La videosorveglianza tra processo penale e codice della privacy

***Stefano Fratucello**, avvocato del foro di Padova e dottore di ricerca in Diritto processuale penale presso l'Università degli Studi di Ferrara*

PREMESSA.

La possibilità di captare immagini di una persona in luoghi pubblici o privati, attraverso i moderni mezzi elettronici, è sempre più frequente. Cogliere abusivamente attimi d'intimità di una persona non è più un evento eccezionale. Ce lo ricorda ogni giorno la cronaca mondana.

Tanto è importante il tema che, anche di recente si sono dovute pronunciare le Sezioni Unite della Cassazione [1], fornendo un'interessante sintesi sullo stato attuale della giurisprudenza sulla materia.

Il problema del controllo del cittadino mediante strumenti audiovisivi se lo è posto espressamente anche il c.d. Codice della privacy e *de iure condendo* se ne sta occupando ancora il legislatore nel progetto di modifica della disciplina delle intercettazioni [2].

Il T.U. (d.lgs. 196\2003) non si dimentica dell'argomento, stabilendo, all'art. 134, che "*Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantire la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 11*".

Pur cercando di essere sintetici, non possiamo esimerci dal ricordare quali siano i principi contenuti nel T.U. poiché la protezione dell'identità personale ha trovato sempre maggior spazio nell'abito della legislazione vigente; uno spazio così importante da comportare anche delle interferenze con il processo penale.

E' doveroso, innanzitutto, interrogarci se esiste un **diritto di rango costituzionale alla protezione dei dati personali** e se questo diritto può interferire con la disciplina di acquisizione dei mezzi di prova nel processo penale.

Non vi è dubbio che il codice di rito si è modificato nel corso degli anni adeguandosi all'esigenza di tutelare la privacy. Basti leggere l'art. 472 c.p.p. nella sua formulazione attuale, ove non si disciplina solo la pubblicità dell'udienza, ma, si è giunti a porre un vero e proprio **divieto probatorio** nell'ambito di procedimenti per i delitti di cui agli artt. 600bis, 600ter,

---

[1] Cass. S.u., 28/07/2006, n. 26795, in **G. dir.**, 2006, n. 33, pag. 51 ss.

[2] Cfr. Atto Camera n. 1638 del 16 settembre 2006, disegno di legge recante "Disposizioni in materia di intercettazioni telefoniche ed ambientali e di pubblicità degli atti di indagine" approvato dal Consiglio dei Ministri nella seduta del 4 agosto 2006, in *www.giustizia.it*

600quinquies, 609bis, 609ter, 609octies c.p. ; l'art. 472 co. 3bis c.p.p., infatti, sancisce il divieto di "porre domande sulla vita privata e sulla sessualità della persona offesa se non sono necessarie alla ricostruzione del fatto".

Il nostro punto di vista, peraltro, sarà, per così dire, "esterno" al codice di procedura (salvo qualche necessario riferimento alle sue norme), tentando una disamina della legislazione vigente, in particolare del T.U. e dei provvedimenti più interessanti del Garante [3].

IL TESTO UNICO COME RIFLESSO DELL'ART. 2 COST. LA TEORIA DELLE "SFERE".

Dal dato normativo positivo (art. 2 t.u.) è ricavabile l'intenzione del legislatore di collocare tra i diritti inviolabili, protetti dall'art. 2, 3 co. 2 e 13 Cost., anche il diritto alla protezione dei dati personali quale *species* del diritto alla riservatezza [4].

Il Garante per la Privacy, già nel lontano 1997, nella sua relazione annuale (pag. 10) sottolineava che la normativa relativa alla protezione dei dati personali collocava questi ultimi "*in una* ***dimensione propriamente costituzionale****, visto che il trattamento deve svolgersi nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche…dignità dell'interessato (ai sensi dell'art. 3 Cost., primo comma, prima parte, e dell'art. 2 Cost.), valore sommo a cui è ispirata la legislazione sul trattamento dei dati personali*".

Peraltro, anche tra i dati personali, vi è una scala gerarchica, caratterizzata da una più o meno ampia tutela positiva (art. 4, 17, 24) [5]. Il T.U. distingue nettamente il *diritto alla riservatezza* e all'*identità personale* da quello di *protezione dei dati personali* (art. 2 T.U.) ed individua all'interno del *genus* "dati personali" (definiti dall'art. 4 lett. b)), la *species* dei *dati sensibili* (art. 4 lett. d)), *supersensibili*, quasi-*sensibili* (art. 17) e i *dati giudiziari* (art. 4 lett. e)), correlandovi un diverso e graduato livello di protezione.

Questa classificazione riecheggia quella elaborata dalla giurisprudenza costituzionale tedesca fin dal 1969 nella c.d. teoria delle sfere, secondo cui ogni diritto racchiude in sé un nucleo inviolabile legato alla dignità umana (1 sfera) all'esterno del quale vi è una seconda sfera

---

[3] Per un'accurata sintesi bibliografica, si veda Codice in materia di protezione dei dati personali, AA.VV. a cura di G. Cassano e S. Fadda, Ipsoa, 2004.

4 Per quanto riguarda il diritto alla riservatezza, la Corte Costituzionale, già con la sent. del 12.4.1973 n. 38, lo collocava tra i diritti inviolabili, protetti dall'art. 2, 3 co. 2 e 13 Cost.

[5] In questo senso, anche la giurisprudenza di legittimità ha evidenziato che "*Il trattamento dei dati personali appartenenti alla species dei supersensibili, che investe la parte più imtima della persona nella sua corporeità e nelle sue convinzioni psicologiche più riservate, riceve, per la sua particolare natura e per i valori costituzionali posti a loro presidio (artt. 2 e 3 Cost.), una "tutela rafforzata" che si estende anche al trattamento operato dai "soggetti pubblici" …*", aggiungendo che "*l'incrocio di dati costituisce un valore aggiunto informativo in sé tutelato*". Nel caso di specie, l'Amministrazione dell'Interno aveva trattato dei dati personali supersensibili riguardanti la diffusione su Internet di immagini di tipo osceno e pornografico da parte di un dipendente e segnalate da un collega funzionario di polizia all'amministrazione competente(Cfr. Cass. civ., Sez. I, 08/07/2005, n.14390).

attinente alla persona la cui tutela è soggetta al bilanciamento con altri rilevanti interessi; infine, vi è una terza sfera liberamente comprimibile dallo Stato[6].

