MARIO G. LOSANO

LE POLIZIE E IL FLUSSO TRANSNAZIONALE DEI DATI PERSONALI NEI PROCESSI PENALI

SOMMARIO

1. La polizia invade il processo penale?

Il congresso del 1989 degli avvocati penalisti tedeschi era dedicato al tema « Stato di sicurezza e difesa penale ». Il concetto di « Stato di sicurezza » viene usato per indicare quella fase dello « Stato di diritto » e dello « Stato sociale » che si preoccupa di prevenire i reati. Ora, la prevenzione attuata con le tecnologie informatiche può soffocare le libertà fondamentali dei cittadini. La polizia accumula sempre più dati sui delinquenti potenziali (e cioè su qualunque cittadino), costruendo così progressivamente la figura di un reo, al cui completamento non manca che un particolare: la commissione del reato.

I penalisti vivono questa realtà su due versanti: come difensori, si ritrovano a dover valutare dati che la polizia ha raccolto, memorizzato o ricevuto da altre polizie; il processo stesso, a sua volta, fornisce alla polizia nuovi dati, che spesso vengono conservati in memoria senza tener conto dell'esito del processo stesso. Avremo modo di vederne alcuni esempi nella Parte II.

Questo scritto non affronta il problema della prevenzione alla luce delle nuove tecnologie, anche se queste ultime stanno già mutando alcuni aspetti della procedura penale. Il Ministero tedesco per la giustizia ha preparato un progetto di riforma della procedura penale che tiene conto dei problemi aperti dai sistemi informativi e che ha susci-

tato un dibattito così serrato, da rendere impossibile il riferirne qui in breve[1].

L'intersecarsi dei sistemi informativi della polizia giudiziaria e del resto della polizia provoca contaminazioni che esigono un ripensamento delle strutture organizzative esistenti. Non è detto che queste strutture debbano essere nuove. Il « Modello Basilea », ad esempio, risale ad una legge di Basel-Stadt del 1931, in base alla quale la polizia giudiziaria è nettamente separata dal resto della polizia. Solo la polizia giudiziaria può accedere ai dati memorizzati, in base al principio « I dati della giustizia vanno solo alla giustizia ». In Germania federale questa divisione non esiste e le commistioni si verificano.

Per questa ragione, dei cinque gruppi di lavoro del congresso, due erano dedicati ai problemi sollevati dalle banche di dati poliziesche in rapporto al processo penale. La già citata riforma del procedimento penale era al centro dell'attenzione del secondo gruppo, che si occupava del tema « Difesa penale e crescente peso della polizia dell'istruttoria a causa delle tecnologie dell'informazione »: purtroppo non è possibile qui approfondire questo argomento.

Il primo gruppo era dedicato al « Processo penale come mezzo per l'acquisizione di informazioni da parte dello Stato ». Infatti, quando svolge indagini, la polizia raccoglie e memorizza dati in vista del processo. Questi dati che fine fanno? Che diritto ha di fatto il cittadino di prendere visione o di chiederne la correzione? Come può il cittadino evitare conseguenze negative derivantigli dai dati memorizzati? La Germania ha infatti una « Legge federale per la protezione dei dati », la quale però non vincola gli organi di polizia.

I cinque relatori erano il garante dei dati del Land di Amburgo, il Presidente dei servizi di sicurezza di Amburgo[2], due avvocati bavaresi e io stesso, per i problemi dei flussi transnazionali dei dati personali.

Questo scritto comprende, nella prima parte, la relazione presentata al congresso di Colonia per illustrare la situazione normativa in Italia. Dopo aver accennato ai progetti di legge sulla privacy, analizzo la ratifica della convenzione di Strasburgo e le sue conseguenze sull'ordinamento giuridico italiano: in particolare, essa non sostituisce una legge sulla privacy. Tenendo conto della legge di riforma della polizia, esamino poi lo scambio di dati con le polizie straniere, cercando di definire anche la natura e la finalità dei dati raccolti, nonché le garanzie di cui essi godono. Infine propongo una convenzione internazionale per rendere omogeneo lo scambio di dati fra polizie.

