetica nel corso del processo penale. Invero, l'illusione per cui, grazie all'avvento della prova scientifica del dna, la rappresentazione del *thema probandum* dovesse raggiungere livelli di altissima definizione – in modo da far diventare l'istruzione dibattimentale un momento deputato alla ratifica di un risultato indiscutibile generato

[294] RICCI – PREVIDERÈ – FATTORINI - CORRADI, *La prova del DNA per la ricerca della verità,* cit. , 437.
[295] BRUSCO, *Il vizio di motivazione nella valutazione della prova scientifica,* in *Dir. pen. proc.*, 2004, 1414.
[296] Vedi par. 1.

dall'acquisizione di tale mezzo probatorio – ha convinto non pochi commentatori e operatori del processo penale[297]. Fin dagli esordi l'attenzione della dottrina si è concentrata su alcune specifiche questioni legate al rapporto esistente tra la prova scientifica – nell'ambito del quale rientra a tutti gli effetti anche l'analisi del profilo genetico del dna – e le varie fasi dinamiche del procedimento probatorio[298].

Per quanto riguarda il momento iniziale di quest'ultimo – ricerca della prova – ha suscitato particolare interesse, sia l'analisi delle varie operazioni tecniche essenziali per poter disporre degli elementi necessari nello svolgimento delle indagini, che delle questioni giuridiche connesse all'impiego degli strumenti scientifici impiegati. In linea con tali considerazioni anche il dibattito in materia d'investigazione genetica, concerne temi di ordine pratico e di carattere giuridico, legati alla banca dati del dna[299].

L'analisi del dna è un'attività complessa caratterizzata da più operazioni pratiche coordinate tra loro: prelievo del materiale biologico sul luogo del delitto, tipizzazione del profilo del dna, confronto con i dati già in possesso dell'autorità giudiziaria. A ben vedere, il *database* rappresenta uno strumento nelle mani dell'investigatore, inserito nel contesto delle azioni di *intelligence* a carattere scientifico con finalità identificativa, che ha come funzione principale quella di aiutare l'individuazione del colpevole di un determinato reato attraverso l'attività di confronto dei profili identificativi. A tal fine i dati del soggetto sospettato della commissione di un determinato reato oppure rinvenuti sulla scena del crimine, vengono comparati con quelli contenuti all'interno della banca dati del dna.

Pare interessante notare come negli stati dove il raffronto effettuato con l'ausilio della catalogazione genetica costituisce una procedura di *routine* nelle indagini svolte su tracce biologiche repertate sul luogo del delitto o su soggetti sospettati, il livello di attenzione degli studiosi si sia spostato verso gli aspetti

---

[297] CESARI, *Prova del DNA e contraddittorio mancato,* in *Cass. pen.*, 2002, 534; PULEIO, *Quando la scienza è alleata del giudice. I nuovi saperi e la ricerca della verità: l'esigenza di attendibilità nell'uso delle conoscenze tecniche*, in *Dir. e giust.*, 2006, n.13, 68; SCALVI, *DNA- Test come "scientific evidence": poteri del giudice e validità della prova. Rilievi comparatistici*, in *Riv. It. med. leg*., 1997, 641.

[298] DOMINIONI, *La prova penale scientifica.*, cit. ,146.

[299] PULEIO, *Banca dati DNA: basta con i rinvii sui prelievi servono più garanzie. L'archivio dei profili genetici è vitale per la lotta al terrorismo,* in *Dir. e giust.*, 2005, n.10, 125.

legati all'utilizzo dell'archivio elettronico[300]. Queste osservazioni, potrebbero essere utili nell'ottica di eventuali correttivi da apportare al neonato progetto della banca dati del dna italiana, in quanto studiano una situazione che nel nostro paese potrebbe verificarsi in modo del tutto similare allorquando si avrà un uso su larga scala del *database*[301].

Inoltre, non va dimenticata la critica mossa, in modo assolutamente condivisibile, dalla dottrina d'oltremanica[302] all'approccio complessivo tenuto dagli investigatori di *common law* in relazione all' indagine genetica con l'ausilio della banca dati. In Inghilterra e negli Stati Uniti l'implementazione dell'archivio elettronico del dna, col contestuale impiego massiccio di tecniche investigative legate all'analisi biologica, ha portato con se una eccessiva "scientifizzazione" dell'intera attività d'indagine giudiziaria posta in essere dagli inquirenti[303].

Invero, il costante miglioramento della ricerca in campo genetico forense ha condotto gli investigatori ad affidarsi maggiormente all'utilizzo della prova del dna a discapito delle fonti classiche considerate più facilmente contestabili di fronte a giudici e giurie popolari. In tal senso, la prova scientifica è diventato il

---

[300] ASHWORTH, *The Criminal Process. An Evaluative Study*, Oxford, 1998, 264;GARLAND, *The Culture of Control: Crime and Social Order in Contemporary Society*, Oxford, 2001, 123.

[301] A tal proposito è necessario richiamare l'attenzione su tre aspetti particolari già anticipati, sotto profili differenti, nei paragrafi precedenti. In primo luogo pare smentita dai fatti la logica per cui un *database* svolge in modo più proficuo le proprie funzioni di carattere special preventivo solo se racchiude in sé un numero elevato di profili genetici identificativi. L'esperienza pratica rilevata in altre realtà, suggerisce semmai una riduzione dei dati da inserire nella banca, a vantaggio di una selezione accurata dei casi in cui prelevare il campione biologico per la tipizzazione del profilo identificativo. Sicché, il *database* dovrebbe contenere solo le informazioni genetiche relative a quei reati che, in virtù di studi statistici, denotano nel tempo un alto grado di recidiva e nei confronti dei quali può essere utile una investigazione fondata esclusivamente su dati preesistenti alla commissione del reato, tipica dell'indagine condotta attraverso la banca dati. Sempre in quest'ottica, va segnalato come un archivio elettronico con numerosi dati risulta difficile da gestire soprattutto con riferimento alla *privacy*. In terzo luogo – anche a seguito di una recente pronuncia correttiva della banca dati nazionale del dna inglese da parte della Corte europea dei diritti dell'uomo (Corte Eur. , S. and Marper v Regno Unito, cit.) – pare assodato come non ci sia spazio alcuno per la conservazione dei profili genetici di soggetti sospettati della commissione di un reato per i quali sia intervenuta una sentenza o un provvedimento giudiziale non definitivo che riconosce l'estraneità al fatto dell'indagato, eventualità peraltro che pare contraria anche al principio generale che riconosce la non colpevolezza dell'imputato fino all'intervento di una sentenza irrevocabile di condanna.

[302] WILLIAM - JOHNSON, *Genetic Policing the Use of DNA in Criminal Investigations*, cit., 10.

[303] WILLIAM - JOHNSON, *Genetic Policing the Use of DNA in Criminal Investigations*, cit., 12.

mezzo principale utilizzato per esplicitare l'intero risultato investigativo: una sorta di fondamento matematico che conferisce un'aurea di certezza e incontestabilità alle conoscenze ottenute e alle decisioni prese[304].

Nella breve storia relativa all'utilizzo della prova genetica nel nostro paese, la percezione d'infallibilità che ha circondato la verifica del dna fin dai suoi esordi nelle aule giudiziarie, è stata ridimensionata nel corso degli anni a causa della fragilità manifestata.

Osservando le peculiarità delle attività di investigazione genetica, si può notare come, fin dal principio l'analisi del materiale biologico – che può essere prelevato sia da un soggetto sospettato sia sulla scena del crimine – necessiti dell'intervento di personale specializzato, capace cioè di non deprimere le potenzialità identificative del campione da analizzare. La costruzione di tale mezzo probatorio si snoda attraverso tutta una serie di passaggi delicatissimi, che attualmente nel nostro paese sono svolti all'interno dei laboratori scientifici della polizia giudiziaria.

In quest'ottica, l'affidabilità di tale strumento è strettamente legata alle capacità dei laboratori che si occupano di queste analisi di assicurare la competenza degli operatori, la disponibilità delle risorse tecnico logistiche necessarie, la validità delle metodiche utilizzate. Bisogna, in sostanza, garantire che i laboratori interessati salvaguardino la qualità del loro operato e delle competenze tecniche di coloro che vi lavorano. Per questo motivo, in generale, si ricorre all'accreditamento dei laboratori sia secondo le norme ISO, sia attraverso linee guida specifiche che siano complementari ad altri strumenti e che devono tenere conto delle ricadute che analisi di questo tipo hanno sulla sicurezza e libertà dei cittadini.

Inoltre, non va dimenticato, che nella pratica delle indagini genetiche, si sono spesso verificati i c.d. falsi positivi, che determinano un'identificazione erronea a danno di un innocente. Per tale motivo è necessario che l'analisi del dna per scopi investigativi, venga ulteriormente perfezionata, soprattutto per quanto riguarda il controllo di qualità e la certificazione dei laboratori e le capacità di intervento degli agenti di polizia giudiziaria sul luogo del delitto.

In particolare, nel momento in cui il reperto biologico viene individuato sulla scena del crimine devono essere osservate ferree prescrizioni legate alla

[304] JASANOFF, *La scienza davanti ai giudici*, Milano, 2001, 138.

integrità della scena del delitto, per evitare eventuali forme di inquinamento del materiale da fattori estranei alla scena stessa o da soggetti non coinvolti nella commissione del reato. Negli Stati Uniti dove ormai l'indagine genetica ha assunto nel corso degli anni sempre maggiore importanza, esiste un reparto speciale della polizia deputato alla conservazione del luogo del crimine per preservarlo da possibili fattori contaminanti che potrebbero mettere a repentaglio le operazioni tecniche degli investigatori[305]. Allo stesso modo anche in Italia è stato implementato lo stesso protocollo d'azione, fatto di un'attività preliminare, c.d. di repertazione, lasciata alla perizia delle unità scientifiche della polizia giudiziaria e una successiva di analisi in laboratorio, di competenza di tecnici preparati per l'estrazione del dna e per l'ottenimento del risultato finale: *id est* il profilo identificativo di un determinato campione, pronto per essere usato nella dinamica delle indagini attraverso il confronto con gli altri dati in possesso dell'autorità giudiziaria[306].

A prescindere da eventuali inquinamenti della prova generati dall' imperizia degli operatori che eseguono le attività di estrazione del profilo e repertazione sul luogo del crimine, esiste un margine di incertezza caratteristico, per la verità bassissimo, del giudizio di identità espresso all' esito del confronto positivo di due profili identificativi del dna[307]. Nel senso che, non si può escludere a priori l'esistenza di un secondo profilo identificativo – oltre a quello appartenente al vero colpevole del delitto – uguale a quello utilizzato dagli investigatori per l'indagine genetica.

In linea di principio solo nell'ipotesi di gemello omozigote esiste una identità certa di profili genetici, tale per cui all'esito delle operazioni di identificazione potrebbero esistere due individui identificabili con lo stesso dato genetico. Negli altri casi l'eventuale comunanza a due o più soggetti delle tredici zone isolate della molecola del dna – che compongono di fatto il dato da confrontare con il soggetto sospettato – costituisce una probabilità vicina ad uno su un milione di miliardi[308].

[305] TONINI, *Manuale di procedura penale,* cit. , 462.
[306] DOMINIONI, *In tema di nuova prova scientifica*, in *Dir. pen. proc.*, 2001, 1062.
[307] GARGANI, *I rischi e le possibilità dell'applicazione dell'analisi del DNA nel settore giudiziario,* in *Riv. it. dir. proc. pen.*, 1993, 1312.
[308] FANUELE, *L'indagine genetica nell'esperienza italiana ed in quella inglese*, cit., 735.

Tale considerazione assume un particolare valore di carattere sistematico, se si pensa al fatto che negli Stati Uniti, proprio l'esistenza di questo ridottissimo margine di fallibilità, ha fatto mutare la denominazione che inizialmente gli studiosi avevano assegnato al suddetto mezzo di prova, da *dna fingerprint*, che solennemente affermava il crisma di unicità del risultato ottenuto dalla comparazione dei profili identificativi impiegati per le indagini, a *dna profiling*[309],che in modo meno formale riconosce all'esito del raffronto un potenziale scientifico di rilievo ma certamente non di carattere assoluto. Occorre rimarcare altresì come lo stesso materiale biologico può generare facilmente la realizzazione di rappresentazioni false della scena del crimine, vista la semplicità con cui il dna può essere trasportato (si pensi al capello lasciato intenzionalmente su luogo del delitto).

Senza dubbio queste considerazioni danno consistenza a dubbi e incertezze, riguardanti soprattutto il grado di autosufficienza probatoria della rappresentazione attuata con l'ausilio del dna. Peraltro, va sottolineato come l'attività di identificazione genetica costituisca a tutti gli effetti un mezzo di prova indiziario, seppur fortemente persuasivo, insufficiente da solo ad accertare la colpevolezza dell'imputato.

Invero – come sottolineato più in generale in relazione alle banche dati criminalistiche – il profilo identificativo tipizzato dal materiale biologico del soggetto sospettato, o repertato sul luogo del delitto, costituisce un indizio che ai sensi dell'art. 192 c.p.p. necessita, per poter essere valutato positivamente dal giudice, delle caratteristiche richiamate dalla norma *de qua*: vale a dire che deve essere confermato da una serie di elementi ulteriori. In tal senso la verifica emergente dall'assunzione di tale mezzo di prova non può andare al di là di una conferma oggettiva rispetto all'identità di un soggetto o, tutt'al più, riguardo alla presenza di quest'ultimo nel luogo in cui è stato rinvenuto il reperto. Eventuali rappresentazioni complete dello svolgimento dinamico del fatto reato, devono risultare da una trama investigativa, all'interno della quale il ragionamento

[309]RICCI – PREVIDERÈ – FATTORINI - CORRADI, *La prova del DNA per la ricerca della verità*,cit. , 471.

induttivo che porta all'identificazione genetica del sospettato non può rappresentare l'unico filo[310].

Se è vero che da un punto di vista puramente pratico, nell'indagine genetica il nostro paese – a parte la l'assenza della banca dati – ha un grado di sviluppo e applicazione che lo pone allo stesso livello di quelli in cui tale forma di investigazione si utilizza da molto più tempo; allo stesso modo si può affermare come sotto un profilo giuridico esista a tutt'oggi una situazione di assoluta inadeguatezza e disomogeneità del quadro normativo di riferimento.

Il legislatore non ha ancora regolamentato in modo compiuto gli aspetti salienti del *dna profiling*, al punto che gli inquirenti vivono una situazione operativa poco chiara[311]. In particolare, fin da quando la Corte costituzionale con la sentenza n. 238 del 1996[312] ha dichiarato l'illegittimità costituzionale dell'art. 224 comma 2 c.p.p. nella parte in cui non prevede i casi e i modi nei quali può essere limitata la libertà personale di un soggetto sottoposto a perizia[313].

Nello specifico la consulta ha considerato lesiva del principio di *habeas corpus* l'apprensione coercitiva di materiale ematico da sottoporre all'attività del perito, sollecitando nel contempo un intervento integrativo in materia da parte del legislatore, tale da individuare i presupposti oggettivi indispensabili per poter avviare l'attività peritale in situazione siffatte[314].

In dottrina[315] vengono indicati come atti sulla persona, per i quali – a seguito della decisione della Corte costituzionale – è vietato un intervento coattivo, quelle azioni che mirano ad apprendere notizie che appartengono alla

---

[310]FERRUA, *Il giudizio penale: fatto e valore giuridico*, in *La prova nel dibattimento penale*, II ed. , Torino, 2005, 312; TONINI, *La prova penale* IV ed., Padova, 2000, 101; UBERTIS, *La prova penale. Profili giuridici ed epistemologici*, Torino, 1995, 105.