Vi è un filo conduttore, però, che sta a monte della necessità di tutela dei dati personali. Questo filo conduttore, a mio avviso, sta nel diritto della persona (ecco il riferimento all'art. 2 e 3 co. 1 della Cost.) a non essere ridotta ad un "*insieme di dati*". Mi spiego: nella raccolta dei dati vi è il fondato pericolo che la personalità dell'individuo venga "schedata", identificata, direi appunto, ridotta **in quei dati**. Ciò non pare lecito; lo dice espressamente l'art. 14 comma 1 del T.U. quando sancisce che "*Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato…*".

Pensiamo a quante volte il giudice è chiamato a valutare il comportamento dell'imputato (per es. la capacità a delinquere prevista dall'art. 133 co. 2 c.p.) o della persona offesa (giudizio sulla personalità previsto dall'art. 236 c.p.p.) o ancora dei testimoni (giudizio sulla credibilità ex art. 236 co. 3 c.p.p.).

Di qui l'esigenza di un controllo sull'uso dei dati personali anche nel processo.

I PRINCIPI APPLICABILI AD OGNI TRATTAMENTO (ART. 11 T.U.) E DIRITTI DELL'INTERESSATO.

L'art. 11 – nonostante la sua collocazione al di fuori dei principi generali – è la norma di fondamentale importanza nella nostra indagine, perché detta le "Regole generali per il trattamento dei dati", valevole per tutti i trattamenti. I criteri enucleati nell'art. 11 recepiscono fedelmente l'art. 6 della direttiva 95\46\CE, nonché l'art. 5 della Convenzione di Strasburgo del 28.1.1981.

In particolare la norma richiede che i dati siano trattati in modo lecito, esatto, completo, per uno scopo determinato e in modo pertinente a questo scopo; infine il trattamento deve avere una durata limitata al raggiungimento dello scopo (c.d. *diritto all'oblio*).

Mentre gli altri diritti riservati all'interessato del trattamento, trovano – come vedremo – dei limiti di fronte ad altri interessi rilevanti (ragioni di giustizia, indagini difensive…), il *diritto all'oblio* sembra godere di privilegio assoluto.

Tale diritto è codificato dall'art. 11 lett. e) e consiste essenzialmente nel diritto alla cancellazione dei dati personali dopo un certo lasso di tempo, o con espressione forse più efficace, nel *diritto di essere dimenticati*.

La determinazione temporale del trattamento dei dati è essenziale acchè il trattamento possa dirsi avvenuto nel rispetto del altri criteri.

[6] Sull'argomento si tornerà oltre.

Quanto alla *liceità* del trattamento, essa si riferisce al rispetto di tutte le norme dell'ordinamento statuale e non solo del codice (è illecito il trattamento effettuato in violazione del segreto professionale, per esempio).
Quanto ai criteri di *correttezza, pertinenza…*(art. 11 lett. c, d), essi rispondono all'esigenza di impedire il potenziale pregiudizio che dati non aggiornati, eccedenti rispetto allo scopo del trattamento, incompleti possono arrecare all'interessato. Pensiamo solo al pregiudizio (anche alla luce del nuovo art. 66bis c.p.p.) che può derivare dall'archivio (c.d. SDI) delle forze di polizia ove sono raccolte segnalazioni all'autorità giudiziaria senza seguito, notizie di reato poi archiviate, omonimie.
I contorni di questi valori, tuttavia appaiono abbastanza sfumati, mancando un parametro legale per valutarne l'effettivo rispetto. Certo è facile dire che "non è pertinente" il dato attinente al rapporto di coniugio dell'imputato nell'ambito di un processo penale ove si discute della sua responsabilità per il reato di truffa; ma lo stesso dato diventa "pertinente" se viene indicata quale teste la moglie. Questo giudizio suppone i parametri normativi indicati dagli art. 187 co. 2 e 190 c.p.p. Ma possiamo dire che effettivamente siano questi i parametri cui fa riferimento il T.U.?
Il principio di pertinenza\non eccedenza, oltre all'aspetto quantitativo, ha riguardo – come poc'anzi detto – anche all'aspetto temporale della conservazione dei dati, nel senso che questi debbono essere conservati "*per un periodo di tempo non superiore a quello necessario per gli scopi per i quali sono stati raccolti*".
Mentre in ambito civilistico il criterio temporale può essere facilmente delimitato (per es., la documentazione necessaria a provare il pagamento di un debito dovrebbe dirsi non più necessaria, decorso il termine prescrizionale), in ambito penale, risulta più arduo identificare il *dies ad quem* (es: le immagini raccolte di videosorveglianza davanti all'ingresso ad una privata abitazione per quanto possono essere custodite? E che dire dell'accertamento fatto alle dogane del passaggio di un autoveicolo?).
Vi torneremo oltre, ma rammentiamo sin d'ora che solo nell'art. 132, relativo alla conservazione dei tabulati telefonici, il legislatore si è preoccupato di stabilire un termine ben definito. Si ricordi inoltre, che l'art. 167 (richiamando l'art. 25) sanziona penalmente la comunicazione o la diffusione dei dati, quando è decorso il tempo indicato nell'art. 11 lett. e).
Nel comma 2 dell'art. 11 è contenuto un **divieto d'utilizzazione** dei dati trattati illegittimamente che pare incidere anche nel processo penale, alla luce della nuova disciplina introdotta dalla legge 281\2006 di conversione del d.l. 259\2006.

Prima di tentare di trarre alcune provvisorie conclusioni, riassumiamo brevemente quelli che paiono essere i diritti fondamentali che il T.U. (anche al di fuori dell'art. 11) riconosce all'interessato per la protezione dei suoi dati personali:

1. il **diritto di accesso** ai propri dati presso il soggetto che li detiene (per controllarne la legittimità dell'uso) (art. 7).
2. il **diritto all'informativa** ed al **consenso al trattamento** (art. 13)
3. il **diritto alla tutela amministrativa e giurisdizionale** (art. 141 ss.)
4. il **diritto all'oblio** (art. 11 lett. e)

LA POSSIBILE INUTILIZZABILITA' DEL DATO RACCOLTO *CONTRAM LEGEM*?