[1] *Strafverfahrensänderungsgesetz 1988 (StVÄG 1988)*, pubblicato dalle Associazioni dei difensori penali, s.l., s.d., 205 pp.; contiene anche le critiche al progetto formulate dai penalisti (*Stellungnahme der Strafverteidigervereiningungen*, pp. 121-205).

[2] Il presidente di un Landesamt für Verfassungschutz corrisponde ad un alto dirigente dei Servizi di sicurezza democratica (SISDE) in Italia. La sua partecipazione ufficiale ad un congresso — e per di più in aperto contraddittorio con il suo antagonista, il garante dei dati — dimostra quanto diverso sia il rapporto fra apparato statale e società in Germania federale e in Italia.

La seconda parte propone al lettore italiano alcuni casi concreti, tuttora senza soluzione, di cittadini tedeschi alle prese con le polizie italiana e spagnola sulla base di segnalazioni provenienti dalla polizia tedesca. I problemi nascono, sul piano giuridico, dall'assenza di una legge sulla privacy nei due Stati mediterranei e, sul piano operativo, da una probabile minor efficienza delle due polizie mediterranee rispetto a quella tedesca. L'ultimo paragrafo si limita a ricordare che la liberalizzazione comunitaria del 1993 verrà sfruttata anche dalla criminalità organizzata: un eccesso di garantismo nei riguardi dell'opera di prevenzione delle polizie potrebbe fare il gioco proprio dei disonesti.

PARTE I: LO SCAMBIO DI DATI PERSONALI FRA LE POLIZIE NEL DIRITTO ITALIANO

2. I PROGETTI PER UNA LEGGE ITALIANA SULLA PRIVACY.

L'Italia e la Grecia continuano ad essere gli unici paesi della Comunità europea privi di un'organica legge sulla privacy, mentre Spagna e Portogallo hanno almeno incluso questo diritto fondamentale del cittadino nei loro testi costituzionali. I progetti presentati in Parlamento sono ormai tutti decaduti perché non discussi entro la fine della legislatura in cui furono presenti: se ne trova una descrizione dettagliata in un mio libro e nel documento in tedesco presentano alla Comunità Europea[3]. Un mio progetto di legge sulla privacy, predisposto nel 1987 su richiesta di un partito, si è perso nei meandri delle segreterie politiche e parlamentari ed è stato infine pubblicato su una rivista, come si conviene ad un prodotto professorale[4].

La legislazione italiana sulla protezione dei dati personali si riduce quindi ad alcune norme dello Statuto dei lavoratori e alla legge per il

[3] *Diritto pubblico dell'informatica*, Einaudi, Torino, 1986, pp. 189-220; *Die Italienische Gesetzenentwürfe über den Schutz personenbezogener Daten*, Statistiches Amt der Europäischen Gemeinschaften, Luxemburg, 1984, 16 pp. La versione francese è stampata nel volume: *Protection de la vie privé, informatique et progrès de la documentation statistique*, « Information de l'Eurostat », Numéro spécial, Office des publications officielles des Communautés européennes, Luxembourg, 1986, pp. 275-304.

[4] *Il computer di cristallo. Progetto di legge sulla protezione dei dati personali*, « Micromega », 1987, n. 1, pp. 159-177; ristampato in questa *Rivista*, 1987, 465.

riordinamento delle forze di sicurezza. Solamente quest'ultima riguarda direttamente il tema di questo congresso. Va sottolineato sin d'ora che si tratta di un « curiosum » legislativo, poiché, nell'ampia legge che regola il coordinamento delle forze di polizia, è stata inserita non tanto una « norma fugitiva », ma addirittura una « lex fugitiva ». Infatti gli articoli da 6 a 12 costituiscono una mini-legge per la protezione dei dati personali dagli abusi compiuti dalle polizie e dagli organi di sicurezza.