[311]Solo recentemente il legislatore ha regolato la materia dei prelevamenti coattivi a carico dell'imputato nel caso di rifiuto di quest'ultimo. L'occasione normativa è stata offerta dalla legge n. 85 del 2009 che ha introdotto nel nostro ordinamento la banca dati del dna, tale disposizione reca una modifica del codice di procedura penale attraverso l' introduzione del nuovo articolo 224 *bis*, che di fatto corregge il codice di rito seguendo gli auspici manifestati dal giudice delle leggi dalla sentenza 238 del 1996. (vedi *infra* par. 3.2). BELFIORE, *La prova del Dna a fondamento di un mandato d'arresto europeo: via libera alla consegna*, in *Cass. pen.*, 2009, 1447.

[312] Corte cost., 27 giugno 1996 n. 238, in *Giur. cost.*, 1996, 2142.

[313]FELICIONI, *Accertamenti personali e coattivi nel processo penale: linee di riforma*, cit., 615;VIGONI, *Corte Costituzionale, prelievo ematico coattivo e test del DNA*, in *Riv. it. dir. proc. pen.*, 1996, 1023.

[314]FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, cit. , 5.

[315]BORDIERI, *Sul valore probatorio del rifiuto ingiustificato dell'imputato di sottoporsi al prelievo del DNA*, in *Cass. pen*., 2004, 4169.

sfera "intracorporale" del soggetto. Per contro sono considerate assolutamente legittime le operazioni tecniche rivolte alla conoscenza di dati c.d. "extracorporali" – attuabili anche con l'immobilizzazione momentanea della persona da descrivere – attraverso la relazione, la fotografia o la misurazione ovvero la registrazione dei dati relativi alle impronte digitali. Peraltro tale costruzione ermeneutica si rifà alla bipartizione effettuata in materia dalla stessa Corte costituzionale con una pronuncia sulla legittimità dell'art 4 t.u.l.p.s.[316] , nella parte in cui consentiva alla polizia di effettuare rilievi segnaletici. In tale decisione la consulta ha teorizzato la distinzione esistente tra i rilievi riguardanti l'aspetto esteriore della persona e i rilievi che si concretizzano in ispezioni personali, individuando solo nei secondi il carattere di limitazione della libertà fisica e morale dell'individuo, con la conseguente applicabilità della duplice garanzia prevista dall'art. 13 della Costituzione[317].

Anche la giurisprudenza della corte di cassazione, nelle pronunce successive alla decisione della Consulta, ha ribadito l'incoercibilità dei prelievi invasivi sull'individuo, seppur attraverso la legittimazione di alcune pratiche investigative, finalizzate ad una progressiva attenuazione degli effetti distorsivi creati dalla lacuna legislativa in materia, e indirizzate al rinvenimento di informazioni genetiche da oggetti contenenti materiale biologico appartenente al soggetto indagato che non ha prestato il consenso al prelievo del materiale biologico. In particolare la Suprema corte afferma la possibilità di compiere accertamenti tecnici sulle tazzine del caffè, sulle sigarette del sospettato, o su qualsiasi reperto biologico individuato in luoghi frequentati da quest'ultimo[318], allo scopo di rinvenire il profilo identificativo del dna. In tali casi non si

[316] Corte cost., 27 marzo 1962 n. 30, in *Giur. cost.*, 1962, 241.

[317] "Merita richiamare l'attenzione su due affermazioni della Corte. In primo luogo la Consulta ha precisato che si ha violazione della libertà personale non soltanto nel caso di coercizione fisica dell' individuo, ma anche qualora si verifichi una menomazione della libertà morale determinata da un assoggettamento totale della persona all'altrui potere. In seconda battuta i giudici costituzionali hanno chiarito che la differenza tra provvedimenti incidenti e provvedimenti non incidenti sulla libertà personale debba essere individuata non tanto nel carattere più o meno momentaneo e lieve dell'eventuale coercizione fisica, quanto nel fatto che la medesima implichi o meno sostanziali limitazioni fisiche o morali della libertà": così, FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, cit., 7; SANTACROCE, *Prelievo coattivo del sangue a scopo probatorio e tutela della libertà personale*, in *Cass. pen.*, 1996, 3570.

[318] E' legittima secondo la corte di cassazione l'acquisizione e l'utilizzo del materiale biologico a fini investigativi di un campione di sangue già precedentemente prelevato dal soggetto a fini diagnostici; Cass., sez. I, 22 giugno 1999, Fata, in *Dir. pen. proc.*, 2006, 983.

configurerebbe un prelievo intracorporale – che necessiterebbe per essere attuato del consenso dell'indagato e per il quale sarebbe vietata un'azione coercitiva dell'autorità giudiziaria – , ma di un'analisi effettuata su materiale biologico non appartenente più alla sfera corporale del soggetto e come tale qualificabile alla stregua di una cosa comune[319] . In queste situazioni il rifiuto dell'indagato al prelievo è stato aggirato oltre che attraverso attività di investigazione finalizzate al recupero di tali oggetti (pedinamenti, offerta di bevande allo scopo di repertare la saliva contenuta sul bicchiere)[320], anche attraverso i classici mezzi di ricerca della prova: *id est* mediante perquisizioni, ispezioni o sequestri diretti all'apprensione di cose appartenenti all'indagato e potenzialmente utilizzabili per attività inerenti ad accertamenti genetici[321]. Inoltre in alcune pronunce la Corte di legittimità ha affermato come lo stesso rifiuto ingiustificato dell'imputato di sottoporsi al prelievo necessario per l'esame del dna è legittimamente valutabile come elemento di prova integrativo: tale rifiuto, infatti, può essere liberamente apprezzato dal giudice nella formazione del suo convincimento e può altresì essere utilizzato come riscontro individualizzante alla chiamata di correo[322].

Peraltro – nonostante la chiara pronuncia della Consulta – l' indiscriminata possibilità di invadere la sfera della libertà personale in occasione dello svolgimento di attività tecniche è stata ribadita dalla modifica dell'articolo 349 c.p.p. da parte della legge 155 del 2005 , la quale non fa alcun riferimento ai casi in cui tale tipo di operazione può essere compiuta. Per di più, oltre ad aver riproposto l'indeterminatezza riguardo alle ipotesi, il legislatore ha colpevolmente attuato un affievolimento delle garanzie personali riconosciute dalla Costituzione, attribuendo l'iniziativa rivolta alla limitazione coercitiva della libertà personale alla polizia giudiziaria.

[319] Cass., sez. I, 11 marzo 2003, Esposito, in *Dir. e giust*., 2003, n. 34, 98.
[320] Cass., sez. I, 23 giugno 2005, P., in *Guida dir.*, , 2005, n. 38, 82; Cass., sez. I, 10 maggio, 2005, D., ivi, , 2005, n. 35, 103.
[321] Cass., sez. II, 13 marzo 2007, M., in *Guida dir.*, 2007, n.18, 96.
[322] Cass., sez. I, 20 settembre 2002, Peddio, in *Cass. pen*, 2003, 3500.

3.1 ***(segue) Il prelievo coattivo di materiale biologico ad opera della polizia giudiziaria***

L'intervento integrativo dell'articolo art. 349 c.p.p., in materia di investigazione genetica, attuato dalla legge "anti terrorismo" n. 155 del 2005, prevede la possibilità di un ingerenza coercitiva da parte della polizia giudiziaria per il recupero del materiale biologico dell'indagato nel corso delle operazioni deputate alla identificazione di quest'ultimo[323]. Questa attività d'indagine – coessenziale rispetto alla risoluzione dell'oggettiva impossibilità di realizzare il riconoscimento del soggetto sospettato della commissione di un reato – avviene attraverso il prelievo di capelli o col metodo dell'*oral swab*, previa autorizzazione scritta del pubblico ministero, oppure resa oralmente e confermata in secondo momento per iscritto.

Da un punto di vista puramente pratico l'innovazione non è di poco conto, se si pensa alle difficoltà operative che si venivano a creare in precedenza a causa della mancanza di una tale previsione. Il fatto di poter disporre del dna del sospettato, senza che questi possa opporre nessuna resistenza alle operazioni degli inquirenti, permette l'avvio immediato della indagine genetica, *id est* la possibilità di realizzare un confronto tempestivo con i reperti individuati sulla scena del crimine. Peraltro la norma nulla dice sulla conservazione del materiale biologico, ne sui possibili eventuali utilizzi che gli inquirenti possono fare di questo in indagini successive a quelle in cui si è realizzata l' apprensione coatta.

In dottrina si rinvengono due interpretazioni distinte sul contenuto dell'articolo *de quo*. Alcuni autori sostengono che i rilievi sull'indagato possono essere compiuti anche nei casi in cui non si nutra nessun dubbio sull'identità di quest'ultimo, nell'ottica della conservazione del dato biologico appreso, attraverso la creazione di "cartelle segnaletiche"[324]. Invero, secondo tale orientamento, dopo

[323]FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico,* cit., 145.

[324]CANTONE, *Le modifiche processuali introdotte con il "decreto antiterrorismo"* , in *Cass. pen.* , 2005, 2507; SCALFATI, *Potenziamento della polizia giudiziaria tra ruoli investigativi ed intrusioni* de libertate, in *Terrorismo internazionale: modifiche al sistema penale e nuovi strumenti di prevenzione*, a cura di ROSI – SCOPELLITI, Milano 2006, 91; TONINI, *Manuale di procedura penale,* cit., 416.

la modifica dell'art. 349 c.p.p. le schede personali contenute negli archivi segnaletici della polizia giudiziaria, dovrebbero essere corredate, oltre che dai dati classici propri dell'attività identificativa, anche dal profilo genetico del sospettato. Come dire che la polizia giudiziaria potrebbe risolvere per via induttiva – attraverso una interpretazione oltremodo estensiva della lettera dell'articolo – il problema pratico dell'assenza della banca dati nazionale del dna. Dare vita a dei profili segnaletici con relativo dna accluso, significa infatti, in altre parole, legittimare in modo capzioso la creazione di micro banche dati surrettizie interne alle forze di pubblica sicurezza[325].

A parere di chi scrive, questa conclusione risulta un po' forzata, se si pensa alla particolare natura dei dati in oggetto. Il garante della *privacy* si è più volte pronunciato in modo critico sulla indebita realizzazione di banche dati genetiche non autorizzate, create dalla polizia giudiziaria[326]. Altri autori, considerano il prelievo coattivo di materiale biologico fatto dalla polizia giudiziaria, limitato alle operazioni di identificazione, tale per cui potrà essere attivato solo in via residuale nei casi in cui non sia possibile arrivare all'identità del soggetto in modi alternativi[327].

Preso atto della lacuna dell'articolo in questione, occorre immaginare, una interpretazione delle norme che tuteli contemporaneamente la protezione del dato genetico del sospettato e che colga la *ratio* della modifica normativa, soprattutto alla luce della recente novella legislativa sulla banca dati nazionale del dna che ha modificato il codice di procedura penale con l'aggiunta di due nuovi articoli il 224 *bis* e il 359 *bis.*

Il prelievo del campione biologico nelle situazioni indicate dall'art. 349 comma 2 - *bis* c.p.p. – nella ricostruzione fatta da quegli autori che ricollegano a quest'ultimo la possibilità di creare cartelle segnaletiche corredate dal profilo genetico dell'indagato [328]– travalica le necessità legate alle attività di mera

---

[325] BARROCU, *Brevi note in tema di indagini per i reati di criminalità organizzata*, in www.*dirittoestoria.it* , quaderno n. 4, 2005.

[326] Vedi par. 3.3

[327] DALIA, *Il prelievo coattivo di materiale biologico per l'identificazione dell'indagato e per l'acquisizione di elementi probatori*, in *Le nuove norme di contrasto al terrorismo*, a cura di DALIA, Milano, 2006, 261; PAULESU, *Commento all' art. 349*, in *Codice di procedura penale commentato*, a cura di GIARDA – SPANGHER, cit., 3090; KOSTORIS, *Prelievi biologici coattivi*, in KOSTORIS – ORLANDI, *Contrasto al terrorismo interno e internazionale*, Torino, 2006, 29.

[328] CANTONE, *Le modifiche processuali*,cit., 2507.

identificazione del soggetto. In definitiva il limite all'utilizzazione del materiale biologico acquisito dall'indiziato ad opera della polizia giudiziaria nel corso delle indagini non può essere individuato nella creazione di cartelle genetiche personali, in quanto la conservazione *tout court* di tale dato allargherebbe oltremodo il significato della modifica operata dalla legge del 2005. Per contro risulta più aderente alla *ratio* della norma *de qua* una esegesi restrittiva, che privilegi la risoluzione delle emergenze oggettive interne alle indagini in corso, e che tenda a fornire una risposta a queste ultime[329], piuttosto che una interpretazione estensiva che arrivi fino a ricomprendere nella lettera della norma anche operazione di mantenimento del dato genetico volte a fronteggiare esigenze di carattere preventivo legate alla necessità di offrire più strumenti possibili alla polizia giudiziaria per le condurre operazioni di identificazione personale.

In tal senso, pare inverosimile individuare il significato dell'art. 349 comma 2 - *bis* c.p.p. nelle operazioni di conservazione alla stregua di informazioni *ad abundantiam*, al fianco di quelle poste in essere attraverso la catalogazione di dati dattiloscopici o antropometrici. Tale scopo potrà essere svolto dalle informazioni genetiche solo nei casi di assoluta necessità, in cui sia totalmente impossibile operare l'identificazione della persona nei cui confronti vengono svolte le indagini con i "rilievi classici".

Sotto il profilo oggettivo le informazioni rilevabili dalle varie operazioni identificative non sono comparabili, perché il materiale biologico di un individuo contiene un bagaglio di notizie personali che va al di la della sterile sequenza alfa numerica utilizzata per costruire il profilo identificativo del soggetto. In quest'ottica, va stigmatizzata la colpevole omissione fatta dal legislatore sulla sorte del materiale biologico adoperato per identificare la persona sottoposta alle indagini, del quale non è prevista né una esplicita distruzione – nel caso in cui ad esempio non sia più utile agli inquirenti – né alcun limite in relazione a forme di utilizzo differenti da quelle per cui è stato prelevato dall'autorità giudiziaria.

[329] Per una ricostruzione sistematica dell'articolo 349 comma 2 - *bis*, e, in senso più generale, del ruolo della polizia giudiziaria nello svolgimento di indagini genetiche, aventi ad oggetto il prelievo e il successivo accertamento del materiale biologico coattivamente appreso, nel solco di quanto disciplinato dalla recente legge n. 85 del 2009 sull'adesione della repubblica italiana al Trattato di Prum, vedi par. 3.2.

Inoltre, va rimarcato come la trama normativa che si presenta agli occhi dell'interprete – generata dalla modifica sostanziale apportata alle norme del codice di rito dalla legge n. 85 del 2009 – appare alquanto sfilacciata.

A parere di chi scrive, tale previsione – creata in un momento storico particolare in cui svolgeva un ruolo di surrogato della banca dati del dna – andrebbe riconsiderata, posto che l'implementazione del *database* nazionale da parte delle legge *de qua* risolve alla radice il motivo di fondo che aveva condotto il legislatore del 2005 a realizzare l'introduzione di un comma 2 - *bis* nella lettera dell'articolo 349: *id est* l'impossibilità da parte dell'autorità giudiziaria, ogniqualvolta l'indagato rifiutasse di consentire al prelievo del materiale biologico, di disporre di dati genetici per lo svolgimento del confronto con i reperti individuati sulla scena del crimine.