L'art. 11 co. 2 è perentorio nel sancire, con terminologia processualistica, l'inutilizzabilità dei dati personali trattati "in violazione della disciplina rilevante in materia di trattamento dei dati personali".

Dubbi, però, possono sussistere, sulla qualificazione di questa sanzione, alla luce delle altre disposizioni del T.U. su cui si leggerà più avanti. Tuttavia, la norma pare assumere qualche rilevanza alla luce del nuovo comma 2 dell'art. 240, modificato dalla l. 281\2006, che oggi sancisce in modo inequivocabile l'inutilizzabilità dei "*documenti formati attraverso la raccolta illegale di informazioni*".

Già qualcuno [7] ha sostenuto che "tra questi documenti dovrebbero annoverarsi quelli che riportano dati sensibili indebitamente acquisiti in violazione della disciplina dettata dal dlgs. 30 giugno 2003, n. 196".

LIMITI DI ESERCIZIO DEL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI.

Tra i diritti fondamentali che afferiscono alla tutela dei dati personali, vi sono – come già detto – quelli menzionati negli artt. 7 e 13, 145 (il **diritto di accesso** ai propri dati presso il soggetto che li detiene, per controllarne la legittimità dell'uso; il **diritto all'informativa** ed al **consenso al trattamento**; il **diritto alla tutela amministrativa e giurisdizionale**).

I diritti che afferiscono alla tutela dei dati personali trovano, nel testo unico, varie limitazioni derivanti dal bilanciamento di interessi con altri valori di rilevanza costituzionale, tra cui il diritto di difesa, l'accertamento e la repressione dei reati.

LE FINALITA' DIFENSIVE E LE RAGIONI DI GIUSTIZIA (OVVERO IL TRATTAMENTO IN AMBITO GIUDIZIARIO EX ART. 47 T.U.).

Le norme d'interesse sono gli art. 8, 13, 24, 25 ma soprattutto, l'art. 160 perchè, al comma 6 contraddicendo apparentemente l'art. 11 comma 2, stabilisce che "*la validità, l'efficacia, e l'utilizzabilità 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*".

[7] R. BRICCHETTI, in *G. dir.* 2006, n. 39, pag. 25.

Ma, il rimando alle regole processuali sull'inutilizzabilità dell'atto probatorio non risolve il problema, perché il problema è se l'art. 191 c.p.p. (e l'art. 240 co. 2 c.p.p.) si riferisca solo alla violazione di divieti probatori contenuti nelle norme processuali o no.

Segnaliamo subito che, per quanto riguarda il trattamento dei dati in ambito giudiziario, il T.U. prevede una regola generale di esclusione dall'applicabilità di determinate disposizioni, rimuovendo preventivamente gli ostacoli che potrebbero derivare all'autorità giudiziaria all'uso dei dati personali. La norma è l'art. 47 che, peraltro, non richiama espressamente l'art. 11 lasciando all'interprete – nei singoli casi – l'onere di verificare quando prevalga l'una o l'altra disposizione.

Venendo ad analizzare i limiti alla tutela dei dati personali, già nell'art. 8 del T.U. si legge (comma 2) che il diritto di accesso è impedito se il trattamento di dati personali è effettuato – per quel che ci interessa – nell'ambito di indagini difensive o per l'esercizio del diritto in sede giudiziaria "*limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per le stesse, ai sensi dell'articolo 24, comma 1, lettera f)*", nonché per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia.

Il diritto di accesso cede il passo di fronte alle esigenze difensive (pur con limiti temporali), ma soprattutto cede il passo di fronte a "ragioni di giustizia".

Non è possibile accedere ai dati detenuti dagli uffici giudiziari, non sembra possibile ottenerne la rettifica, l'aggiornamento, la cancellazione. L'unico rimedio per l'interessato parrebbe quello di segnalare al Garante l'eventuale violazione del T.U. e sperare nell'attivarsi di quest'ultimo che, nei modi previsti dall'art. 160, può disporre ispezioni ed accertamenti.

L'art. 160 necessita di ulteriore approfondimento perché – pur prevedendo la facoltà di accertamento da parte del garante sul corretto uso dei dati personali da parte degli uffici giudiziari – permette a questi di opporre il segreto d'ufficio; ma soprattutto, come si è già detto, il comma 6 dell'art. 160, contraddicendo apparentemente l'art. 11 comma 2, stabilisce che "*la validità, l'efficacia, e l'utilizzabilità 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*".

Anche **l'art. 13** che disciplina il diritto all'informativa preventiva da parte del titolare del trattamento e il diritto al consenso al trattamento trova gli stessi limiti del diritto d'accesso.

Infatti, l'informativa non è dovuta quando i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria e, ancora, quando i dati sono trattati ai fini dello svolgimento delle investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Infine, l'informativa non è dovuto

quando il trattamento è effettuato per ragioni di giustizia, in virtù del richiamo espresso dell'art. 47.

In modo analogo, l'art. 24 esclude la necessità del **consenso al trattamento**, per le stesse ragioni sopra individuate, con la precisazione, però che, nell'ambito delle investigazioni difensive, è esclusa la possibilità della diffusione dei dati personali [8].

Più in generale, il divieto di comunicazione e diffusione dei dati è esteso ai privati dall'art. 25 in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo indicato nell'articolo 11, comma 1, lettera e) ovvero per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.

Mentre i privati (anche le parti e i difensori, quindi) incontrano un limite temporale o derivante da un provvedimento autoritativo all'uso dei dati personali, tale limite viene meno quando il trattamento è necessitato da finalità di accertamento e repressione dei reati, purchè la richiesta dell'autorità giudiziaria sia "conforme alla legge" (id est, rispetti le norme di procedura penale) [9].

Il punto rimane quello già sopra evidenziato e cioè: l'esigenza di accertamento di reati prevale anche sulla regola generale contenuta nell'art. 11 (come parrebbe dal dato testuale) ovvero si deve leggere nella regola generale un richiamo all'art. 191 c.p.p.?

IL TRATTAMENTO DA PARTE DELLA POLIZIA GIUDIZIARIA.