L'Italia viene così a trovarsi in una situazione paradossale rispetto agli altri paesi comunitari. Questi ultimi hanno quasi tutti una legge sulla privacy, che non si applica però alle forze di polizia ed ai servizi di sicurezza; l'Italia, invece, non ha una legge generale, ma regola invece proprio quelle banche che altrove restano in ombra. L'efficacia del controllo, naturalmente, è un discorso diverso.

D'altra parte, proprio nei giorni precedenti il congresso di Colonia, l'Italia ha ratificato la Convenzione del Consiglio d'Europa sulla protezione dei dati personali. È indispensabile chiedersi che cosa comporta questa novità nel panorama legislativo italiano.

3. L'Italia e la Convenzione del Consiglio d'Europa.

L'Italia aderì il 2 febbraio 1983 alla Convenzione del Consiglio d'Europa del 28 gennaio 1981, ma è riuscita a renderla operante, per lo meno sul piano formale, soltanto con la legge 21 febbraio 1989, n. 98, intitolata « Ratifica ed esecuzione della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 ». Otto anni di ritardo: non male. Si aggiunga che questa legge di febbraio venne pubblicata nel supplemento ordinario de « La Gazzetta Ufficiale » n. 66 del 20 marzo 1989. Questo spiega il fatto che la legge di ratifica sia di fatto passata inosservata.

« Habemus legem », annunciava una breve notizia pubblicata su una rivista informatica[5]. Ora, non è proprio sicuro che con questa ratifica sia nata la legge italiana sulla riservatezza. Nel bilanciamento tra i poteri dello Stato, infatti, la legge di ratifica è un'autorizzazione che il Parlamento concede al Presidente della Repubblica affinché ratifichi la convenzione. quindi l'art. 3 di questa legge non

[5] *Zerouno*, aprile 1989, p. 24.

deve trarre in inganno. Quando vi si legge che « la presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta ufficiale* », si deve intendere che dal 21 marzo 1989 il Presidente della Repubblica può dar corso alla ratifica della convenzione.

Ma tutta questa materia pare incontrare ostacoli continui. Una rivista specializzata descrive i retroscena che ne hanno accompagnato l'approvazione nell'aprile 1989 in modo giuridicamente impreciso ma sociologicamente illuminante:

« La legge di ratifica ha avuto l'effetto di una autentica bomba presso l'Ufficio legislativo del Ministero di Grazia e Giustizia dove un gruppo di lavoro presieduto da Giuseppe Mirabelli aveva da poco ultimato l'elaborazione di un nuovo schema di legge sulla cosiddetta « privacy informatica », a cui la legge che ratifica la convenzione di Strasburgo si riferisce.

Il problema sollevato dai magistrati ed esperti che hanno lavorato a tale disegno di legge [...] è di natura squisitamente tecnica. È noto infatti che lo strumento di ratifica di una convenzione è costituito da una legge nazionale del paese che ha sottoscritto la convenzione medesima sulla materia da questa considerata. Nella specie, questa legge, strettamente intesa, ancora in Italia non è stata emanata: mancherebbe quindi lo strumento di ratifica specificamente previsto (cfr. artt. 22-23-24) dalla convenzione in questione.

« Abbiamo tentato di bloccare questa approvazione senza riuscirci — ha riferito con sommo rammarico un autorevole esponente del gruppo di lavoro del Ministero di Grazia e Giustizia. Pare che ci siano dietro ragioni di ordine internazionale o quantomeno diplomatico. Certo è che un giudice non potrebbe avere alcun potere di applicazione della convenzione in un caso concreto. Obbligatorietà ed efficacia dunque a futura memoria, cioè per quando una legge nazionale ci sarà? Troppo poco! ».

[...] Tragica sarebbe addirittura l'eventualità che il Consiglio della CEE respingesse il deposito della ratifica rilevando che è sfornito del relativo strumento (vale a dire della legge formale dello Stato aderente) »[6].