Se, come accennato in precedenza, l'obiettivo legato alla identificazione individuale può essere facilmente risolto con l'ausilio di metodi tradizionali – affidabili almeno quanto i dati genetici – non si capisce la necessità di rafforzare il novero di informazioni personali a disposizione delle autorità di pubblica sicurezza; né tantomeno l' opportunità di avere un catalogo alternativo alla banca dati nazionale del dna, corredato da notizie genetiche utilizzabili in future indagini, visto e considerato come il neonato *database* può assolvere da solo a questo compito, in modo preciso, e nel rispetto della *privacy* genetica. Stilare cartelle segnaletiche arricchite dei profili identificativi genetici dell' indiziato, equivarrebbe a costruire una specie di " banca dati di secondo livello ", totalmente slegata dalla cornice normativa ricavata dalla legge di adesione al Trattato di Prum.

Peraltro, seguendo l'impostazione della legge *de qua* e vista la soppressione dell'ultima parte del comma 3 dell'articolo 354 che richiamava la possibilità per la polizia giudiziaria di effettuare accertamenti urgenti sul materiale biologico prelevato da una persona con le modalità d'intervento richiamate dal comma 2 - *bis* dell'articolo 349, si può concludere come tali attività siano ormai prerogativa dell'autorità giudiziaria, in base alle regole previste dai nuovi articoli inseriti dalla legge n. 85 del 2009. A tal proposito, qualora la necessità di un accertamento tecnico sul dna del sospettato dovesse manifestarsi nel corso delle indagini, troverebbe spazio la previsione degli artt. 359 e del nuovo 359 *bis* nel particolare caso in cui il soggetto neghi il proprio consenso al prelievo del

campione biologico da sottoporre ad analisi comparativa. Tutto ciò nel solco di una logica di sistema che privilegia l'attivazione delle operazioni legate all'analisi genetica dei reperti biologici solo nel caso in cui questi siano indispensabili per la prosecuzione delle indagini.

3.2) ***(segue) Gli accertamenti tecnici sulla persona nella legge del 30 giugno 2009 n.85***

La legge n. 85 del 2009 – che ratifica l'adesione della repubblica italiana al Trattato di Prum[330] – introduce una serie di modifiche al codice di rito volte al riequilibrio di una situazione pratica alquanto disorganica e caratterizzata da un palese squilibrio funzionale, se si considera il modo in cui – in contesti affini – il potere di disporre prelievi coattivi veniva concesso alla polizia giudiziaria, previa autorizzazione del pubblico ministero, ma non all'autorità giudiziaria.

Infatti, come visto in precedenza, in base al disposto dell'art. 349 comma 2 *bis*, il prelievo coattivo di materiale biologico poteva avvenire solo in occasione della necessità di identificare il soggetto sottoposto alle indagini.

Al contrario, nei casi in cui l'autorità giudiziaria intendeva svolgere accertamenti tecnici o perizie sulla persona rivolte al prelievo di materiale biologico, si verificava una limitazione evidente dell'attività investigativa, dovuta all'assenza di norme specifiche sui casi e i modi d'esercizio di un'azione coercitiva nei confronti dei soggetti che non prestavano il loro consenso alle attività tecniche richieste.

Pertanto la legge *de qua* risolve positivamente una difficoltà sistematica che il nostro processo penale si trascinava dietro ormai da più di un decennio. Peraltro nel corso degli anni non sono mancati gli interventi della dottrina volti a segnalare al legislatore la necessità di una presa in carico per la risoluzione del problema. Quest'ultimo da parte sua ha individuato possibili soluzioni della

[330] Vedi par. 3.4.

questione, tuttavia senza andare mai al di la di sterili e improduttivi progetti di legge[331].

Contrariamente al passato, lo strappo normativo creato dalla previsione di illegittimità costituzionale dell'art. 224 c.p.p. dichiarata dalla Corte con la sentenza n. 238 del 1996[332] è stato ricucito in modo sostanziale dalla disposizione dalla legge *de qua*, attraverso una interpolazione del codice di rito con l'introduzione di due nuove norme: gli artt. 224 - *bis* e 359 - *bis*, in merito alla possibilità da parte dell'autorità giudiziaria di prelevare coattivamente materiale biologico per consentire lo svolgimento degli accertamenti tecnici nel corso delle indagini preliminari o nell'esecuzione di una perizia.

Il nuovo articolo 224 - *bis*, prevede la possibilità da parte dell'autorità giudiziaria di disporre il prelievo coattivo di materiale biologico nei confronti di un soggetto che non presti il proprio consenso all'attività tecnica, ogniqualvolta questo sia necessario per eseguire una perizia. La lettera della norma non fa alcun richiamo alla distinzione teorizzata in dottrina, tra atti invasivi e atti non invasivi sulla persona, in relazione alle modalità di intervento da parte dell' autorità giudiziaria, al contrario si limita ad un più generale riferimento ad "atti idonei ad incidere sulla libertà personale" finalizzati alla determinazione del profilo genetico, indicando in particolare il prelievo di capelli, di peli o di mucosa del cavo orale o accertamenti medici[333]. L'articolo *de quo* individua come modalità preferibile di accertamento, a parità di risultati ottenibili, la pratica di interventi non invasivi, e prevede altresì al comma 4, alcuni limiti in base ai quali non possono essere disposte in nessun modo perizie; in particolare, nel caso in cui queste contrastino con espressi divieti posti dalla legge o mettano in pericolo la

[331] FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, cit., 219.

[332] Corte cost., 27 giugno 1996 n. 238, cit., 2142. Nel periodo di vuoto legislativo, a causa di quanto disposto dalla Corte Costituzionale, quando nel corso delle indagini preliminari l'attività di un consulente tecnico necessitava del dna del sospettato – per eseguire un'indagine genetica attraverso un accertamento tecnico non ripetibile *ex* art. 360 c.p.p. –, l'ausiliare del pubblico ministero aveva necessariamente bisogno del consenso dell'indagato per effettuare il prelievo di materiale biologico; alle stesse condizioni sottostava l'esecuzione di una perizia – da svolgersi durante il dibattimento o nel corso di un incidente probatorio – avente il medesimo oggetto.

[333] "Il riferimento agli accertamenti medici pone qualche disagio in più all'interprete. L'espressione utilizzata da legislatore, infatti, appare così indeterminata da legittimare una vasta gamma di accertamenti dalle tecniche di percezione visiva alla somministrazione di sostanze , fino all'introduzione di strumenti all'interno del corpo dell'individuo". FELICIONI, *L'acquisizione di materiale biologico a fini identificativi o di ricostruzione del fatto*, cit., 225.

vita, l'integrità fisica o la salute della persona o del nascituro, ovvero quando secondo la scienza medica, possano provocare sofferenze di non lieve entità.

Peraltro nell'ottica di un'analisi complessiva delle modalità di esecuzione della perizia *ex* art. 224 - *bis* c.p.p. , va rimarcato che "il parlamento ha scelto di lasciare libertà agli esperti chiamati ad eseguire le operazioni, senza tracciare una disciplina di dettaglio che avrebbe imbrigliato l'evoluzione tecnologica"[334].

Inoltre, la nuova norma prescrive al giudice l'inserimento, nella motivazione posta a base del provvedimento che dispone la perizia, di una verifica legata alle potenzialità probatorie del mezzo di prova. A tal fine la pronuncia dell'ordinanza dovrà dar conto dell'assoluta indispensabilità dell'attività peritale per la prova dei fatti.

Il provvedimento col quale il giudice ordina la perizia contiene, in aggiunta al contenuto ordinario previsto dall'articolo 224 c.p.p. , anche una serie di ulteriori requisiti legati: alla peculiare situazione in cui si inserisce l'accertamento peritale, e alle specifiche attività che il perito deve svolgere[335]. La pronuncia giudiziale presuppone che si debba procedere a perizia per reati per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a tre anni. Va precisato infine, in che cosa consiste la coazione esercitabile su provvedimento del giudice. Ciò dipende dall'entità della non collaborazione del soggetto passivo che può non comparire senza addurre un legittimo impedimento nel luogo, nel giorno e nell'ora stabiliti per le operazioni peritali; può non comparire e, accompagnato coattivamente, rifiutare di sottoporsi alle operazioni; può presentarsi ma non consentire al prelievo o all'accertamento medico. In concreto quindi, la persona può subire alternativamente l'accompagnamento coattivo oppure l'accompagnamento coattivo e l'esecuzione forzosa del prelievo (o dell'accertamento medico), oppure il solo prelievo (o accertamento medico) coattivo

[334] TONINI, *Manuale di procedura penale*, cit., 330.

[335] L'ordinanza contiene a pena di nullità: le generalità della persona da sottoporre all'esame del perito e quanto valga ad identificarla, l'indicazione del reato per cui si procede con la descrizione sommaria del fatto, l'indicazione specifica del prelievo o dell'accertamento da effettuare e delle ragioni che lo rendono assolutamente indispensabile per la prova dei fatti, l'avviso della facoltà di farsi assistere da un difensore o da persona di fiducia, l'avviso che, in caso di mancata comparizione non dovuta a legittimo impedimento, potrà essere ordinato l'accompagnamento coattivo, l'indicazione del luogo, del giorno e dell'ora stabiliti per il compimento dell'atto e delle modalità di compimento.

La legge n. 85 del 2009 ha introdotto anche il nuovo articolo 359 - *bis*, relativo alla possibilità del pubblico ministero di disporre il prelievo coattivo di materiale biologico nel corso delle indagini, nel caso in cui si proceda ad un accertamento tecnico ripetibile attraverso l'ausilio di consulenti tecnici.

In tali casi la nuova norma impone all'organo inquirente di rivolgersi al giudice delle indagini preliminari per ottenere un provvedimento autorizzativo al fine di poter svolgere l'accertamento coattivamente nei confronti dell'indagato che non presti il proprio consenso alle operazioni necessarie. In situazioni di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave o irreparabile pregiudizio alle indagini, il pubblico ministero è legittimato a disporre in prima persona lo svolgimento coattivo delle attività tecniche, attraverso la pronuncia di un decreto motivato, che dovrà essere confermato, entro le quarantotto ore successive dalla decisione, da un ordinanza del giudice per le indagini preliminari.

Inoltre la legge *de qua* all'art. 27 prevede la soppressione del secondo periodo dell'articolo 354 c.p.p. . In particolare del richiamo adesivo fatto da quest'ultimo al comma 2 - *bis* dell'art. 349 c.p.p. , relativo alle modalità per porre in essere gli accertamenti biologici effettuati dalla polizia giudiziaria sulle persone indiziate, in situazioni di particolare urgenza. Tale cancellazione pare affermare la priorità del pubblico ministero nella direzione di tutte le attività tecnico scientifiche inerenti al prelievo coattivo di materiale biologico; sicché la polizia giudiziaria non potrà più attivarsi autonomamente – *id est* senza impulso da parte del p.m. –, per la realizzazione di operazioni legate al prelievo forzoso di campioni biologici, neanche se questi siano necessari in relazione a situazioni di particolare urgenza.

In quest'ottica, va segnalato come anche le attività legate alla identificazione dell'indagato, svolte attraverso l'apprensione di materiale biologico in casi di urgenza, debbano necessariamente essere autorizzate, dal pubblico ministero. Peraltro, il fatto che tale norma non sia stata modificata o cancellata dalla legge *de qua* impone, una interpretazione sistematica dello stesso art. 349 comma 2 - *bis*, considerato come il ruolo di quest'ultimo, non sia più inquadrabile – così come ampiamente indicato nel paragrafo precedente – nelle operazioni di identificazione. L' idea che la possibilità di prelevare materiale biologico da un soggetto indagato riguardi, in situazioni particolari legate

all'identificazione dello stesso, anche le forze di polizia giudiziaria, s'inserisce nella categoria di quelle operazioni d'investigazione attivabili in chiave assolutamente anticipatoria rispetto all'iniziativa dell'autorità giudiziaria. In circostanze siffatte, come avviene ad esempio per gli accertamenti urgenti sul luogo del reato o delle perquisizioni nei casi di evasione o arresto in flagranza, verrebbe messo in sicurezza l'oggetto dell'indagine tecnica in funzione di un ulteriore approfondimento investigativo.

Il presupposto oggettivo per l'attivazione da parte della polizia giudiziaria deve essere ricercato nella assoluta necessità di operare un confronto genetico tra il dna dell'indagato e quello individuato sul luogo del delitto: vale a dire in tutti quei casi in cui si rinviene sulla scena del crimine del materiale biologico appartenente a soggetti ignoti e la ricerca del colpevole attraverso il raffronto dei profili genetici diventa una assoluta emergenza investigativa. Per far fronte a tali situazioni di urgenza la polizia giudiziaria potrebbe operare i prelievi del materiale biologico dal soggetto sospettato, e fare gli accertamenti tecnici necessari per verificare la corrispondenza genetica tra il dna di quest'ultimo e quello individuato sul luogo del delitto.

In tal modo si configurerebbe una nuova e caratteristica forma di accertamento tecnico urgente delle forze di polizia, con riferimento agli accertamenti genetici in situazioni di particolare necessità, nel solco di quanto previsto dalle norme del codice in contesti riconducibili a questi ultimi ed alla previsione dell'articolo 13 della Costituzione, che richiede, come requisito indispensabile nelle attività *ex abrupto* poste in essere dalla polizia giudiziaria, i requisiti di necessità ed urgenza.

Inoltre, il fatto stesso che nell'ipotesi di prelievo coatto da parte della polizia giudiziaria per le operazioni di identificazione dell'indiziato indicata dall'attuale comma 2 - *bis* dell'articolo 349 c.p.p. sia prevista un'autorizzazione da parte del pubblico ministero – scritta o orale a seconda del grado di tempestività col quale deve essere avviata l'indagine –, pone tra le due attività, ricerca del materiale genetico e accertamento tecnico, un collegamento pragmatico difficilmente scindibile, nel senso che risulta arduo pensare ad un prelievo confinato e finalizzato solo ed elusivamente alla identificazione dei soggetti indagati. Pare invece più aderente alla realtà dei fatti uno sviluppo dinamico delle due attività in un rapporto di assoluta interconnessione, tale per cui

ad un prelievo di materiale biologico con successiva tipizzazione del profilo genetico, debba conseguire una operazione di confronto rivolta all'accertamento di eventuali corrispondenze tra il dna del sospettato e quello a disposizione dell'autorità giudiziaria. In quest'ottica, anche alla luce di quanto previsto dalla recente novella legislativa, pare più corretto inserire l'iniziativa della polizia giudiziaria indicata dal comma 2 - *bis* dell'art. 349, nel solco generale delle azioni legate agli accertamenti tecnici sulla persona operati dall'autorità giudiziaria, *id est* come attività prodromica o sostitutiva degli stessi in casi di particolare urgenza.

Del resto, anche l'art. 359 - *bis* nell' *incipit* fa salvo il riferimento al disposto dell'art. 349 comma 2 - *bis*, lasciando intendere come quest'ultimo si inserisca a pieno titolo, per far fronte a situazioni speciali, nel novero delle attività tecniche limitative della libertà personale, per le quali è necessario un prelievo coattivo di campioni biologici su persone viventi.

Peraltro sarebbe auspicabile una riscrittura della norma *de qua*, che metta in risalto il ruolo costruttivo che può esercitare la polizia giudiziaria nelle operazioni di accertamento genetico svolte dall'autorità giudiziaria e che elida completamente il rapporto tra dato biologico e operazioni di mera identificazione, confinando quest' ultimo solo a casi marginali, in cui risulti assolutamente impossibile identificare il soggetto con i rilievi dattiloscopici classici.