Quanto sopra detto per gli altri soggetti del procedimento (pubblico ministero, difensori, giudice), vale in buona parte anche per la polizia giudiziaria, in virtù della norma generale (art. 53) che le consente di comprimere in varia misura i diritti previsti dal T.U.

---

[8] In relazione all'art. 24, è d'interesse la decisione della Corte Cost., 02/03/2004, n. 83, con la quale si è riconosciuto il diritto della persona offesa ad ottenere i dati anagrafici dell'imputato per esercitare la facoltà di ricorso diretto nell'ambito del procedimento penale avanti al Giudice di Pace.

[9] In materia civile, interessante è Cass. civ., Sez. I, 07/11/2001, n. 13766, in **Giust. Civ.**, 2002, I, 1930, secondo cui: "*In sede di giudizio per la dichiarazione giudiziale di paternità naturale il rifiuto ingiustificato di sottoporsi a esami ematologici costituisce comportamento valutabile ai sensi dell'art. 116, comma 2 c.p.c. Non vale a giustificare un tale rifiuto (ai fini di escluderne l'utilizzabilità ex art. 116 cit.) il mero timore di una violazione della normativa sulla tutela dei dati personali e, in particolare, di un uso non consentito dei dati stessi, nonché l'omesso richiamo, nella ordinanza ammissiva del mezzo istruttorio, all'obbligo di osservanza della l. 31 dicembre 1996 n. 675. Nè, ancora, in una tale eventualità, sussiste alcun obbligo, per il giudice del merito, di interpellare il Garante per la tutela dei dati personali per riceverne indicazioni sulle cautele da adottare nell'affidamento dell'incarico, non configurandosi nel sistema alcun potere di controllo o di indirizzo dell'autorità garante sulle modalità di esercizio della giurisdizione.*".

Il legislatore sembra, però, aver prestato maggior attenzione alla potenziale dannosità insita nelle banche-dati dell'autorità di pubblica sicurezza (CED) o di polizia giudiziaria (SDI) per la loro idoneità a creare profili d'identità di "sospettati" basati su dati trattati in modo non corretto.

Il Garante ha avuto modo di pronunciarsi più volte su questo punto, segnalando alle forze di polizia (ma anche alle Procure) il mancato rispetto dell'art. 11 e 54 del T.U. (in particolare, per quel che riguarda l'accesso indiscriminato ai dati e il loro mancato aggiornamento). Ma il punto più critico, per quanto attiene, la polizia giudiziaria, sta nel trattamento di dati sensibili.

5.3. LA TUTELA DEI DATI SENSIBILI, QUASI-SENSIBILI E SUPERSENSIBILI.

Più attenzione sembra aver prestato il legislatore nella tutela dei dati c.d. sensibili e, all'interno di questa categoria dei dati "quasi sensibili" ("*che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato*") e "supersensibili", cioè, quelli "*idonei a rivelare lo stato di salute e la vita sessuale*".

Quanto ai primi (dati **quasi-sensibili**), l'art. 17 stabilisce che Il trattamento degli stessi necessita di modalità di protezione maggiore*, "in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare".* Le misure e gli accorgimenti necessarie sono prescritti dal Garante.

Tra i dati quasi-sensibili, vengono individuati quelli detenuti dagli istituti di credito (nelle c.d. "centrali rischi", ove sono inclusi i soggetti protestati; ovvero i dati biometrici acquisiti tramite le impronte digitali)

In attuazione dell'art. 17 il Garante (con provvedimento del 27 ottobre 2005) ha stabilito che è inibita alle banche "un'attività di raccolta indifferenziata di dati particolarmente significativi (quali quelli relativi alle impronte digitali), poiché contrasta con il principio di necessarietà, a meno che non si tratti di filiali, per esempio, esposte a particolari rischi di rapina (circostanza questa che deve essere verificata in concreto, anche con riferimento temporale, poiché la cessazione dell'esigenza di particolare sicurezza obbliga alla cancellazione immediata dei dati).

Inoltre, gli interessati devono essere informati del rilevamento e devono poter accedere ugualmente all'istituto se non prestano il consenso.

Se vi è abbinato un sistema di videosorveglianza (vedremo poi, le regole specifiche dettate dall'art. 134 del T.U.), occorre che le riprese siano limitate all'ingresso della banca. Per quanto concerne la conservazione, immagini e dati biometrici debbono essere cancellati dopo una settimana.

A questi dati può accedere solo l'autorità giudiziaria e di polizia, con riferimento a specifiche attività investigative connesse all'accertamento o alla prevenzione di reati svolte in conformità al codice di procedura penale.

Vi è, però, da chiedersi, che cosa ne sia dei dati trattenuti più del tempo consentito dal provvedimento del garante: se non venissero distrutti, potrebbero ugualmente essere acquisiti

dall'autorità giudiziaria o dalla polizia giudiziaria? Probabilmente no, alla luce del nuovo art. 240 co. 2 c.p.p.

Quanto ai **dati sensibili** e **supersensibili**, l'art. 26 sancisce che, di regola, per il trattamento, occorre 1) *il consenso scritto dell'interessato* 2) *la previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.*

Quanto al primo presupposto, lo stesso art. 26 esclude la necessità del consenso (come per gli altri dati), quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive o per far valere o difendere in sede giudiziaria un diritto. Se, però, i dati sono idonei a rivelare lo stato di salute e la vita sessuale (c.d. dati supersensibili), "il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile".

Quanto al secondo presupposto, (*previa autorizzazione del Garante*), il T.U. prevede (artt. 39\41) che il Garante, in via generale, possa autorizzare preventivamente il trattamento (e così ha fatto per avvocati, investigatori privati e altri soggetti pubblici), rimuovendo in modo permanente, di fatto, quest'ostacolo.

Per il trattamento in ambito giudiziario è l'art. 47 lett. *a)* che esclude, in via generale, la necessità della previa autorizzazione del Garante.

Rimane il dubbio sulla necessità del consenso, perché di questo presupposto né l'art. 47 né l'art. 26 dicono.

Forse "la dimenticanza" è legata al fatto che, nel processo, l'acquisizione di dati "supersensibili" necessità sempre del consenso dell'interessato ovvero di una copertura di legge. Ma qui entra in gioco l'art. 13 più che l'art. 2 della Costituzione.