L'unica affermazione chiara è quella dell'« autorevole esponente del gruppo di lavoro » sul tentativo non riuscito di bloccare la legge di autorizzazione alla ratifica. In particolare, è oscuro il motivo per cui si sia tentato di bloccare la ratifica di una convenzione sottoscritta otto anni prima, quando la sua applicazione richiede necessariamente l'emanazione di una legge nazionale cui sta lavorando il gruppo stesso.

[6] Nino Catania, *Legge imperfetta ma diplomatica*, « Anfov News. Periodico dell'associazione nazionale fornitori di videoinformazione », VII, febbraio-giugno 1988, n. 29, p. 48.

Che forze frenanti siano ancor oggi all'opera è dimostrato anche dal fatto che, alla metà dell'ottobre 1989, non ha ancora avuto luogo la ratifica da parte del Presidente della Repubblica.

a) *La Convenzione e il diritto interno italiano*. Supponiamo, in attesa di conferma, che la ratifica presidenziale abbia luogo in tempi stretti. L'art. 2 della legge 98/1989 stabilisce che « piena ed intera esecuzione è data alla convenzione » e specifica il termine della sua entrata in vigore: « a decorrere dalla sua entrata in vigore in conformità a quanto disposto dall'art. 22 della convenzione stessa ». Quest'ultimo indica come data di entrata in vigore « il primo giorno del mese successivo allo scadere del termine di tre mesi dalla data del deposito dello strumento di ratifica ». Supponendo dunque che la ratifica presidenziale italiana venga depositata presso il Segretario Generale del Consiglio d'Europa prima della fine dell'aprile 1989, l'entrata in vigore si avrà dal 1° agosto 1989. (Però, come abbiamo detto, nei fatti questa ratifica presidenziale non aveva ancora avuto luogo al 15 ottobre 1989).

Ma l'Italia avrà una legge sulla privacy dopo la ratifica presidenziale? Ho ancora dei dubbio, poiché la convenzione diverrà legge interna, ma richiederà — a mio giudizio — l'emanazione di una normativa interna specificamente rivolta alla protezione dei dati personali. Così com'è, infatti, la convenzione non è un testo direttamete applicabile. Né intende esserlo; intende invece dettare le linee generali di una legislazione interna sulla privacy. Questo giudizio si fonda sull'art. 4 della convenzione: « [1] Ogni Parte adotta, nel suo diritto interno, le misure necessarie per dare effetto ai principi fondamentali per la protezione dei dati enunciati nel presente capitolo. [2] Dette misure debbono essere adottate al più tardi al momento dell'entrata in vigore della presente convenzione nei suoi confronti ». Ritornando ai termini individuati sopra, questo significa che l'Italia dovrebbe approvare una legge sulla privacy entro il 1° agosto 1989.

Se così non fosse, tutta la normativa entrata in vigore attraverso la convenzione sarebbe di fatto inoperante in quanto priva di sanzioni, poiché l'art. 10 delega giustamente questo punto fondamentale al singolo Stato: « Ogni parte si impegna a fissare sanzioni e ricorsi adeguati, relativi alle violazioni delle disposizioni del diritto interno di esecuzione dei principi fondamentali per la protezione dei dati ». Inoltre la convenzione non può determinare quale autorità interna applicherà queste disposizioni e, di conseguenza, con l'art. 13, comma 2, lett. *a*), rimette anche questa nomina allo Stato contraente: « ogni Parte designa uno o più autorità di cui comunica nome ed indirizzo al Segretario Generale del Consiglio d'Europa ».

All'inevitabilità di una normativa interna rinviano anche altre disposizioni della convenzione.

L'art. 6 vieta che vengano elaborati automaticamente i dati personali più sensibili (opinioni politiche, razza ecc.) e quelli relativi alle condanne penali « a meno che il diritto interno non preveda garanzie adatte ». In Italia, il Casellario giudiziale è automatiz-

zato, cosicché la sua esistenza risulterebbe incompatibile con questa norma.

I capisaldi della protezione dei dati individuali sono contenuti negli artt. 5, 6 e 8. Tuttavia il diritto interno può derogarvi « qualora tale deroga, prevista dal diritto della Parte, costituisca una misura necessaria in una società democratica » (art. 9).