3.3) ***Archivi genetici atipici: una vicenda tutta italiana***

I reparti speciali della polizia giudiziaria scientifica nazionale, praticano già da tempo i raffronti delle informazioni genetiche a scopi ricognitivi, utilizzando le metodologie classiche importate dagli Stati Uniti, ormai considerate alla stregua di leggi scientifiche persuasive e attendibili.

L'indagine condotta sui *locus* STR [336], infatti costituisce la base tecnico-scientifica dell'inferenza, che porta ad affermare, con una percentuale ridottissima di errore, che in presenza di un valore corrispondente tra due profili del dna di tredici porzioni del genoma – alleli – ci si trova al cospetto della stessa persona.

[336] Vedi cap. I, par. 3.

A tal proposito, la crescente importanza delle operazioni di confronto dei dati biologici, unita al fatto che tale tipo di investigazione risulta decisamente più efficace se accompagnata dall' ausilio della banca dati del dna, ha portato i reparti di investigazione scientifica della polizia giudiziaria a creare archivi genetici non autorizzati. La realizzazione di tali banche dati, in assenza di una cornice normativa di riferimento, suscita perplessità, se si pensa agli standard di tutela del dato genetico ormai riconosciuti e ribaditi da diverse norme di carattere nazionale ed internazionale agli innumerevoli profili dei quali ha dovuto tener conto il legislatore nell'approntare la recente legge sull'implementazione delle banche dati ufficiali del dna nel nostro paese.

Quelle in uso presso i reparti speciali di polizia giudiziaria, oltre che operare in un regime di assoluta segretezza, fanno venir meno tutta una serie di garanzie – peraltro riconosciute in tutti i paesi occidentali dove le banche dati sono utilizzate e sottoposte a ferree prescrizioni regolamentari – di capitale importanza per i soggetti sottoposti al prelievo di materiale biologico[337]. Al momento si conoscono le banche dati istituite presso il R.IS di Parma, Messina, Cagliari e Roma. L'emersione di questa "pratica investigativa *borderline*" è avvenuta del tutto casualmente, in occasione di un indagine genetica svolta a carico di un soggetto effettuata dalla sezione del R.I.S. di Parma.

Il garante per la *privacy*, interpellato sulla regolarità della raccolta dati utilizzata per l'investigazione, ha dichiarato l'inammissibilità del ricorso presentato dall'indagato, sottolineando l'impossibilità di un intervento autoritario in prima persona, a causa del richiamo al combinato disposto degli artt. 8 e 145 del codice per la *privacy* in virtù dei quali non può essere attivato lo strumento del ricorso al garante "se i trattamenti di dati personali sono effettuati per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado "[338]. Nello specifico bisogna far cenno al fatto che il profilo genetico del soggetto era stato catalogato

[337] 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, Vulicevic, in *Ced 235969*

[338] Bollettino n. 77 del 30 novembre 2006, in *www.garanteprivacy.it*.

nonostante il procedimento si fosse concluso con un provvedimento di archiviazione. Tale notazione non appare di poco conto se si pensa al fatto che la banca dati inglese è stata recentemente dichiarata contraria all' art. 8 della Convenzione europea dei diritti dell'uomo, proprio perché non prevede la cancellazione del profilo genetico dell'indagato nel caso in cui un intervenga in suo favore una sentenza di proscioglimento[339]. Ad ogni modo l'autorità di garanzia ha disposto – all'esito della decisione di inammissibilità sul ricorso – un'indagine ispettiva conclusasi con l'indicazione di una serie di parametri ai quali le banche dati costituite presso i RIS di Parma, Messina, Cagliari e Roma devono uniformarsi[340].

Oltre all' impiego di archivi elettronici, la polizia giudiziaria ha avuto modo di sperimentare nel corso degli ultimi anni anche forme particolari di *screening* genetici, allo scopo di utilizzare le caratteristiche peculiari della molecola del dna, per trarne informazioni utili alle indagini.

In particolare, l'ereditarietà del dna umano[341], ha rappresentato il presupposto oggettivo della ricerca di un soggetto sospettato della commissione di un reato di omicidio avvenuto nella cittadina alto atesina di Dobbiaco. In questo caso singolare gli investigatori hanno creato un *database* genetico interno al paese, a contribuzione volontaria, partendo dal fondato sospetto che il colpevole del reato potesse nascondersi tra gli abitanti di sesso maschile della stessa cittadina e facendo leva proprio sul livello di consonanza tra le diverse molecole del dna appartenenti a soggetti legati tra loro da un vincolo di parentela .

Il grado di affinità del dna dei parenti del sospettato – ignari di aver consegnato ai magistrati la prova della colpevolezza – rispetto al reperto individuato dagli investigatori sulla scena del crimine, ha indirizzato l'indagine verso un soggetto determinato, il quale, chiamato a render conto dei riscontri

[339] Corte Eur. dei diritti dell'uomo, S. and Marper v Regno Unito, cit. .

[340] Le misure prescritte dal garante e adottate recentemente dal Ris per la messa in sicurezza dei dati sono particolarmente rigorose. Tra le principali figurano l'obbligo di conservare la 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. Comunicato stampa – 25 maggio 2009, in *www.garanteprivacy.it*.

[341] vedi cap. I, par. 3

investigativi, ha in breve tempo confessato la propria responsabilità in relazione alla commissione del reato[342].

A parere di chi scrive, il *modus operandi* scelto dagli inquirenti per la risoluzione di questo caso specifico, lascia qualche dubbio sulla legittimità dell'intera operazione. Invero, occorre segnalare come l'atto volontario di contribuzione del materiale genetico posto in essere dai cittadini di Dobbiaco, che in modo del tutto intenzionale hanno concesso il proprio dna agli inquirenti, non sia di per sé sufficiente a coprire il rischio di un eventuale coinvolgimento di un parente in un indagine penale.

In termini più generali, va segnalato come l'assenza di norme di riferimento dalle quali trarre indicazioni positive da utilizzare nella circostanza in cui nel corso delle indagini si presenti la necessità di operare *screening* genetici come quello attuato per il caso Dobbiaco, dovrebbe spingere gli investigatori a comunicare in modo chiaro a coloro che in maniera spontanea prestano la propria collaborazione alle indagini, che la concessione volontaria di materiale biologico da sottoporre ad analisi genetica potrebbe coinvolgere indirettamente nelle indagini altri soggetti a questi legati da un vincolo di parentela; tale circostanza, viene allineata da alcuni autori alla garanzia riconosciuta nel codice di rito ai testimoni prossimi congiunti prevista dall'art. 199[343]. In tal modo si genererebbe una specie di consenso informato all'uso del dato genetico legato a tutte le possibili implicazioni e conseguenza che l'indagine può produrre. Invero nel caso di Dobbiaco l'idea dello *screening* di massa di fatto è nata dalla ragionevole certezza che il sospettato della commissione del reato appartenesse alla comunità dobbiachese; come dire che l'attività d'indagine è stata concepita *ab initio* come una investigazione generale su un intero paese di potenziali colpevoli.

Un'ulteriore caratteristica della molecola del dna che negli ultimi anni è stata sfruttata nel nostro paese come parametro investigativo nella soluzione di indagini per particolari reati, è l'analisi sul cromosoma Y. Quest'ultimo infatti costituisce un dato caratteristico della molecola del dna in quanto viene trasmesso di padre in figlio in tutta la progenie maschile. L'isolamento di tale cromosoma rappresenta una modalità d'indagine particolarmente efficace nei casi di violenza sessuale, utilissima per l'individuazione delle tracce biologiche di genere

[342] GAROFANO, *Delitti imperfetti II*, Milano, 2007, 167.
[343] GENNARI, *Identità genetica e diritti della persona*, in *Riv. crit. dir. priv*., 2005, 633.

maschile, in quei casi specifici in cui i reperti della vittima di sesso femminile e quelli appartenenti all'aggressore si presentino uniti, e quindi difficili da esaminare. In situazioni siffatte il profilo genetico ricavato dall'isolamento cromosoma Y rappresenta il dato identificativo del soggetto da ricercare[344].

In ultima analisi occorre sottolineare come l'idea stessa di banca dati risponda, per ovvie ragioni, legate essenzialmente alle caratteristiche strutturali di questo strumento, alle necessità proprie di forme di indagine quali le analisi genetiche sul cromosoma Y, o sulle affinità parentali della molecola del dna; nel senso che per l'attuazione di queste ultime, l'analisi di un numero elevato di informazione genetiche costituisce una condizione necessaria, essenziale per la loro riuscita.

4) ***La tutela del dato genetico nella normativa internazionale***

La continua progressione delle scoperte nel campo delle biotecnologie, ha generato un intenso dibattito sull'individuazione dei limiti normativi che dovrebbero condizionare le attività legate al trattamento del dna umano. Tale quesito costituisce la *ratio* di molte disposizioni internazionali, che nel corso degli anni hanno cercato di fornire *standard* generali di tutela dei diritti della persona rispetto alle applicazioni della biomedicina.

Fra i testi più importanti va ricordata la Convenzione di Oviedo, promossa dal Consiglio d'Europa ed aperta alla firma ad Oviedo il 4 aprile 1997[345].

Tale Convenzione, spesso ricordata in dottrina per l'importanza del suo protocollo addizionale sul divieto di clonazione di esseri umani, reca al suo interno un intero capitolo dedicato alla definizione e protezione del genoma umano[346]. Questo capitolo costituisce una punto rilevantissimo della Convenzione *de qua* perché contiene l'affermazione di un principio di carattere generale, in base al quale viene dichiarata la preminenza dell'essere umano in quanto tale rispetto all'interesse della società e della scienza. Nel solco di questa previsione,

[344] POLI, *Biotecnologie*, cit., 47.
[345] "*Convention for the protection of Human Rights and dignity of the human being with regard to the application of biology and medicine*", in www.idi.it/ric/ce/oviedo .
[346] SCAFFARDI, *Le banche dati genetiche personali*, cit., 14.

qualsiasi individuo che si sottoponga a *test* genetici dovrà fornire un consenso libero e informato, riconoscendo così il carattere riservato proprio di questo tipo di indagini. Inoltre, particolare rilievo va attribuito all'indicazione contenuta nella Convenzione riguardo ai diritti fondamentali della persona "da rispettare in ogni caso", non sottoponibili cioè ad alcun tipo di limitazione. In base alla previsione dell'articolo 11, il patrimonio genetico di un soggetto può subire forme di trattamento di vario genere purché non si rivelino come un mezzo per porre in essere attività discriminatorie " è vietata qualsiasi tipo di discriminazione di una persona a causa del suo patrimonio genetico". Nello stesso senso l'art. 13 vieta espressamente interventi diretti sul genoma umano con l'eccezione di "finalità preventive, diagnostiche o terapeutiche, e solo se non tende a introdurre modifiche nel genoma dei discendenti"[347].

Nel 2004 è stato aperto alla firma il protocollo aggiuntivo alla Convenzione di Oviedo[348] , che ha per oggetto la protezione dell'essere umano nella sua dignità e identità e che contiene indicazioni rivolte alla possibile maggior tutela dell'integrità e dei diritti fondamentali con riguardo ad ogni futura ricerca biomedica che preveda un intervento sulla persona.

Segue la linea dell'individuazione dei principi etici e giuridici che devono emergere nelle diverse applicazioni pratiche della ricerca genetica, anche la Dichiarazione universale del genoma umano e sui diritti umani[349]. Le questioni trattate dalla Dichiarazione *de qua* possono essere raggruppate in quattro differenti aree riconducibili ai temi della dignità umana, della libertà di ricerca, della solidarietà tra esseri umani e della cooperazione internazionale. In particolare vengono considerati come dei limiti per le attività rivolte al trattamento e all'uso del genoma umano: il principio della non discriminazione in base alle caratteristiche genetiche soggettive, la necessità del consenso libero e informato di ogni individuo sui propri dati genetici, la garanzia della riservatezza nell'uso di tali dati. In termini più generali viene affermata la possibilità di

[347] PENASA, *Alla ricerca dell'anello mancante: il deposito dello strumento di ratifica della Convenzione di Oviedo*, in *www.forumcostituzionale.it* .

[348] Additional protocol to the Convention on human rights and biomedicine concerning biomedical research, in *www.idi.it/ric/ce/oviedo* .

[349]La dichiarazione universale del genoma umano e sui diritti umani è stata adottata dalla Conferenza generale dell'Unesco durante la sua ventinovesima sessione dell'11 novembre 1997 ed approvata dall'Assemblea generale dell'Onu il successivo 9 dicembre 1998; Dichiarazione universale del genoma umano e sui diritti umani, in *www.unesco.org* .

limitare il diritto alla *privacy* genetica, che può avvenire solo per legge ed in base a particolari necessità, nei limiti del diritto internazionale e delle convenzioni internazionali sui diritti umani.

Il Consiglio d'Europa ha emanato nel corso degli anni diverse raccomandazioni che, pur non avendo valore vincolante, hanno segnato un crescente interesse verso la specifica tematica del rapporto tra indagini giudiziarie e trattamento dei dati personali. In particolare nel 1987 venne approvata la prima raccomandazione, R(87) 15 sull'uso dei dati personali nelle indagini di polizia, nella quale si stabilisce che la conservazione dei dati personali deve essere limitata ai soli casi in cui questa risulti necessaria per la prevenzione di specifici reati di particolare gravità o allarme sociale[350]. Ancora più importante nell'ottica del discorso affrontato nel presente capitolo è la raccomandazione R(92) 1 adottata dal Consiglio d'Europa il 10 febbraio del 1992, sull'uso del dna per fini giudiziari. Con tale provvedimento si è inteso fornire una serie di principi generali riconducibili al tema dell'indagine genetica forense, posta in essere con l'ausilio di banche dati automatizzate di raccolta dei profili genetici identificativi, attraverso l'indicazione di una serie di specifici parametri[351].

Allo stesso modo la successiva Raccomandazione R (97) 5 relativa alla protezione dei dati sanitari (compresi quelli genetici) specifica criteri di particolare utilità che devono essere rispettati nella raccolta e nel trattamento dei dati di carattere sanitario, sempre da attuarsi nel "rispetto dei diritti e delle libertà fondamentali, in particolare il diritto alla vita privata". Costituisce uno spunto particolarmente interessante la chiara definizione contenuta nel provvedimento rispetto al significato delle parole "dato genetico" , "informazione genetica", e "linea genetica". La raccomandazione si sofferma sui criteri da seguire nell'uso dei dati genetici raccolti e trattati, indicando come questi dovranno essere utilizzati a soli fini di prevenzione, diagnostici o terapeutici dell'individuo sottoposto a prelievo. Lo specifico trattamento nell'ambito di un procedimento

[350] Il documento individua una lunga serie di adempimenti che ogni stato membro dovrebbe attuare per il trattamento dei dati individuali relativi al settore delle indagini di polizia, così da scongiurare eventuali abusi nei confronti della vita privata dell'individuo. Cfr. testo integrale della Raccomandazione R(87) 15, in *www.coe.int* .

[351] La raccomandazione individua in particolare: l'individuazione dei laboratori legittimati ad operare le analisi, il grado di protezione minimo da garantire a cura degli stessi, il rispetto degli individui sottoposti ad analisi genetica. Raccomandazione R(92) 1, in *www.coe.int* .

giudiziario o di un procedimento penale dovrà essere oggetto di una legge distinta che offra garanzie appropriate. I dati dovranno servire esclusivamente a verificare l'esistenza di un collegamento genetico ai fini della raccolta delle prove della prevenzione di un concreto pericolo o della repressione di una specifica infrazione penale. In nessun caso essi dovranno essere usati per individuare altre informazioni che possano essere collegate geneticamente[352].