Non occorre ricordare, infatti, che la Corte Cost. (sent. n. 238 del 9/7/1996) ha dichiarato "*illegittimo, per contrasto con l'art. 13 cost., l'art. 224 comma 2 c.p.p. nella parte in cui consente che il giudice, nell'ambito delle operazioni peritali, disponga coattivamente misure (come il prelievo ematico) che comunque incidano sulla libertà personale dell'indagato o dell'imputato o di terzi, al di fuori di quelle specificamente previste nei "casi" e nei "modi" dalla legge*.)".

Non occorre ricordare, inoltre, che il legislatore, per colmare il buco normativo, ha introdotto il comma 2bis nell'art. 349 e modificato il comma 3 dell'art. 354 c.p.p. per permettere il prelievo coattivo di materiale biologico, ai fini dell'individuazione dell'indagato.

Quanto sopra detto vale anche per la presa visione o il rilascio di copia di **Cartelle cliniche** (art. 92) a favore di soggetti diversi dall'interessato [10]. Anche in questo caso, le indagini

[10] L'art. 92 dispone:…2. Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

difensive dirette all'acquisizione dei dati contenuti nelle cartelle non necessitano del consenso dell'interessato e dell'autorizzazione del Garante viene rilasciata in via preventiva.

Anche in questo caso, però, nulla si dice, del trattamento "per ragioni di giustizia", dandosi per scontato, ancora una volta, che la tutela dei dati personali ceda il passo di fronte alla necessità di accertamento e, prima, di repressione di reati.

Ed, in effetti, già nella vigenza della l. 675\96, il Garante aveva avuto modo di pronunciarsi a fronte del ricorso (qualificato poi come reclamo) di un medico sociale che riteneva illegittima l'acquisizione delle cartelle cliniche relative a calciatori accusati di doping sportivo. Il Garante specificava allora, in relazione agli art. 4 lett. e) e 9 della l. 675\96 che nell'indagine penale, alla polizia giudiziaria (e, a maggior ragione all'autorità giudiziaria) era possibile accedere ai dati delle cartelle cliniche e che quei dati erano comunque, "pertinenti".

L'art. 48 conferma questa lettura legittimando la creazione di banche-dati (anche acquisiti per via telematica) presso gli uffici giudiziari, perché raccolti "***in conformità alle vigenti disposizioni processuali***" [11].

La norma ricalca quella dell'art. 54 per la polizia giudiziaria.

Per l'attività di quest'ultima, però, il legislatore si è ulteriormente preoccupato di stabilire che, quando il trattamento riguarda dati quasi-sensibili ed, in particolare "*banche di* ***dati genetici o biometrici****, a tecniche basate su dati relativi all'ubicazione, a banche di dati basate su particolari tecniche di elaborazione delle informazioni e all'introduzione di particolari tecnologie"*, occorre rispettare le prescrizioni adottate dal Garante ai sensi dell'art. 17.

A questo proposito, il Garante, pur se sollecitato dal reclamo (*rectius*, segnalazione) di un soggetto indagato nell'ambito di un procedimento penale per furto (e identificato mediante il confronto con tracce di DNA detenute in una banca-dati dei Carabinieri del Ris), non si è

---

a) di far valere o difendere un diritto in sede giudiziaria ai sensi dell'articolo 26, comma 4, lettera c), di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

[11] L'art. 48 dispone: 1. Nei casi in cui l'autorità giudiziaria di ogni ordine e grado può acquisire **in conformità alle vigenti disposizioni processuali** dati, informazioni, atti e documenti da soggetti pubblici, l'acquisizione può essere effettuata anche per via telematica. A tale fine gli uffici giudiziari possono avvalersi delle convenzioni-tipo stipulate dal Ministero della giustizia con soggetti pubblici, volte ad agevolare la consultazione da parte dei medesimi uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei princìpi di cui agli articoli 3 e 11 del presente codice.

L'art. 49 prevede: Disposizioni di attuazione.

1. Con decreto del Ministro della giustizia sono adottate, anche ad integrazione del D.M. 30 settembre 1989, n. 334 del Ministro di grazia e giustizia, le disposizioni regolamentari necessarie per l'attuazione dei princìpi del presente codice nella materia penale e civile.

ancora pronunciato nel merito. Tuttavia, l'autorità non ha mancato di evidenziare "il vuoto normativo" in materia [12].

Quasi a voler correre ai ripari, il Consiglio dei Ministri [13] ha programmato la modifica del c.p.p. per estendere l'applicazione dell'art. 349 c.p.p. anche a finalità diverse dalla sola identificazione dell'indagato.

SULLA VIDEOSORVEGLIANZA IN PARTICOLARE.

Come abbiamo già detto, l'art. 134 T.U. si occupa anche della videosorveglianza, ma senza entrare nel dettaglio, rimandando all'emanazione di codici di autoregolamentazione per l'attuazione della norma di principio.

Il Garante, più che il codice di deontologia, si è preoccupato di emettere un provvedimento (prima nel 2000 e aggiornato nel 2004 [14]) che disciplina in maniera analitica, in ogni settore, la raccolta di immagini senza il consenso dell'interessato. Rimandando a quanto già detto per i dati biometrici, è interessante il punto di partenza del Garante, preoccupato del fatto che "*…nei luoghi pubblici o aperti al pubblico… non si possono privare gli interessati del diritto di circolare senza subire ingerenze incompatibili con una libera società democratica (art. 8 Conv. europea diritti uomo ratificata con l. n. 848/1955), derivanti da rilevazioni invadenti ed oppressive riguardanti presenze, tracce di passaggi e spostamenti, facilitate dalla crescente interazione dei sistemi via Internet ed Intranet*.".

E' in questo *incipit* che si coglie il profondo punto di attrito tra l'esigenza del singolo di non essere spiato ovunque egli vada dall'occhio nascosto del "grande fratello" e l'esigenza di repressione di condotte penalmente rilevanti.

Il provvedimento del Garante pare porre dei limiti rilevanti all'occhio indiscreto delle telecamere, richiamando i principi stabiliti dall'art. 11 del T.U.: in particolare quello di liceità (con particolare riferimento al rispetto delle norme penali di procedura penale); quello di necessarietà; di proporzionalità (es: attenzione all'angolo di ripresa delle immagini, anche se in luoghi pubblici).