Qui la norma si apre a qualsiasi uso ed abuso, perché nessuna società negherà di essere democratica (anzi, addurrà a riprova di ciò proprio le adesioni più sospettamente plebiscitarie). Inoltre solo lo Stato interessato è in grado di dire se la limitazione introdotta è o non è necessaria.

Un ulteriore elemento apparentemente negativo è dovuto ad un errore della traduzione non ufficiale, che accompagna il testo della legge 98/1989 insieme con il testo francese (che, con quello inglese, è l'unico a far fede). Se la deroga fosse fondata sul « diritto » della Parte, qualsiasi atto amministrativo abrogherebbe questa convenzione. Il testo originario dice più limitativamente « loi » (e non « droit »); e mi pare ovvio che qui il termine « legge » va inteso in senso formale.

b) *La Convenzione e la circolazione internazionale dei dati.* Tutto il Capitolo III è dedicato al movimento dei dati oltre frontiera, ma si riduce ad un unico articolo, il 12, di cui mi pare che vada qui sottolineato il comma 2: « Una parte non può, ai soli fini della protezione della vita privata, proibire o condizionare ad un'autorizzazione speciale il movimento oltre frontiera di dati a carattere personale destinati ai territori di un'altra Parte ». Ritorna qui il principio generale sancito nel preambolo della convenzione, che è favorevole alla libera circolazione dell'informazione (anche se in una forma non chiara, che unifica dati personali e informazioni, ad esempio, giornalistiche). I limiti a questa libera circolazione delle informazioni sono dettati soltanto dal criterio della reciprocità, quando cioè i dati dovrebbero andare a Stati che non offrano garanzie equivalenti a quelle dello Stato d'origine.

Anche il capitolo VI, dedicato all'assistenza reciproca, si limita agli aspetti più formali di essa. Quando lo Stato avrà nominato l'autorità garante dei dati personali, questa entrerà in contatto con le autorità omologhe degli altri Stati firmatari per chiedere e ricevere informazioni. Ma sul contenuto di queste informazioni l'art. 2, lett. *b)* è molto chiaro; « adotterà conformemente al suo diritto interno [...] tutte le misure adeguate per fornire informazioni di fatto relative ad una data elaborazione effettuata sul suo territorio, *ad eccezione tuttavia dei dati di carattere personale oggetto di tale elaborazione* ».

Le norme sui residenti all'estero contengono un divieto di trasmissione di dati che potrà suscitare qualche problema di applicazione. L'art. 15, comma 3 dice: « in nessun caso un'autorità designata sarà autorizzata a presentare [...] una domanda di assistenza in nome di una persona interessata che sia residente all'estero, di

sua propria iniziativa e senza il consenso espresso di detta persona ». L'autorità di cui qui si parla è quella del « garante dei dati ». Ora, è stato correttamente osservato che « questa norma può suscitare qualche perplessità » in merito alle sue applicazioni nel campo dei rapporti giudiziari, quando si presenti il bisogno di una richiesta di informazioni su persone giuridicamente incapaci o su imputati o testimoni contumaci[7].

4. Lo scambio di dati con polizie anche straniere nel diritto vigente italiano.

Per migliorare la lotta alla criminalità organizzata, nel 1981 venne approvata una legge sul coordinamento delle forze di polizia[8], al cui interno — dall'art. 6 al 12 — si trova una minilegge sulla privacy. Il Dipartimento di pubblica sicurezza opera nell'ambito del Ministero degli interni che, tra i vari uffici e direzioni centrali, dispone anche di un Ufficio per il coordinamento e la pianificazione, cui è dedicato per intero l'art. 6. È su di esso che deve concentrarsi la nostra analisi, poiché esso costituisce il fulcro operativo intorno a cui ruota l'intera normativa dei restanti articoli sulla protezione dei dati personali.