Tratta lo specifico tema della tutela del dato genetico – seppur di riflesso e non attraverso previsioni dirette – anche la Direttiva 95/46 CE[353] sulla protezione dei dati personali. Invero l'art. 8 di questa importante direttiva inserisce i dati sulla salute fra le informazioni che richiedono precauzioni particolari rispetto alle normali cautele che circondano l'impiego dei dati relativi alla sfera della persona. Il succitato articolo non fa riferimento ai dati genetici, questi tuttavia potrebbero comunque raffigurarsi come rientranti nell'alveo dei dati sulla salute, poiché forniscono informazioni sulle caratteristiche fisiognomiche e sullo stato di salute presente ed in certi casi anche su quello futuro dell'individuo. Pare importante sottolineare che la direttiva afferma il principio di proporzionalità come criterio cardine per le attività legate all'archiviazione dei dati personali, tale per cui l'utilizzo degli stessi può essere concepito solo a seguito di una valutazione dell'adeguatezza, della pertinenza e della non eccessività nel trattamento rispetto allo scopo per cui sono stati raccolti[354].

In maniera ancora più specifica, il Consiglio dell'Unione Europea, tenendo conto dell'importanza dell'analisi del dna nelle indagini di polizia criminale e del possibile scambio dei risultati di tali analisi quale contributo per migliorare la loro efficienza, ha invitato gli stati membri a fissare criteri uniformi per la costituzione di banche dati nazionali relative al dna, in modo tale da costruire un sistema di banche dati uniformi, cioè di possibile e compatibile lettura. Vista l'importanza delle informazioni scambiate, queste dovranno essere limitate alle parti non codificanti del dna. Invero la catalogazione genetica per finalità giudiziarie deve tendere ad uniformarsi in tutti gli stati dell'U.E., per tale motivo la selezione dei marcatori da utilizzare per l'inserimento nella relativa banca dati dovrà essere uguale per tutti i paesi membri. Quello che, invero, rimane nella piena determinazione degli stati attiene alla tipologia dei reati per cui è possibile

[352] Raccomandazione R (97) 5, in *www.coe.int* .
[353] Vedi cap. II, par. 3.3.
[354] STEFANINI, *Dati genetici e diritti fondamentali,* cit., 18.

avvalersi di tali analisi. Questa di fatto rappresenta l'impostazione della recente decisione quadro 2008/615/GAI adottata dal Consiglio, e relativa all'implementazione dei contenuti del Trattato di Prum nel diritto dell'Unione Europea[355]. Peraltro gli stessi concetti sono ribaditi in precedenza nella Carta Europea dei diritti fondamentali c.d. Carta di Nizza, inserita recentemente quale protocollo aggiuntivo al Trattato di Lisbona[356].

In ultima analisi va rilevato come il dna sia un dato molto particolare che rivela informazioni relative non solo alla persona, ma anche ai suoi familiari, e proprio per queste caratteristiche numerosi sono i problemi etici e giuridici legati alla creazione di database genetici e al trattamento dei dati in essi inseriti. In primo luogo, occorre considerare gli interessi dei soggetti i cui campioni biologici sono raccolti dal momento che l'analisi del dna, oltre ad identificare gli eventuali colpevoli di un reato, può anche rivelare legami parentali e genitoriali non richiesti, diagnosi di malattie genetiche o di predisposizione a queste con ricadute possibili in chiave negativa sia sull'individuo come sulle persone a lui prossime.

Tutto ciò comporta che la formazione di un database genetico a fini di indagini giudiziarie non può prescindere dalla creazione di un corretto bilanciamento fra gli interessi legati a condotte invasive e discriminatorie nei confronti della riservatezza e la dignità delle persone[357].

4.1) ***Lo schema istitutivo previsto dal Trattato di Prum per il database statale dei profili genetici***

La cooperazione interstatale attuata attraverso lo scambio di informazioni personali, utili per lo svolgimento delle indagini forensi, rappresenta un tratto caratteristico dello spazio comune europeo in ambito giudiziario. A tal proposito

[355] Vedi par. 4.1.

[356] L'art. 8 della Carta di Nizza dispone dettagliatamente come ogni individuo abbia il diritto alla protezione dei dati di carattere personale e come questi debbano essere trattati secondo il principio di lealtà e per finalità determinate e comunque sempre a seguito del consenso informato della persona o in mancanza di questo attraverso modalità la cui legittimità si basi su di un disposto legislativo. Carta dei diritti fondamentali dell'Unione europea, proclamata a Nizza il 7.12.2000 , in *www.europarl.europa.eu/charter* .

[357] FANUELE, *Dati genetici e procedimento penale,* cit., 78.

l'attuazione di una piena collaborazione tra Stati, attraverso il passaggio di informazioni genetiche per le operazioni di *law enforcement* – previsto quale forma di sostegno investigativo transfrontaliero dal terzo paragrafo dell'accordo dell'Aia del 2004 [358]– costituisce un profilo importante da analizzare nell'ottica dell'indagine sull'archivio elettronico nazionale del dna. Tale considerazione assume maggiore importanza se si pensa al fatto che la recente introduzione della banca dati nel nostro paese costituisce il frutto della ratifica da parte dell'Italia degli impegni presi con la stipula del Trattato di Prum[359]. Invero, nonostante quest'ultimo costituisca a tutti gli effetti una fonte di diritto internazionale, non riconducibile al novero delle fonti normative caratteristiche dell'Unione Europea, può essere considerata come una sorta di "attuazione indiretta" della regola generale dell' *information scharing* nel solco di quanto stabilito dall'accordo dell' Aia[360].

Attraverso il Trattato, sette stati europei, nel 2005 hanno stabilito una particolare forma di collaborazione rivolta allo scambio diretto di informazioni personali – profili identificativi del dna, impronte digitali e targhe di autoveicoli – tra le autorità preposte all'attività di indagine giudiziaria dei singoli paesi[361]. In particolare tale accordo realizza una forma di collaborazione ad un livello superiore rispetto ai modelli di "cooperazione informativa" [362] che in precedenza avevano caratterizzato la creazione delle banche dati in ambito europeo, come quelle previste da Eurodat, SIS, ed Eurojust[363].

---

[358] Programma dell'Aia: rafforzamento della libertà, della sicurezza e della giustizia nell'Unione Europea, in *G.U.U.E.*, 3 marzo 2005, C 53, 1.

[359] MARANDOLA, Information sharing *nella prospettiva del Trattato di prum e della decisione di recepimento nel quadro giuridico dell'Unione,* in *Cooperazione informativa e giustizia penale nell'Unione europea*, cit. , 164.

[360] La progressione normativa frutto dell'attuazione diretta del programma dell'Aia da parte del Consiglio si sostanzia nelle due Decisioni Quadro 2006/960/GAI e la 2008/977/GAI, che danno corso ai punti cardinali del programma stesso. La prima in particolare riguarda la semplificazione dello scambio di informazioni e *intelligence* tra le autorità degli stati membri dell' Unione europea incaricate dell' applicazione della legge, la secondala protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale.

[361] GANDINI, *Il Trattato di Prum articolo per articolo*, cit., 60.

[362] "Il Consiglio europeo è convinto che il rafforzamento della libertà, della sicurezza e della giustizia richieda un approccio innovativo nei confronti dello scambio transfontaliero di informazioni in materia di applicazione della legge. Il fatto che le informazioni attraversino le frontiere non dovrebbe essere più rilevante". Par. 2, art. 2.1, del Programma dell' Aia, cit. .

[363] "Questi strumenti catalizzano le informazioni provenienti dagli Stati membri convogliandole all'interno di una banca dati centrale che può essere compulsata, a

Ciò che contraddistingue il Trattato è la possibilità di un rapporto diretto di interscambio di dati tra gli Stati aderenti, in base al quale ogni singolo firmatario – per il tramite di una autorità governativa preposta all' intervento – potrà consultare direttamente i repertori informativi messi a disposizione dagli altri Stati. L'evoluzione rispetto al passato risiede proprio in questa caratteristica. Occorre segnalare inoltre come le parti del Trattato di Prum aventi ad oggetto lo scambio di informazioni, sono state inserite in una decisione quadro del consiglio, che estende, a tutti gli stati dell'U.E., tanto l'obbligo di collaborazione diretta, così come previsto dallo spirito originario del trattato, quanto la materiale istituzione di una banca dati del dna, quale fonte di riferimento informativo[364].

I parametri europei tracciati dal trattato – riportati dalle successive pronunce del consiglio d'Europa – sono rivolti alla determinazione delle linee direttive per l'attuazione della collaborazione dinamica interstatale nell'ottica dello scambio d'informazioni genetiche. Il contenuto dell' accordo nulla dice sulla disciplina della biobanca intesa come contenitore delle informazioni raccolte nei singoli stati[365]. Va evidenziato come la parte del Trattato di Prum, dedicata alla

---

richiesta, dalle autorità competenti dei singoli Stati. Il meccanismo operativo è caratterizzato da un sistema "a stella": il dato viene immesso da parte di un'autorità nazionale e, transitando per mezzo di una unità centrale di supporto tecnico, viene reso disponibile alle autorità degli altri paesi. L'unità centrale non rielabora il dato, ma si limita a renderlo identico,e, dunque, disponibile per tutti gli utenti del sistema realizzando, per tale via, una forma di cooperazione "orizzontale" mediata". In tali banche dati il dato d'interesse comune viene trasportato dal singolo stato verso un punto di raccolta unico, che funge da connettore informativo, al quale tutti gli stati che hanno un interesse ad ottenere un certo tipo di informazioni si possono rivolgere. La differenza col *network* informativo creato dal trattato di prum è sostanziale, visto che in tal caso è previsto un collegamento diretto tra gli Stati che richiedono la notizia e quelli che la detengono. DECLI – MARANDO, *Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia*, cit., 103.

[364] Decisione quadro 2008/615/GAI del Consiglio sul potenziamento della cooperazione transfontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfontaliera, in *G.U.U.E.*, 10 agosto 2008, L 210, 1.

[365] Per quanto riguarda quest' ultimo aspetto, una descrizione piuttosto dettagliata delle specifiche tecniche sulle banche dati del dna sono confluite nella decisione quadro 2008/616/GAI del consiglio d' Europa, che fissa una serie di parametri indicativi sulla omogeneità del dato da inserire nei singoli archivi elettronici – profilo alfa numerico del dna non codificante relativo alle zone altamente polimorfiche denominate STR – , a tal proposito, gli stati membri hanno il dovere di far riferimento alle indicazioni operative contenute nella decisione, visto e considerato come una collaborazione fattiva nell'ottica del principio di *information scharing* in ambito giudiziario, non può prescindere da un dato genetico uniforme in tutti i paesi.

banca dati del dna, non faccia alcun cenno alle prescrizioni minime sulla determinazione del contenuto del *database* – inteso come individuazione dei soggetti colpevoli, indiziati o solo sospettati di aver commesso determinati reati dai quali prelevare e catalogare il profilo identificativo del dna – che sarà cura del singolo stato, il quale potrà articolare l'archiviazione in base a scelte e valutazioni politiche interne ad esso.

Per quanto riguarda lo scambio di informazioni legate alle impronte digitali e alle targhe di autoveicoli, il trattato fa riferimento a delle banche dati già esistenti, fotografando una situazione oggettivamente differente da quella presa in considerazione per le banche dati del dna. In quest' ultimo caso si parla di realizzazione, negli altri della creazione di un *network* tra *database* già utilizzati e operanti nei singoli stati.

Peraltro, in relazione alla circolazione dei dati da uno stato all'altro previste dalle norme del trattato, l'identità del soggetto sottoposto ad indagine genetica attraverso la banca dati del dna, potrà essere richiesta, allo stato che detiene il dato nel proprio *database*, solo in seguito ad una eventuale riscontro positivo. In quest'ottica la garanzia dell'anonimato assoluto del profilo identificativo fornito o ricevuto, costituisce una precauzione importante nella collaborazione investigativa tra stati. Invero le notizie contenute nell'archivio, consultabile da ogni singolo stato appartenente al *network* interstatale delle banche dati del dna, dovranno riprodurre solo la successione alfanumerica identificativa indispensabile per il confronto genetico. Inoltre la collaborazione impone la contestuale individuazione degli organi – punti di contatto – legittimati a tessere questo tipo di rapporto a livello statale.

5) ***La banca dati del dna nella legge 30 giugno 2009 n.85***

Il disegno di legge originario sull'istituzione della banca dati nazionale del dna, presentato al parlamento con lo scopo di ratificare la partecipazione del nostro paese al Trattato di Prum, risale al 2007, tale proposta di adesione è stata assorbita nella recentissima legge 30 giugno 2009 n.85, che oltre alla disciplina

organica della banca dati, reca – come appena visto[366] – anche una serie di modifiche al codice di procedura penale sui casi e i modi in cui può essere limitata la libertà personale di un soggetto in occasione di una perizia.

La legge *de qua* ha raccolto le indicazioni, provenienti dal mondo scientifico, sulla necessità di operare – contestualmente all'introduzione della banca dati del dna nel nostro paese – una modifica del codice di rito nel solco di quanto previsto dalla Corte costituzionale con la sentenza n. 238 del 1996. In tal senso, assume particolare rilevanza l' implementazione nel codice di rito degli artt. 224 - *bis* e 359 - *bis*, che consentono all'autorità giudiziaria la possibilità di svolgere prelievi coattivi di materiale biologico ogniqualvolta la situazione oggettiva lo richieda

Operando questa ricostruzione, la legge n. 85 del 2009 pare aver colto il significato della complementarietà tra le varie operazioni di raccolta e successiva comparazione del dato genetico, considerato come – in termini generali – la realizzabilità di un confronto ha come presupposto logico che si ragioni come minimo in termini di dualità.

Invero, occorre far notare come l'esclusiva catalogazione dei profili genetici in un *database* nazionale, risulterebbe fine a se stessa, se l'autorità giudiziaria non potesse recuperare coattivamente il dna da comparare dal soggetto sottoposto a procedimento penale. Allo stesso modo se si consentisse unicamente l'apprensione forzosa delle sostanze da analizzare attraverso la previsione dei casi e dei modi in cui questa può essere attuata – senza l'implementazione di una banca dati nazionale –, il campione biologico potrebbe essere utilizzato solo per gli accertamenti tecnici interni alle indagini, ma non per i controlli ad ampio raggio effettuabili con l'ausilio dell'archivio elettronico del dna, con un conseguente depotenziamento dell'attività di *intelligence* nel suo complesso.

In quest'ottica si può cogliere il senso dell' accorpamento sostanziale effettuato dalla legge *de qua*, volto essenzialmente alla creazione di un equilibrio tra i due elementi costitutivi dell'attività di riscontro posta in essere dagli investigatori: *id est* la ricerca di una corrispondenza tra il profilo genetico rinvenuto su una scena del crimine e quello del soggetto sospettato di aver commesso un reato.

[366] Vedi il paragrafo precedente.

Come accennato, il legislatore nella strutturazione della banca dati del dna, ha dovuto tener conto di una serie di parametri di garanzia fissati dal Trattato di Prum. I riferimenti ai punti essenziali dell'accordo internazionale costituiscono l'asse portante della sezione della legge dedicata all'implementazione della banca dati dei profili genetici del dna nel nostro paese. In particolare negli articoli dedicati all'istituzione delle autorità deputate alla conservazione e al trattamento del dato genetico, alla tipizzazione del profilo – da eseguire sulla base dei parametri riconosciuti a livello internazionale e indicati dall' *European Network of Forensic Science* in modo da assicurare l'uniformità degli stessi a livello europeo[367] –, alle disposizioni relative alla metodologia di analisi dei reperti biologici.