La violazione delle disposizioni contenute nel provvedimento espongono – per espressa previsione – all'inutilizzabilità dei dati raccolti (art. 11), al blocco o sospensione del trattamento, a sanzioni penali.

Cerchiamo di esemplificare.

---

[12] Si veda SOLE-24 ORE n. 255 del 17.9.2006.

[13] Si veda SOLE-24 ORE n. 275 del 11.10.2006.

[14] Cfr, provvedimento generale 29.11.2000 e 23.4.2004 editi su *www.garanteprivacy.it*.

Davanti all'ingresso di una banca è posta una telecamera che inquadra la porta d'accesso ma anche la prospicente piazza in cui avviene il furto di una bicicletta lasciata aperta.
L'autorità giudiziaria, dopo alcuni mesi dal fatto, chiede alla banca di consegnare il filmato della telecamera necessario per le indagini. La banca consegna il filmato che non era stato ancora distrutto.
E' questa una prova utilizzabile nel processo penale?
Leggiamo alcune parti del provvedimento generale del garante per cercare una risposta (se c'è) al quesito:

"*Principio di liceità…La videosorveglianza deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati, di quanto prescritto da altre disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi.*

Vanno richiamate al riguardo le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela (toilette, stanze d'albergo, cabine, spogliatoi, ecc.). Vanno tenute presenti, inoltre, le norme riguardanti la tutela dei lavoratori, con particolare riferimento alla legge 300/1970 (Statuto dei lavoratori)….

Principio di proporzionalità… Nel commisurare la necessità di un sistema al grado di rischio presente in concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorre un'effettiva esigenza di deterrenza… In applicazione del principio di proporzionalità (v. anche art. 11, comma 1, lett. e), del Codice), anche l'eventuale conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo tempo necessario - e predeterminato - a raggiungere la finalità perseguita.
La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria…"

La lettura di queste prescrizioni parrebbe far propendere per l'esistenza di un trattamento illecito di dati in quanto la banca non si è attenuta, in particolare al rispetto del principio di proporzionalità che le imponeva di cancellare i dati al massimo dopo una settimana e, comunque, di non inquadrare con il mezzo visivo luoghi diversi dall'ingresso alla banca stessa da sorvegliare per scongiurare il rischio di rapine.
Può dunque la protezione del dato personale prevalere sulla necessità di accertamento del reato?

I POSSIBILI RIMEDI ALLA VIOLAZIONE DELL'ART. 11 T.U.

Abbiamo già parlato della sanzione dell'inutilizzabilità (che è l'aspetto più interessante) dei dati illegalmente raccolti, giungendo alla conclusione che – salva la nuova stesura dell'art. 240 c.p.p. – l'art. 11 difficilmente può fungere da parametro di valutazione per il giudice penale.

Tuttavia, il legislatore, sia per quanto riguarda il trattamento per ragioni di giustizia che per quello delle forze dell'ordine, non ha escluso l'applicazione dell'art. 143, legittimando, quindi, la possibilità di **reclamo** da parte dell'interessato [15]. Tale strumento, anche se non permette uno sbocco giurisdizionale, autorizza il Garante ad emettere un divieto di trattamento dei dati, la sospensione e il blocco.

Come possa farlo nei confronti dell'autorità giudiziaria, sinceramente, ci è difficile capire, ma resta il fatto che il T.U. ammette questa possibilità.

Infine, vi è da segnalare che il trattamento illecito dei dati può costituire reato, ai sensi dell'art. 167 T.U. [16].

Richiedendo la fattispecie il dolo specifico dell'ingiusto profitto, pare difficile che l'acquisizione "illegale" da parte della polizia giudiziaria, dell'autorità giudiziaria, ma anche dei privati, possa integrare gli estremi del reato previsto dall'art. 167 (da cui potrebbe discendere l'inutilizzabilità processuale, secondo una certa lettura dell'art. 191 c.p.p.).

---

[15] Art. 143: 1. Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento:

a) prima di prescrivere le misure di cui alla lettera b), ovvero il divieto o il blocco ai sensi della lettera c), può invitare il titolare, anche in contraddittorio con l'interessato, ad effettuare il blocco spontaneamente;

b) prescrive al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti;

c) dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera b), oppure quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati;

d) può vietare in tutto o in parte il trattamento di dati relativi a singoli soggetti o a categorie di soggetti che si pone in contrasto con rilevanti interessi della collettività.

2. I provvedimenti di cui al comma 1 sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti.

[16] Art. 167: 1. 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 sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro 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 uno a tre anni.

Quadro comparativo con la legislazione tedesca attinente la trattazione dei dati personali

Volendo fare una breve panoramica della legislazione europea, crediamo sia utile al fine di una valutazione comparatistica analizzare a grandi linee, la legislazione tedesca. Innanzitutto, nel codice di procedura penale (*Strafprozeßordnung*, StPO) sono state introdotte alcune norme che autorizzano e disciplinano il trattamento automatizzato dei dati personali.

Si segnalano, in primo luogo, i §§ 98a, 98b e 98c StPO. Questi paragrafi, introdotti con una legge del 1992[17] consentono la c.d. *Rasterfahndung*, ovvero il raffronto informatizzato «tra dati relativi a persone in possesso di caratteristiche presumibilmente corrispondenti a quelle del colpevole di un reato, e altri dati, al fine di escludere dal novero dei sospettati del reato determinate persone, ovvero di individuare persone che possiedono caratteristiche significative in relazione alle indagini» (§ 98° comma 2).

La misura è consentita solo per perseguire alcuni reati (particolarmente gravi) elencati uno ad uno (§ 98a), e soltanto quando non se ne possa proprio fare a meno, e cioè qualora, rinunciandovi, le indagini risulterebbero oltremodo difficoltose; essa va autorizzata, inoltre, dal giudice per iscritto (§ 98b comma 1); i dati cosi raccolti, infine, possono essere conservati e utilizzati in un altro procedimento penale, ma solo se questo ha per oggetto reati che avrebbero consentito di disporre la misura in prima battuta. L'ultima disposizione, il § 98c, consente più in generale il raffronto automatizzato di dati personali, raccolti nel corso di un procedimento penale, con dati memorizzati in altri procedimenti, anche di esecuzione penale o di prevenzione dei reati, al fine di accertare un reato (qualsiasi, stavolta), ovvero di risalire al luogo in cui si trovi una determinata persona.

Si segnalano, poi, le norme di cui ai §§ 163d, 163e e 163f della StPO:

a) il § 163d consente la memorizzazione in una banca dati di informazioni raccolte dalla polizia nel corso dell'attività di controllo alle frontiere, o nel corso della più generale attività di controllo; la memorizzazione è consentita, ancora una volta, solo se vi siano indagini in corso per reati specifici, indicati al primo comma del § 163d, e previa autorizzazione scritta da parte di un giudice; i dati vanno cancellati non appena non servano più nel procedimento interessato;

b) il § 163e autorizza la polizia giudiziaria a redigere annotazioni dell'attività di osservazione e pedinamento della persona sospettata, per accertare però reati di particolare gravità (non elencati), e sempre soltanto su autorizzazione scritta del giudice;

c) il § 163f consente l'osservazione per lunghi periodi (*Langfristige Obsevation*: per periodi superiori alle 24 ore, se continuativa, oppure superiori a due giorni, se non continuativa) della persona indagata, per perseguire reati di particolare gravità e solo se

[17] BR-Drs. 12/2720 del 4.6.1992.

diversamente le indagini risulterebbero particolarmente difficoltose; questa misura deve essere autorizzata per iscritto dal pubblico ministero.

Si tratta, in tutti questi casi, di norme che autorizzano la raccolta di dati personali direttamente nel processo penale. Quanto, invece, alla trasmissione di dati da e verso il processo, il quadro è, a grandi linee, il seguente. Per ciò che riguarda l'acquisizione di dati dall'esterno, i presupposti fissati dal *Bundesverfassungsgericht* nella decisione sul censimento erano, come si ricorderà, l'apposita previsione normativa (anche a mezzo di clausole generali), all'esito di bilanciamento degli interessi in gioco, e il rispetto del principio di chiarezza normativa. A questi criteri si è attenuto il legislatore tedesco, che è intervenuto sulla legislazione specifica disciplinando diverse ipotesi di trasmissione di dati: le leggi che regolamentano i più importanti settori dell'amministrazione, in cui normalmente si provvede alla raccolta autorizzata di dati personali, contengono, pressoché tutte, alcune disposizioni specifiche che stabiliscono a quali condizioni i dati possono essere trasmessi all'autorità giudiziaria, su richiesta di quest'ultima. Alcuni esempi: il codice sulla legislazione sociale (*Sozialgesetzbuch*, che disciplina tutta la materia del *welfare* tedesco, inclusa quella previdenziale) consente, al § 73 del suo libro X, la trasmissione dei dati raccolti dalle istituzioni del settore, alle autorità che procedono in un procedimento penale, solo se quest'ultimo abbia per oggetto delitti o altri reati di particolare rilevanza (il successivo § 78 prevede il vincolo di scopo, stabilendo che i dati potranno essere utilizzati esclusivamente per la specifica finalità per cui sono stati trasmessi, e che ne è vietata la successiva trasmissione a terzi); il codice della materia tributaria (*Abgabenordnung*), al suo § 393, disciplina un'ipotesi di *Zweckbindung*, disponendo che il pubblico ministero o il giudice i quali nel corso di un procedimento penale vengano a conoscenza di documenti fiscali, fatti o mezzi di prova che il contribuente abbia fornito all'autorità finanziaria, in adempimento di obblighi previsti dalle leggi tributarie, prima o nell'ignoranza dell'avvio del procedimento penale, non possano utilizzarli contro di lui per la repressione di un reato (fatti salvi i reati tributari e quei reati la cui repressione risponda a un pressante interesse pubblico).

Vi è poi una miriade di altre disposizioni, contenute in diverse leggi di settore, che disciplinano la trasmissione di informazioni all'autorità giudiziaria. Al punto che la dottrina segnala livelli di inflazione eccessivamente elevati, talvolta con rinvii e rimpalli da una disposizione all'altra, che rischiano di svuotare di ogni contenuto il diritto all'autodeterminazione informativa, impedendo alla persona interessata un'effettiva *Überschaubarkeit*, cioè un effettivo del controllo del percorso seguito dai propri dati, e consentendo altresì, nel fatti, un facile aggiramento del vincolo di scopo[18].

[18] Cfr. DUTTGE, *Was bleibt noch von der Wissenschaftsfreiheit? - Zur Hypertrophie des Datenschutzes*, in *Neue Juristische Wochenschrift*, 1998, p. 1616. Sui molti rimpalli e sulla sostanziale indecifrabilità delle disposizioni in materia di dati personali nel settore delle leggi finanziarie si veda L.GÖRES, *Kontenabfrage tritt vorläufig in Kraft – Nur ein Pyrrhussieg für den Gesetzgeber?*, in *Neue Juristische Wochenschrift*, 2005, fasc. 27, p. 1903. Già all'epoca della sentenza sul censimento, qualcuno aveva messo in guardia

Infine, sul versante opposto, quello della trasmissione ad altre autorità dei dati raccolti nell'ambito del procedimento penale, vanno segnalati almeno due provvedimenti. Il primo è il *Justizmitteilungsgesetz*, entrato in vigore nel 1997[19], e detta le regole per la comunicazione di informazioni relative a procedimenti giudiziari (non solo penali, ma anche civili e amministrativi) ad altre autorità, con riferimento, però, ai provvedimenti adottati nel corso o all'esito del procedimento giudiziario, più che ai singoli dati personali ivi raccolti.