Il conferimento dei profili genetici nell'archivio elettronico avviene in due modi distinti, vale a dire attraverso una modalità di carattere statico e una di tipo dinamico. Ci si riferisce alla prima in tutti quei casi in cui la possibilità di un prelievo automatico del campione biologico, con successiva tipizzazione del profilo individuale, avvenga qualora si verifichi una delle situazioni soggettive richiamate dall'art 9 della norma, e nel rispetto delle eccezioni da essa indicate[368] ; oppure di profili genetici appartenenti a persone scomparse o loro consanguinei, di cadaveri e resti cadaverici non identificati. In tali casi, la repertazione del materiale biologico e la successiva tipizzazione del profilo genetico, vengono fatti in un unico laboratorio nazionale, istituito presso il ministero della giustizia, il c.d. laboratorio centrale del dna. Questa struttura si occuperà della trasmissione del profilo identificativo alla banca dati nazionale, istituita presso il ministero degli interni – dipartimento di pubblica sicurezza – e curerà la conservazione del materiale biologico utilizzato per determinare il dato che materialmente verrà inserito nell'archivio statale.

[367] Vedi nota 285.

[368] Ai fini dell'inserimento del profilo del dna nella banca dati nazionale, sono sottoposti a prelievo di campioni biologici: i soggetti ai quali sia applicata la misura della custodia cautelare in carcere o quella degli arresti domiciliari, i soggetti arrestati in flagranza di reato o sottoposti a fermo di indiziato di delitto, i soggetti detenuti o internati a seguito di sentenza irrevocabile per un delitto colposo, i soggetti nei confronti dei quali sia applicata una misura alternativa alla detenzione a seguito di sentenza irrevocabile per un delitto non colposo, i soggetti ai quali sia applicata in via provvisoria o definitiva una misura di sicurezza detentiva. Il prelievo può essere effettuato solo se si procede nei confronti di delitti non colposi per i quali è consentito l'arresto facoltativo in flagranza. Nel caso di arresto in flagranza di reato o di fermo di indiziato di delitto, il prelievo è effettuato dopo la convalida da parte del giudice. Vedi par. 5.1.

Il profilo identificativo del dna può convergere alla banca dati nazionale anche dalla tipizzazione del dna raccolto nel corso dello svolgimento delle indagini da parte di ausiliari tecnici dell'autorità giudiziaria o delle forze di polizia: modalità "dinamica" . Invero l'art. 10 della norma afferma che "se nel corso del procedimento penale […] sono tipizzati profili del dna da reperti biologici a mezzo di accertamento tecnico, consulenza tecnica o perizia, l'autorità giudiziaria procedente dispone la trasmissione degli stessi dati alla banca dati nazionale del dna, per la raccolta e i confronti". Il fatto che l'articolo *de quo* non faccia alcun riferimento particolare ai reperti rinvenuti sulla scena del crimine, lascia pensare ad un disegno onnicomprensivo del legislatore tale per cui il riferimento ai reperti e da intendere come relativo ad ogni ritrovamento di materiale biologico fatto nel corso del procedimento penale.

In tali situazioni il laboratorio che effettua l'estrazione del profilo identificativo conferisce direttamente il dato alla banca dati nazionale e si occupa del trasferimento del materiale biologico al laboratorio centrale istituito presso il ministero della giustizia per la conservazione del dna utilizzato per le operazioni di tipizzazione . Invero, va rimarcato come la banca dati raccoglie al suo interno solo ed esclusivamente i profili identificativi soggettivi, asportati dal dna di un soggetto, mentre il materiale biologico utilizzato, viene conservato in un luogo differenti, il laboratorio centrale del dna, ed è soggetto a cautele e protezioni diverse rispetto al dato contenuto nell'archivio nazionale.

In linea con quanto indicato dalle norme sovranazionali la legge stabilisce l'utilizzo di informazioni genetiche c.d. non codificanti, da impiegare nella catalogazione genetica, ed una serie di certificazioni – a norma ISO/IEC – necessarie per tutti quei laboratori che concretamente potrebbero conferire profili del dna tipizzati da campioni biologici nel corso del procedimento penale. Con questa previsione la norma ha di fatto creato i presupposti per un allargamento potenziale dei soggetti legittimati al conferimento del dato genetico. Una scelta, quella fatta dal legislatore, sicuramente apprezzabile visto la mole di dati con i quali ci si dovrà confrontare nella pratica. Tuttavia, ciò non esclude in assoluto la possibilità per i laboratori scientifici della polizia giudiziaria, che attualmente svolgono le attività di carattere scientifico sui campioni biologici – purché rientranti nei parametri fissati dalla legge – di continuare con le operazioni

tecniche di estrazione del dna per il quale fino ad oggi hanno avuto una sorta di tacita esclusiva.

D'altra parte va sottolineato come la *ratio* della legge sia quella di operare una divisione dei ruoli delle autorità chiamate a eseguire l'identificazione genetica, nell'ottica di una maggiore specializzazione possibile nelle azioni esercitate da ciascuna di queste. Seguendo questa linea esegetica, nella successione di attività che conducono alla creazione del profilo da inserire nella banca dati, si ritiene che alla polizia giudiziaria rimanga la competenza delle operazioni di prelievo – sulla scena del crimine o sul sospettato di un reato – del materiale biologico; viceversa tutta l'attività di analisi, elaborazione e inserimento nel *database*, dovrebbe aver luogo presso laboratori specializzati, assolutamente indipendenti rispetto alle forze dell'ordine, e certificati per questo tipo di attività. In tal modo si eviterebbe la detenzione di tutte le informazioni da parte di un unico soggetto, dando corso a quello che, come detto, pare l'obiettivo principale perseguito dalla legge.

Peraltro, la necessaria "scomposizione" dell'indagine genetica risponde ad una serie di cautele doverose allorquando si operano delle analisi sul materiale biologico di un soggetto, in particolare, per evitare che rimangano a disposizione delle autorità di pubblica sicurezza una serie di notizie ricavabili dal materiale biologico. Tali informazioni, assolutamente inutili rispetto alle attività di identificazione *tout court*, rappresentano un dato delicato ed importante, in quanto portatore di notizie "sensibili" sulle caratteristiche fenotipiche della persona.

Inoltre occorre ridurre il rischio che tutta la serie di passaggi ai quali è sottoposto il dna produca un inquinamento dello stesso, con conseguente pregiudizio per tutta l'attività investigativa. Fin dal momento del suo prelievo, infatti, il campione biologico è soggetto a fenomeni di alterazione o deterioramento nel caso in cui non venissero applicati tutti gli accorgimenti necessari. Per questo motivo è indispensabile innalzare il livello di preparazione di tutti quei soggetti che vengono coinvolti nelle varie attività di cui si compone l'indagine genetica e richiedere il massimo grado di attenzione nella fase più delicata: quella della determinazione del profilo genetico. Va pure sottolineato come questa forma di articolazione dell'attività di *intelligence* – tra gli organi istituzionalmente preposti all'investigazione e laboratori certificati autorizzati – sia attuata con successo in molti paesi europei.

Nulla quaestio al contrario per quanto riguarda l'attività legata al confronto dei profili genetici, operazione questa di competenza esclusiva dell'organo preposto allo svolgimento delle indagini, e peraltro, affermata in modo chiaro e inequivocabile anche dalla stessa legge che nel secondo comma dell'articolo 12, prevede una esclusiva d'accesso ai dati contenuti nella banca dati appannaggio della polizia[369] e dell'autorità giudiziaria[370]. Peraltro, risulta diversificata la procedura di accesso alla banca dati dei profili identificativi, rispetto a quella prevista per il laboratorio centrale di analisi dei campioni biologici. Nel primo caso infatti, sia la polizia giudiziaria che pubblico ministero, possono effettuare direttamente una consultazione dei profili solo a fini di identificazione personale o per finalità legate alla collaborazione internazionale di polizia; per contro l'accesso al laboratorio centrale presuppone una specifica autorizzazione concessa dall'autorità giudiziaria che potrà essere rilasciata, alla polizia giudiziaria o al pubblico ministero, per le stesse finalità previste per la ricerca degli archivi contenuti nella banca dati dei profili[371]. L'utilizzo chiaramente seguirà le necessità emergenti nello svolgimento pratico delle

[369] Il riferimento generico alla polizia giudiziaria, dovrebbe essere interpretato alla luce dell'indicazione contenuta nell'art. 9 della legge n.121 del 1981, sulla possibilità di accesso ai dati archiviati nella banca dati del C.E.D. del ministero degli interni, vedi cap. III, par. 1.1. Così, 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 *Prelievo del DNA e banca dati nazionale*, cit., 113.

[370] In base al primo comma dell'art. 12 "i profili del DNA e i relativi campioni non contengono le informazioni che consentono l'identificazione diretta del soggetto cui sono riferiti". Tale norma sembra ricollegabile al principio di necessità stabilito dall'art. 3 del Testo unico sulla *privacy*, (vedi cap. III, par. 1), poiché, per la banca dati del dna è previsto un sistema di identificazione dell'interessato che può avvenire solo in situazioni particolari; *id est* nel caso in cui si rilevi una corrispondenza tra i dati genetici confrontati. 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, cit., 115.

[371] L'art. 12 contiene, altresì, l'indicazione delle regole sulla tracciabilità degli accessi ai dati contenuti nella banca dati nazionale e nel laboratorio centrale; a tal proposito il terzo comma prevede che le operazioni legate alla gestione e all'organizzazione dei dati avvengano in modo tale "da assicurare l'identificazione dell'operatore"; inoltre il comma 4 dell'articolo *de quo* limita la possibilità d'accesso "al personale espressamente autorizzato" che "è tenuto al segreto per gli atti, i dati e le informazioni di cui sia venuto a conoscenza a causa o nell'esercizio delle proprie funzioni". A ben vedere sembra che i cenni fatti dalla norma costituiscano solo la cornice di un problema che il legislatore dovrà regolamentare in dettaglio al più presto, dato che tutti gli aspetti tecnici legati all'attuazione di un "trattamento in sicurezza" (così come previsto dagli artt. 33 ss. del Testo unico sulla *privacy*), necessitano di un intervento particolare che tenga conto in concreto dei possibili rischi ai quali potrebbero essere esposti i dati contenuti nel DNA *database*. 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, cit., 123.

indagini[372] e potrà avere ad oggetto una comparazione di tipo "verticale", mirata cioè ad individuare nella banca dati la presenza del profilo identificativo dell'indagato; oppure una consultazione "orizzontale", tra profili identificativi tipizzati da reperti biologici individuati in diverse scene del crimine, allo scopo di creare un collegamento tra reati commessi in luoghi differenti.

A ben vedere, la legge *de qua* costituisce un compendio ben bilanciato di tutta una serie di osservazioni che negli anni si sono succedute in materia. Invero, hanno trovato spazio negli articoli del provvedimento le indicazioni del garante della *privacy*, in relazione ad alcuni punti che la stessa autorità aveva indicato come necessari per riequilibrare la situazione venutasi a creare dopo la scoperta di una banca dati genetica non autorizzata presso il RIS di Parma[373], oltre che le indicazioni del comitato nazionale sulla biosicurezza in merito all'istituzione delle autorità di garanzia[374], deputate alla realizzazione del controllo sul grado di funzionamento[375] e attuazione della legge nel tempo[376].

La legge, inoltre, prevede tempi differenti di conservazione per il materiale biologico e per il profilo identificativo. Il primo verrà custodito per un periodo massimo di venti anni dall'ultima circostanza che ne ha determinato il prelievo,

[372] Sembra che le attività di confronto col repertorio di informazioni genetiche contenute nella banca dati del dna possano aver luogo ogni qual volta le autorità inquirenti abbiano a disposizione il materiale biologico di un soggetto sospettato della commissione di un delitto perché repertato sulla scena del crimine, o prelevato in seguito alle svolgimento di una perizia o di un accertamento tecnico, o alle attività di identificazione previste dall'art. 349 comma 2- *bis*.

[373] Vedi, par. 3.3.

[374] L'art. 15 della legge n. 85 del 2009 stabilisce l'esercizio di un controllo diretto sulla banca dati nazionale del dna da parte dall'autorità garante per la *privacy*, oltreché indicare in capo al comitato nazionale per la biosicurezza, le biotecnologie e le scienze della vita, la conduzione del controllo scientifico sul laboratorio centrale che detiene il materiale biologico utilizzato per l'estrazione dei profili a livello nazionale, e sui 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".

[375] Il controllo esercitato dall'autorità garante per la *privacy* sulla banca dati del dna rientra nell'ambito dei c.d. particolari accertamenti previsti dall'art. 160 del Testo unico, per i trattamenti di dati personali effettuati in ambito giudiziario o dalle forze di polizia. Tale norma indica al primo comma le modalità che caratterizzano la verifica degli archivi di materiale genetico, che "viene effettuata per il tramite di un componente designato dal garante".

[376] *Comitato nazionale per la biosicurezza e le biotecnologie. Gruppo di lavoro Biosicurezza componenti ex DPCM 3 marzo 2004*, in RICCI – PREVIDERÈ – FATTORINI - CORRADI, *La prova del DNA per la ricerca della verità*, cit. , 578.

viceversa il mantenimento del profilo alfanumerico non potrà superare i quaranta anni dall'ultima circostanza che ne ha determinato l'inserimento[377].

In conclusione va sottolineato come la legge *de qua* preveda una cancellazione del profilo identificativo contenuto nella banca dati e della relativa distruzione del campione biologico nel caso in cui nel corso del procedimento intervenga una sentenza di proscioglimento nel merito, in linea con un recente orientamento giurisprudenziale espresso dalla Corte europea dei diritti dell'uomo[378]. Peraltro, la norma non fa alcun riferimento alle pronunce di non doversi procedere, a quelle che dichiarano l'estinzione del reato, alla sentenza di non luogo a procedere e al proscioglimento prima del dibattimento[379].

5.1) ***(segue) Un database "emergenziale"***

L'articolo 9 della legge sull'istituzione del *database* genetico, identifica i soggetti che dovranno subire il prelievo coattivo di materiale biologico, finalizzato alla tipizzazione del dato da inserire nell'archivio elettronico[380]. La norma *de qua* esclude inoltre, al secondo comma, che il prelievo possa essere effettuato quando si procede per alcune fattispecie di reato tassativamente elencate[381], tra le quali si ricordano quelle contro l'amministrazione della giustizia ovvero quelle previste nel codice civile o in materia tributaria.

---

[377] Si segnalano le perplessità di chi ritiene che qualora si verifichino nuove e non meglio precisate circostanze determinanti il prelievo del campione o l'inserimento del profilo, si sposterebbe in avanti il *dies a quo* del termine massimo di conservazione potendosi superare in concreto i quaranta e i venti anni previsti. Così, BUSIA, Privacy *a rischio per la durata della conservazione*, in *Guida dir.*, 2009, n. 30, 78.

[378] Corte Eur. dei diritti dell'uomo, S. and Marper v Regno Unito, cit .

[379] L'art. 13 prevede la cancellazione del profilo identificativo dalla banca dati e la distruzione del materiale biologico a seguito dell'identificazione di un cadavere o di resti cadaverici, nonché del ritrovamento di persona scomparsa. Costituisce una causa di eliminazione l'eventuale archiviazione del profilo fatta in modo illegittimo, senza tener conto dei parametri normativi fissati dall'art. 9 della stessa legge.