Più interessante è pertanto l'altro importante intervento del legislatore tedesco: si tratta della legge di modifica al codice di procedura penale del 1999 (StVÄG 1999)[20], in vigore dall'agosto del 2000, che riscrive completamente (e sostanzialmente aggiunge) l'ottavo libro, l'ultimo, della StPO, in materia di trasmissione ad altre autorità giudiziarie, alla polizia, e ai privati, dei dati personali raccolti nel corso del procedimento penale. Il provvedimento è stato molto sollecitato dalla dottrina, che da lungo tempo segnalava l'assenza di una previsione legislativa per le molteplici ipotesi di trasmissione di dati provenienti dai procedimenti penali, e soprattutto per lo scambio di informazioni tra autorità giudiziaria e autorità di polizia. In particolare, la critica più forte si appuntava sul c.d. sistema INPOL: un sistema gestito dalla polizia tedesca, in cui venivano memorizzate indistintamente informazioni raccolte nel corso di procedimenti penali e dell'attività preventiva di polizia, al fine di potervi attingere, in futuro, per individuare il colpevole di eventuali reati, o ancora per l'attività preventiva, ovvero per altri scopi ancora, in ogni caso diversi da quelli propri del procedimento nel quale o per il quale erano state raccolte. Da più parti si denunciava che la memorizzazione, per un periodo indefinito, di dati derivanti dall'attività repressiva e da quella preventiva di polizia, mescolati tra loro e non più distinguibili per provenienza, nonché il successivo indistinto utilizzo, costituiva una palese violazione del vincolo di scopo, in carenza, peraltro, di una specifica previsione normativa[21]. L'assenza di un bilanciamento operato dal legislatore appariva, inoltre, particolarmente lesiva dell'*informationelle Selbstbestimmungsrecht*,
alla luce della circostanza che si trattava di dati in gran parte sensibili, la cui consultazione era accessibile a un numero elevatissimo di persone (tutti gli agenti di polizia)[22].

---

contro il rischio di inflazione legislativa connesso ai nuovi principi dettati dal *Bundesverfassungsgericht*: ROGALL, *Moderne Fahndungsmethoden*, cit., p. 12.

[19] Pubblicato sul *Bundesgesetzblatt* del 18 giugno 1997, parte I, p. 1430.

[20] Pubbicata sul *Bundesgesetzblatt* del 2 agosto 2000, parte I, p. 1253.

[21] Si veda SIEBRECHT, *Die polizeiliche Datenverarbeitung im Kompetenzstreit zwischen Polizei- und Prozeßrecht*, in *Juristenzeitung*, 1996, I, p. 711.

[22] La banca dati INPOL non era invece consultabile direttamente dall'autorità giudiziaria. Sul punto si veda J.WOLTER, *Datenschutz und Strafprozeß*, in *Zeitschrift für die gesamte Strafrechtswissenschaft*, 1995, p. 793, 795-796, che, prima ancora, aveva denunciato, in relazione alla stessa banca dati, la violazione della riserva di legge ritenuta costituzionalmente imposta dalla sentenza sul censimento: ID., *Heimliche und automatisierte Informationseingriffe wider Datengrundrechtsschutz*, in *Goltdammer's Archiv für Strafrecht*, 1988, p. 49.

A queste disposizioni (anche in forza, come si è visto, di espliciti rinvii) devono aggiungersi quelle dettate dalla legge di polizia (*Polizeigesetz*), la quale:

a) autorizza la creazione di banche dati di polizia, consentendo l'utilizzo dei dati personali in esse memorizzati per lo scopo per il quale i dati sono stati ottenuti, ovvero per altre finalità, se per perseguire quest'ultime avrebbe potuto ottenere quelle informazioni anche in prima battuta (§ 37 PolG);

b) autorizza la polizia a memorizzare e utilizzare i dati raccolti nel corso delle indagini preliminari anche a fini di prevenzione dei reati, ma a condizione che vi siano elementi concreti per ritenere che la persona indagata nel procedimento penale di provenienza possa commettere in futuro nuovi reati (§ 38 co. 1 PolG);

c) obbliga la polizia a controllare, a cadenze periodiche, se la conservazione dei dati sia ancora necessaria (§ 38 comma 2 PolG);

d) autorizza la polizia a pretendere la trasmissione di dati personali da altre autorità, pubbliche o private, al fine di raffrontarli con quelli contenuti nelle proprie banche dati, solo per perseguire reati di particolare gravità (§ 40 PolG).

d) autorizza la polizia a pretendere la trasmissione di dati personali da altre autorità, pubbliche o private, al fine di raffrontarli con quelli contenuti nelle proprie banche dati, solo per perseguire reati di particolare gravità (§ 40 PolG).

provvedimento di proscioglimento;

e) l'autorità che ha provveduto a memorizzare i dati deve verificare, a cadenze periodiche (individuate con precisione), se questi debbano essere cancellati (§ 489)

. In conclusione, la normativa del settore consente in ampia misura il trasferimento di informazioni da un'autorità all'altra, sia pure con alcune, ridotte, limitazioni dettate principalmente a salvaguardia del vincolo di scopo.

Il legislatore è intervenuto introducendo, ai §§ 474-495 della StPO, una dettagliata disciplina, che è impossibile, tuttavia, in questa sede, analizzare nella sua totalità. Si segnalano soltanto alcune norme fondamentali, senza pretese di esaustività:

a) si autorizza innanzitutto, in via generale, la creazione di banche dati da parte dell'autorità giudiziaria, in cui possono essere memorizzate le informazioni raccolte nel corso di ogni singolo procedimento penale, per l'utilizzo in futuri procedimenti (§ 483 co. 1);

b) se la memorizzazione avviene nelle banche dati della polizia, e unitamente a dati la cui memorizzazione è disciplinata dalle leggi di polizia, per il regime di utilizzo dei dati si fa riferimento alle norme dettate nel settore di competenza dell'autorità che provvede alla memorizzazione (§ 483 co. 3 e § 484 co. 4);

c) i dati memorizzati possono essere utilizzati anche per futuri procedimenti penali, se necessario per l'accertamento dei reati; ne è altresì consentita la trasmissione ad altre autorità, per le finalità connesse alla concessione di provvedimenti di grazia ovvero alla

cooperazione giudiziaria penale internazionale: in queste ipotesi l'utilizzo dei dati è consentito solo per lo scopo per cui gli stessi sono stati trasmessi (§§ 483 co. 2 e 487);

d) è vietato memorizzare i dati relativi alla persona indagata, quando nei suoi confronti venga pronunciato un provvedimento di proscioglimento;

e) l'autorità che ha provveduto a memorizzare i dati deve verificare, a cadenze periodiche (individuate con precisione), se questi debbano essere cancellati (§ 489).