[380] Vedi paragrafo precedente

[381] Si tratta dei seguenti delitti: contro l'amministrazione della giustizia(ad eccezione di calunnia, false informazioni al pubblico ministero, false dichiarazioni al difensore, falsa testimonianza, frode processuale aggravata, favoreggiamento personale o reale); delitti contro l'autorità delle cose giudiziarie (ad eccezione della procurata inosservanza di pena); falsità in monete in carte di pubblico credito e in valori di bollo (tranne la falsificazione di denaro); falsità in sigilli; delitti contro l'economia pubblica (eccetto

Sulla scorta di queste precisazioni si può affermare come il neonato *database* italiano sia riconducibile al modello definito in dottrina come "emergenziale". In linea con le banche dati appartenenti a quest'ultimo *genus* , il legislatore nazionale ha limitato il prelievo dei campioni biologici e la conservazione dei profili identificativi di indiziati della commissione di un reato – oltre alla elencazione precisa delle singole fattispecie oggetto di catalogazione – ad una serie di rigidi parametri: *id est* il fatto che si tratti di soggetti ai quali sia stata applicata la misura della custodia cautelare in carcere o quella degli arresti domiciliari, di individui arrestati in flagranza o indiziati sottoposti a fermo.

In tali casi la catalogazione nel *database* avviene *ex lege,* al di là di qualsiasi considerazione legata allo sviluppo delle indagini e solo sulla base della riconducibilità sostanziale alle situazioni giuridiche indicate dall'art. 9 della stessa legge.

La norma *de quo* allinea le situazioni dell'indiziato limitato delle libertà personale in seguito al fermo, arresto in flagranza, o applicazione della custodia cautelare in carcere, a quelle dell' imputato detenuto o internato a seguito di sentenza irrevocabile per un delitto non colposo; nel senso che vengono tutte complessivamente indicate come circostanze idonee ad attivare l'autorità giudiziaria per le operazioni di prelievo del campione biologico e la tipizzazione del profilo del dna da inserire nel *database* genetico nazionale a scopo identificativo[382].

A tal proposito occorre sottolineare come l'indiziato nel corso del processo penale, vive una condizione in continua evoluzione, direttamente legata allo sviluppo progressivo della vicenda processuale che lo riguarda, e ai risultati che si ottengono nel corso di quest' ultima, secondo una logica diretta di causa effetto, tutta interna al procedimento in corso. Si pensi ad esempio alle situazioni richiamate dalla stessa lettera a) della norma *de qua* . L'applicazione di una misura cautelare coercitiva come la custodia cautelare in carcere o agli arresti domiciliari, risponde ad esigenze derivanti dal procedimento principale di

distruzione di materie prime, prodotti agricoli o industriali); delitti contro l'industria e il commercio (eccetto illecita concorrenza con minacce e violenza); delitti contro il matrimonio; reati fallimentari, reati societari, reati tributari, reati in materia di intermediazione finanziaria.

[382] FELICIONI, *L'acquisizione di materiale biologico a fini identificativi o di ricostruzione del fatto,* cit., 201.

riferimento, rappresenta pertanto un istituto accessorio e strumentale rispetto a quest'ultimo, legato all'emersione delle necessità richiamate dall'art. 274 c.p.p. . In quest'ottica il venir meno di tali esigenze nel corso del procedimento determina la revoca delle misure applicate – per contro l'aggravarsi della situazione oggettiva produce un inasprimento di queste – , in piena sintonia con la logica evolutiva fondata sull'idea che tutto possa cambiare, essere messo in discussione o confermato dagli eventi futuri.

Allo stesso modo l'arresto in flagranza e il fermo di indiziato, costituiscono la diretta conseguenza di alcune particolari situazioni di evidente pericolo oggettivo riscontrato in concreto nel corso del procedimento: *id est* la commissione di un determinato reato o il pericolo di fuga.

Idealmente il procedimento penale cessa di essere una concatenazione progressiva di eventi, positivi o negativi per un soggetto – indagato o imputato – solo nel momento in cui si arriva alla pronuncia di un provvedimento irrevocabile di proscioglimento o di condanna. Fintanto che non si giunga a tale conclusione la vicenda processuale, è soggetta ad una naturale evoluzione, condizionata dalle norme del codice di rito.

Lascia dunque, perplessi il fatto che gli inserimenti dei profili identificativi nella banca nazionale del dna nel corso delle indagini preliminari – nel caso in cui riguardi soggetti indiziati della commissione di un reato – si fondino sullo stesso presupposto oggettivo di quelli operati all'esito del procedimento penale, qualora questo si concluda con una sentenza di condanna irrevocabile. A tal proposito, l'obiettivo special preventivo richiamato per giustificare l'inclusione del dato genetico dell'indiziato nel *database* – per permettere, cioè, l'identificazione del soggetto sottoposto ad indagini nel caso in cui questi in futuro commetta ulteriori reati – non rispecchia in modo corretto la fase del procedimento nel quale interviene la catalogazione del dato.

Nel corso delle indagini, l'operazione di conservazione dell' informazione genetica dovrebbe essere considerata come un atto di carattere investigativo, fino al punto che la stessa opportunità, sull'introduzione della notizia nel *database* del dna, dovrebbe discendere da ragioni direttamente connesse allo svolgimento delle indagini, all'interno delle quali si è sviluppata l'attività di confronto tra profili identificativi. Invero le operazioni di raffronto del dna dell'indiziato costituiscono un mezzo per lo svolgimento delle indagini preliminari, attivabile quando una

circostanza oggettiva relativa a queste ultime lo richieda. In quest'ottica l'indagine genetica si realizza per la soluzione di un caso attraverso il confronto tra il dna dell'indiziato e quello in possesso dell'autorità giudiziaria repertato sulla scena del crimine, oppure tramite il raffronto ad ampio raggio attuato con i profili identificativi contenuti nella banca dati nella sezione relativa al materiale biologico rinvenuto su altri luoghi del delitto, c.d. *open record* .

Seguendo questa linea interpretativa si può valutare come, in situazioni siffatte, la conservazione del dato personale – effetto – dovrebbe avere come obiettivo primario la realizzazione dell'accertamento del fatto di reato – causa – e non essere un operazione di carattere automatico, legata, ad esempio, all'applicazione della custodia cautelare in carcere. Infatti l'attività di identificazione biologica, come rimarcato in precedenza, necessita di un fine per poter essere avviata, e deve essere equilibrata rispetto agli obiettivi che intende perseguire.

Per dar corpo alle considerazioni di carattere generale testé indicate, appare paradigmatica l'analisi di una situazione che in linea teorica si potrebbe verificare che rappresenta una situazione marginale, ma significativa, della criticabile – e criticata – impostazione delineata dall'art. 9.

Ipotizziamo il caso in cui un indagato per un reato rientrante tra quelli previsti dall'art. 9 comma 2 subisca – nel corso del procedimento – l'applicazione della custodia cautelare, e allo stesso tempo sia soggetto ad un indagine genetica non andata a buon fine tra il proprio profilo del dna e quelli detenuti all'autorità giudiziaria. In una circostanza di questo tipo occorrerebbe interrogarsi sull'opportunità di un possibile utilizzo alternativo del dato impiegato per l'indagine genetica, ovvero – alla luce della recente introduzione nel nostro ordinamento della banca dati del dna – sull'eventuale conservazione di quest'ultimo. Come visto in precedenza, stando alla lettera dell'art. 9, in una situazione siffatta, il profilo del soggetto indagato verrebbe inserito nel catalogo della banca dati nazionale, non considerando se questo sia necessario o meno per il compimento di un indagine genetica, ma per il solo avverarsi della condizione oggettiva richiesta dalla lett. a dell'art. 9: *id est* l'applicazione di una custodia cautelare.

In tale caso, è da ritenere che si debba eliminare il materiale biologico e cancellare il profilo tipizzato utilizzato per l'indagine identificativa infruttuosa.

Questo perché mantenere il dato genetico dell'indagato – a disposizione degli inquirenti – significherebbe proiettarne l'utilizzo oltre il naturale confine oggettivo interno alle indagini: vale a dire la verifica dell'effettiva corrispondenza tra il dna dell'indagato e quelli già detenuti dall'autorità giudiziaria.

Per contro l' eventuale inserimento del dato *de quo* in un *database,* – senza altro motivo se non la tutela della collettività da pericoli derivanti dall' aver commesso reati per i quali il soggetto allo stato degli atti è "solo" gravemente indiziato – realizzerebbe un indebita lesione della libertà personale dell'individuo, attraverso l'anticipazione ad una fase differente rispetto all'esito del dibattimento di una serie di valutazioni conseguenti all'accertamento dell'effettiva responsabilità penale dell'imputato. Occorre sottolineare infatti come, l'archiviazione del profilo identificativo dell'imputato condannato si fondi sulla logica del "mezzo deterrente" , e sia diretta alla creazione di uno strumento che permetta la facile individuazione del colpevole di un determinato reato nel caso di reiterazione di quest'ultimo.

Peraltro un analisi complessiva dei limiti individuati nei tre modelli di banche dati attualmente esistenti in Europa, porta a considerare come nessuno di questi colga il senso della collocazione procedimentale in cui si effettua l'indagine biologica sul soggetto sospettato. Invero, né l'assenza di barriere all'inserimento del dato genetico individuata come soluzione dalle banche dati del modello universale, né l'idea restrittiva del modello emergenziale – dove il confine è rappresentato dall' individuazione di fattispecie di reato predeterminate, e dal fatto che ci si riferisca a situazioni avallate dalla presenza di gravi indizi di colpevolezza – , né altresì la soluzione individuata dal modello intermedio, caratterizzata dalla valutazione prognostica del giudice sulla eventuale opportunità di catalogare il dato genetico del sospettato, rappresentano appieno il ruolo che dovrebbe svolgere la banca dati del dna nel corso delle fasi antecedenti alla definizione del processo. In tali situazioni la funzione dell'archivio genetico, come recettore d'informazioni, dovrebbe seguire al verificarsi di situazioni particolari, motivate dallo sviluppo delle indagini nel caso concreto.

Il fatto che ci si trovi, in un momento in cui non è stata formulata un imputazione a carico dell' indagato dovrebbe, ad avviso di chi scrive, spingere alla ricerca di soluzioni interpretative differenti da quelle fin qui proposte: se, infatti, pare del tutto apprezzabile lo slancio pragmatico di individuare stili di

catalogazione dei profili identificativi del dna legati al successo futuro delle indagini operabili con tale mezzo, questo non può, tuttavia, essere un parametro di valutazione da adottare, quantomeno nelle fasi antecedenti alla conclusione del procedimento.

BIBLIOGRAFIA

AA.VV., *Banche dati, telematica e diritti della persona*, Padova, 1984.

AA.VV., *Codice di procedura penale commentato*, a cura di GIARDA – SPANGHER, Milano, 2007.

AA.VV., *Commentario alla Costituzione. Principi fondamentali*, a cura di BRANCA, Bologna, 1975.

AA.VV., *Commento al nuovo codice di procedura penale*, a cura di CHIAVARIO, vol. II, Torino, 1989.

AA.VV., *Compendio di procedura penale*, IV ed., a cura di CONSO – GREVI, Padova, 2009.

AA.VV., *Cooperazione informativa e giustizia penale nell'Unione europea*, a cura di PERONI – GIALUTZ, Trieste, 2009.

AA.VV., *Il DNA nella società attuale: test genetici, disastri di massa, identificazione criminale*, a cura di CICOGNANI – PELOTTI, Milano, 2006.

AA.VV., *Il prelievo del DNA e banca dati nazionale*, a cura di SCARCELLA, Padova, 2009.

AA.VV., *La banca dati del DNA fra* privacy *e sicurezza*, a cura di INTINI, in *Gnosis rivista italiana di* intelligence, 2007, n.4.

AA.VV., *La tutela della riservatezza*, a cura di LOIODICE – SANTANIELLO, Padova, 2000.

AA.VV., Privacy *e banche dati*, Bologna, 1981.

AA.VV., *Profili del nuovo codice di procedura penale*, a cura di CONSO – GREVI, Padova, 1990.

AA.VV., *Protezione dei dati personali e accertamento penale, verso la creazione di un nuovo diritto fondamentale?*, a cura di NEGRI, Roma, 2007.

AA.VV., *Biochimica*, Bologna, 2003.

AA.VV., *Biologia molecolare della cellula*, Bologna, 2000.

AA.VV., *Diritto alla riservatezza e circolazione dei dati personali*, a cura di PARDOLESI, Milano, 2003.

AA.VV., *DNA: L'impronta che rivela*, in *Polizia moderna*, 2009, n.6, 10.

AA.VV., *La prova scientifica nel processo penale*, a cura di DE CATALDO NEUBURGER, Padova, 2007.

AA.VV., *La prova scientifica nel processo penale*, a cura di TONINI, in *Dir.pen. proc. dossier*, 2007.

AA.VV, *Le nuove norme di contrasto al terrorismo*, a cura di DALIA, Milano, 2006.

AA.VV., *Nuove tecnologie e processo penale, giustizia e scienza a confronto*, a cura di CHIAVARIO, Torino, 2006.

AA.VV., *Terrorismo internazionale: modifiche al sistema penale e nuovi strumenti di prevenzione*, a cura di ROSI – SCOPELLITI, Milano, 2006.

AA.VV., *Trattato di medicina legale e scienze affini II*, diretto da GIUSTI, Padova, 1998.

ACCIAI, *Privacy e banche dati pubbliche. Il trattamento dei dati personali nelle pubbliche amministrazioni*, Padova, 2001.

ALBANO – GHELI – ORSINI, *Fondamenti di base dati*, Bologna, 2005, 87

ALPA, *La direttiva comunitaria sul trattamento dei dati personali*, in www.jei.it.

ANTONINI, *Il trattamento illecito di dati personali nel codice della* privacy*: nuovi confini della tutela penale*, in *Dir. pen. proc.*, 2005, 338.

ASHWORTH, *The Criminal Process: An evacuative Study*, Oxford, 1998.

AULETTA, *Riservatezza e tutela della personalità*, Milano, 1978.

BARBATO, *Le banche dati tecnico – scientifiche*, in *Dir. pen. proc.*, 2000, 1659.

BARBATO – CORRADI – LAGO, *Come ovviare al vuoto sui prelievi coattivi creato dalla sentenza n. 238 del 1996,* in *Dir. pen. proc.*, 1997, 363.

BARBATO – CORRADI – LAGO, *L'identificazione personale tramite Dna,* in *Dir. pen. proc.*, 1999, 216.

BARILE, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984.

BARROCU, *Brevi note in tema di indagini per i reati di criminalità organizzata,* in *www.dirittoestoria.it*, quaderno n.4, 2005.

BELFIORE, *La prova del DNA a fondameto di un mandato d'arresto europeo: via libera alla consegna,* in *Cass. pen.*, 2009, 1447.

BENEVENTANO – BERGAMASCHI – GUERRA, *Progetto di base di dati relazionali. Lezioni ed esercizi*, Bologna, 2007.

BLASI, *La protezione dei dati personali nella giurisprudenza della Corte europea dei diritti dell'uomo*, in *Riv. int. dir. uomo*, 1999, 543.

BOLINO – GRANDE, *L'identificazione individuale mediante la metodica di rilievo dattiloscopico F.I.T.* (fingerprint identification technology), in *Arch. med. leg. ass.*, 1994, n.16, 273.

BOLOGNI, *E' un inglese il* killer *della pineta, smascherato dalla banca dati del DNA*, in *La repubblica*, 15 febbraio 2003, 26.

BOLOGNI, *Omicidio Vicentini, il secondo test del DNA scagiona il barista inglese*, in *La repubblica*, 10 marzo 2003, 2.

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

BONETTI, *Riservatezza, diritti dell'uomo e processo penale: aspetti problematici*, in *Ind. pen.*, 1995, 587.

BORDIERI, *Sul valore probatorio del rifiuto ingiustificato dell'imputato di sottoporsi al prelievo del DNA,* in *Cass. pen.*, 2004, 4169.

BRICOLA, *Prospettive e limiti della tutela penale della riservatezza,* in *Riv. it. dir. proc. pen.*, 1967, 1079.

BRICHETTI – PISTORELLI, *La distruzione immediata della prova rischia di ledere i diritti dell'imputato*, in *Guida dir.*, 2006, n.32, 22.

BRUSCO, *Il vizio di motivazione nella valutazione della prova scientifica*, in *Dir. pen.proc.*, 2004, 1414.

BUSIA, Privacy *a rischio per la durata della conservazione*, in *Guida dir.*, 2009, n.30, 78.

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

CALDIROLA, *Il diritto alla riservatezza*, Padova, 2006.

CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc.pen.*, 2005, 624.

CAMON, *Sulla inutilizzabilità nel processo penale dei tabulati relativi al traffico telefonico degli apparecchi "cellulari", acquisiti dalla polizia senza autorizzazione dell'autorità giudiziaria*, in *Cass. pen.*, 1996, 3722.

CANTONE, *Le modifiche processuali introdotte con il "decreto antiterrorismo"*, in *Cass. pen.*, 2005, 2507.

CAPPELLETTI, *Processo e ideologie*, Bologna, 1969.

CARBONI, Scotland Yard *vuole il DNA dei bambini, l'idea di schedare il patrimonio genetico dei piccoli con comportamenti "sospetti"*, in *Corriere della sera*, 17 marzo 2008, 35.

CARDARELLI – SICA – ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Milano, 2004.

CARNELUTTI, *Diritto alla vita privata (contributo alla teoria della libertà di stampa)*, in *Riv. Trim. dir. pubbl.*, 1955, 5.

CAROTA, *Prime ipotesi applicative della normativa sulle banche dati contro la criminalità*, in *Foro it.*, 1986, II, 138.

CAUTADELLA, *La tutela civile della vita privata*, Milano, 1972.

CAVALLI SFORZA – MENOZZI – PIAZZA, *Storia e geografia dei geni umani*, Milano, 2000.

CERRI, *Libertà negativa di manifestazione del pensiero e di comunicazione – diritto alla riservatezza: fondamento e limiti*, in *Giur. cost.*, 1974, 610.

CESARI, *Prova del DNA e contraddittorio mancato*, in *Cass. pen.*, 2002, 534.

CHIAVARIO, *Passi avanti sulle intercettazioni illegali ma c'è bisogno di un ampio ripensamento*, in *Guida dir.*, 2006, n. 39, 13.

CONTI, *Le intercettazioni illegali:* lapsus linguae *o nuova categoria sanzionatoria?*, in *Dir. pen. proc.*, 2007, 163.

CORDERO, *Prove illecite*, in *Tre studi sulle prove penali*, Milano, 1963,

CORDERO, *Dialogo sulle prove*, in *Jus*, 1964, 35.

CORDERO, *Procedura penale*, IX ed., 1987.

CRESPI, *La tutela del segreto*, Palermo, 1952.

A.A.DALIA, *Il controllo giurisdizionale sulla banca dati del ministero dell'interno*, in *Dir. inf.*, 1986, 577.

DE LEO – TURRINA – ORRICO, *Lo stato dell'arte in genetica forense*, Milano, 2003.

DINACCI, *Elaborazione elettronica dei dati presso il ministero dell'interno ed orientamenti giurisprudenziali in tema di procedure di correzione*, in *Giust. Pen.*, 1987, III, 398.

DOLSO, *Libertà personale e prelievi ematici coattivi*, in *Giur. cost.*, 1996, 3222.

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

DOMINIONI, *La prova penale scientifica. Gli strumenti scientifici – tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005.

DOMINIONI, *In tema di nuova prova scientifica*, in *Dir. pen. proc.*, 2001, 1062.

ELMASTRI RAMIREZ – NAVATHE SHAMKANT, *Sistemi di base di dati. Fondamenti*, Milano, 2007.

FACCHIN, *L'interpretazione giudiziaria della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentale: guida alla giurisprudenza della Corte*, Padova, 1990.

FELICIONI, *Accertamenti personali e coattivi nel processo penale: linee di riforma*, in *Dir. pen. proc.*, 2005, 621.

FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Milano, 2007.

FELICIONI, *Considerazioni sugli accertamenti coattivi nel processo penale: lineamenti costituzionali e prospettive di riforma*, in *Ind. pen.*, 1999, 495.

FELICIONI, *L'esecuzione coattiva del prelievo ematico: profili problematici*, in *Cass. pen.*, 1997, 315.

FANUELE, *Dati genetici e procedimento penale*, Padova, 2009.

FANUELE, *L'indagine genetica nell'esperienza italiana ed in quella inglese*, in *Riv. it. dir. proc. pen.*, 2006, 732.

FANUELE, *Un archivio centrale per i profili del DNA nella prospettiva di un diritto comune europeo*, in *Dir. pen. proc.*, 2007, 386.

FERRARO, *C.E.D. del ministero dell'interno e tutela del cittadino*, in *Cass. pen.*, 1991, 826.

FIORI, *I polimorfismi del DNA nuove frontiere e problemi del laboratorio medico – legale*, in *Riv. it. med. leg.*, 1988, 399.

L.FILIPPI, *Distruzione dei documenti e illecita divulgazione di intercettazioni: lacune ed occasioni perse di una legge nata già vecchia*, in *Dir. pen. proc.*, 2007, 152.

L.FILIPPI, *Misure urgenti per il contrato al terrorismo. Le disposizioni processuali*, in *Dir. pen. proc.*, 2005, 1215.

FRIGO, *La consulta salva la libertà personale: il legislatore intervenga subito senza ambiguità*, in *Guida dir.*, 1996, n. 30, 65.

FRIGO, *Ridotti gli spazi della tutela penale*, in *Guida dir.*, 2006, n.47, 27.

V.FROSINI, *La protezione della riservatezza nella società informatica*, in *Inf e dir.*, 1981, 7.

V.FROSINI, *I diritti umani nella società tecnologica*, in *Riv. Trim. dir. pubbl.*, 1981, 1163.

GABRIELI, *La decisione del "prelievo" torna al giudice*, in *Guida dir.*, 2009, n.30, 68.

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

GAMBOTTO MANZONE – CONSOLINI, *Matematica con applicazioni informatiche*, Milano, 1991.

GANDINI, *Il Trattato di Prum articolo per articolo ecco le nuove frontiere per la sicurezza. Banche dati antiterrorismo e interventi congiunti in sette stati dell'UE*, in *Dir. giust.*, 2006, n. 37, 60.

GARGANI, *I rischi e le possibilità dell'applicazione dell'analisi del DNA nel settore giudiziario*, in *Riv. it. dir. proc. pen.*, 1993, 1312.

GARLAND, *The Culture of Control: Crime and Social Order in Contemporary Society*, Oxford, 2001.

GAROFANO, *Delitti imperfetti II*, Milano, 2007.

GENNARI, *Identità genetica e diritti della persona*, in *Riv. crit. dir. priv.*, 2005, 633.

GIACCA, *In tema di prelievo ematico coatto: brevi note a margine della sentenza della Corte cost. n. 238 del 1996*, in *Riv. it. dir. proc. pen.*, 1997, 602.

GIACOBBE, *Riservatezza (diritto alla)*, in *Enc. dir.*, XL, Milano, 1977.

GIANNANTONIO, *Il nuovo disegno di legge sulle banche di dati personali*, in *Riv. Dir. informat. Informaz.*, 1991, 80.

GIANNANTONIO, *Le banche dati contro la criminalità*, in *Cass. pen.*, 1985, 1254.

GIUSI, *DNA, processo ai test, troppi errori, non ci sono certezze. Londra riapre duecento indagini*, in *Corriere della sera*, 23 febbraio 2007, 29.

GLICK – PASTERNAK, *Biotecnologia molecolare, principi e applicazioni del DNA ricombinante*, BOLOGNA, 2001.

GRANELLI, *Banche dati e riservatezza*, in *AIDA*, 1997, 235.

GROSSI, *Inviolabilità dei diritti*, in *Enc. dir.*, XXII, Milano, 1972.

JASANOFF, *La scienza davanti ai giudici*, Milano, 2001.

JEFFRETS – WILSON – THEIN, *Individual, Specific "Fingerprint" of Human DNA*, in *Nature*, 1985, 76.

KOSTORIS, *Alt ai prelievi di sangue coattivi*, in *Dir. pen. proc.*, 1996, 1093.

KOSTORIS – ORLANDI, *Contrasto al terrorismo interno e internazionale*, Torino, 2006.

LEWIN, *Il gene*, Milano, 1999.

MANNA, *Codice della* privacy*: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali*, in *Dir. pen. proc.*, 2004, 17.

MANNA, *I beni della personalità e limiti della protezione penale*, Padova, 1989.

MANNA, *Tutela penale della personalità*, Bologna, 1993.

MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità di fatti criminosi*, in *Arch. giur.*, 1968, 41.

MARCOLINI, *Regole di esclusione costituzionali e nuove tecnologie*, in *Criminalità*, 2006, 393.

MARTINES, *La protezione degli individui rispetto al trattamento automatizzato dei dati nel diritto dell'U.E.*, in *Riv.it.dir.pubbl.com.*, 2000, 724.

MAZZACUVA – PAPPALARDO, *Osservazioni in tema di prelievo ematico coattivo*, in *Ind. pen.*, 1999, 485.

MELILLO, *L'acquisizione dei tabulati relativi al traffico telefonico fra limiti normativi ed equivoci giurisprudenziali*, in *Cass. pen.*, 1999, 743.

MENCARELLI, *L'inutilizzabilità e l'acquisizione delle prove nel nuovo sistema processuale, in Giust. pen.*, 1989, III, 84.

MENDELLA, *Banca dati del DNA: l'arma anticrimine. Nel resto d'Europa funziona così*, in *Dir. giust.*, 2005, n. 21, 11.

MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, *Dir. inf.*, 1993, 313.

MIRAGLIA, *La ricerca della verità per condannare ed assolvere: il test del DNA e l'esperienza statunitense*, in *Dir. pen. proc.*, 2003, 1555.

MISSORICI, *Banche dati e tutela della riservatezza*, in *Riv. int. dir. uomo*, 1996, 54.

MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, Torino, 1995.

MONTANARO, *Per le esigenze della polizia scientifica occorrono norme al passo con le nuove tecnologie*, in *Guida dir.*, 1996, n. 30, 69.

NUVOLONE, *Le prove vietate nel processo penale nei paesi di diritto latino*, in *Riv. dir. proc.*, 1968, 448.

ORLANDI – PAPPALARDO, *L'indagine genetica nel processo penale germanico: osservazioni su una recente riforma*, in *Dir. pen. proc.*, 1999, 762.

PACE, *Nuove frontiere della libertà di comunicare riservatamente (o piuttosto del diritto alla riservatezza)?*, in *Giur. cost.*, 1993, 742.

PAGANO, *Tutela dei dati personali: evoluzione della legislazione europea e stato del dibattito*, in *Infor. e dir.*, 1986, 67.

PALUMBO, *Progettare database. Modelli, metodologie e tecniche per l'analisi e la progettazione di basi di dati relazionali*, Bologna, 2009.

PATRONO, Privacy *e vita privata (dir. pen.)*, in *Enc. dir.*, XXXV, Milano, 1986.

PENASA, *Alla ricerca dell'anello mancante: il deposito dello strumento di ratifica della Convenzione di Oviedo*, in *www.forumcostituzionale.it*.

PERRI, Privacy, *diritto e sicurezza informatica*, Milano, 2007.

PICOTTI, *Trattamento dei dati genetici, violazioni della* privacy *e tutela dei diritti fondamentali*, in *Dir. dell'inf. e dell'inform.*, 2003, 722.

POLI, *Biotecnologie, principi e applicazioni dell'ingegneria genetica*, Torino, 2000.

PULEIO, *Banca dati DNA: basta con i rinvii sui prelievi, servono più garanzie. L'archivio dei profili genetici è vitale per la lotta al terrorismo,* in *Dir. e giust.*, 2005, n. 10, 125.

PULEIO, *Quando la scienza è alleata del giudice. I nuovi saperi e la ricerca della verità: l'esigenza di attendibilità nell'uso delle conoscenze tecniche*, in *Dir. e giust.*, 2006, n. 13, 68.

RICCI – PREVIDERÈ – FATTORINI – CORRADI, *La prova del DNA, per la ricerca della verità. Aspetti giuridici biologici e probabilistici*, Milano, 2006.

ROSSETTI, *Commento alla direttiva 95/46*, in *Dir. industr.*, 1997, n.3, 246.

RUGGIERI, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001.

SANTACROCE, *Prelievo coattivo del sangue a scopo probatorio e tutela della libertà personale*, in *Cass. pen.*, 1996, 3570.

SCAFFARDI, *Le banche dati genetiche personali per fini giudiziari e i diritti della persona*, in *www.forumcostituzionale.it*, 2008.

SCALVI, *DNA – Test come* "scientific evidence"*: poteri del giudice e validità della prova. Rilievi comparatistica*, in *Riv. it. dir. med. leg.*, 1997, 641.

SCHELLINO, *Corte costituzionale e accertamenti coattivi incidenti nella sfera corporale della persona*, in *Leg. pen.*, 1997, 173.

SERROTTI, *Libertà di informazione e libertà informatica: la tutela della riservatezza*, in *Inf. e dir.*, 1996, 84.

SPINELLA – SOLLA, *L'identificazione personale nell'investigazione scientifica: DNA e impronte digitali*, in *Cass. pen.*, 2009, 431.

STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Padova, 2008.

STILO, *Il diritto all'autodeterminazione informativa: genesi storica di un diritto fondamentale dell'*homo tecnologicus, in *Nuovo dir.*, 2002, 20.

D.SIRACUSANO – GALATI – TRANCHINA – ZAPPALÀ, *Diritto processuale penale*, Milano, 2004.

TAMIETTI, *L'utilizzazione di prove assunte in violazione di un diritto garantito dalla Convenzione non viola l'equo processo: riflessioni sul ruolo della Corte europea e sulla natura del sindacato da essa operato in margine alla sentenza P.J. e J.H. v. Regno Unito*, in *Cass. pen.* , 2002, 1827.

TONINI, *La prova penale*, IV ed., Padova, 2000.

TONINI, *Manuale di procedura penale*, X ed., Milano, 2009.

TONINI, *Prova scientifica e contraddittorio*, in *Dir. pen. proc.*, 2003, 1460.

UBERTAZZI, *Il diritto alla* privacy. *Natura e funzioni giuridiche*, Padova, 2004.

UBERTIS, *Attività investigativa, e prelievo di campioni biologici*, in *Cass. pen.*, 2008, 8.

UBERTIS, *La conoscenza del fatto nel processo penale*, Milano, 1990.

UBERTIS, *La prova penale. Profili giuridici ed epistemologici*, Torino, 1995.

VIGONI, *Corte Costituzionale, prelievo ematico coattivo e test del DNA*, in *Riv. it. dir. proc. pen.*, 1996, 1023.

VIGORITI, *Prove illecite e Costituzione*, in *Riv. dir. proc.*, 1968, 71.

WARREN – BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, 1891, 4.

WILLIAMS – JONSON, *Forensic DNA Databasing: a European Prospective, Interim Report*, Durham, 2005.

WILLIAMS – JONSON, *Genetic Policing, the Use of DNA in Criminal Investigations*, London, 2008.