Per chiarire i limiti entro cui può essere consentito lo scambio transfrontaliero di dati bisogna individuare in queste norme — che sono legislativamente ben formulate — tre elementi fondamentali: *a*) che cosa può essere lecitamente raccolto ed elaborato; *b*) a che fini tassativi possono essere raccolti i dati così individuati; *c*) a quali condizioni possono essere trasmessi a polizie straniere i dati lecitamente raccolti per i fini consentiti. La legge fornisce una risposta per ciascuno di questi tre quesiti.

a) *Quali dati si possono raccogliere.* La legge definisce con precisione all'art. 7 i dati genericamente indicati all'art. 6, lett. *a*). Essi « devono riferirsi a notizie risultanti da documenti che comunque siano conservati dalla pubblica amministrazione o da enti pubblici, o risultanti da sentenze o provvedimenti dell'autorità giudiziaria o da

[7] *La convenzione europea sulla protezione dei dati*, in *Riv. dir. eur.*, 1984, p. 15.

[8] Legge 1° aprile 1981, n. 121, *Nuovo ordinamento dell'amministrazione della pubblica sicurezza.* Esso va integrato con il decreto del Presidente della Repubblica, 3 maggio 1982, n. 378, intitolato *Regolamento concernente le procedure di raccolta, accesso, comunicazione, correzione, cancellazione ed integrazione dei dati e delle informazioni registrati negli archivi magnetici del centro di elaborazione dati di cui all'art. 8 della legge 1° aprile 1981, n. 121.*

atti concernenti l'istruzione penale acquisibili ai sensi dell'art. 165-*ter* del codice di procedura penale[9] o da indagini di polizia ». Non possono invece essere raccolti i dati sensibili su razza, religione, opinione politica o sindacale ecc.

Il comma 3 dello stesso articolo prevede che le informazioni bancarie possano essere acquisite « nei limiti richiesti da indagini di polizia giudiziaria e su espresso mandato dell'autorità giudiziaria, senza che possa essere opposto il segreto da parte degli organi responsabili delle aziende di credito o degli istituti di credito di diritto pubblico ».

I dati raccolti fuori da questi campi — la cui indicazione va ritenuta tassativa — espongono il funzionario alle sanzioni previste da questa legge, sempre che non configurino reati più gravi.

b) *La finalità della raccolta dei dati personali.* L'art. 6 elenca sette funzioni affidate all'Ufficio per il coordinamento, tra le quali due sono rilevanti per individuare i fini cui deve attenersi la raccolta dei dati personali. Tra questi fini v'è la « classificazione, analisi e valutazione delle informazioni e dei dati che devono essere forniti anche dalle forze di polizia in materia di tutela dell'ordine, della sicurezza pubblica e di prevenzione e repressione della criminalità [...] (lett. *a*). Questi dati possono venir trasmessi all'estero nell'ambito del « mantenimento e sviluppo delle relazioni comunitarie e internazionali » (lett. *g*), di cui ci occuperemo al punto seguente.

La determinazione delle finalità della raccolta è fondamentale, perché essa condiziona la circolazione dell'informazione, come si vedrà nel par. 4, lett. *a*).

È di fronte a questo articolo che l'interprete incontra le massime difficoltà, anche perché non esistono casi concreti cui richiamarsi.

[9] Questo articolo è stato aggiunto al cod. proc. pen. dall'art. 4 del d.l. 21 marzo 1978, n. 59 conv., con modif. nella legge 18 maggio 1978, n. 191; v. anche art. 8 d.l. 15 dicembre 1979, n. 625. Ecco il testo dell'art. 165-*ter* cod. proc. pen.: « Il Ministro dell'interno, direttamente o per mezzo di ufficiali di polizia giudiziaria, appositamente delegati, può chiedere all'autorità giudiziaria competente copie di atti processuali e informazioni scritte sul loro contenuto, ritenute indispensabili per la prevenzione dei delitti non colposi previsti dai capi I e II del titolo I del libro II del codice penale (241-293 cod. pen.) e dei delitti indicati negli artt. 306, 416-*bis*, 422, 423, 426, 428, 432, comma 1, 433, 438, 439, 575, 628, comma 3, 629, comma 2, e 630 dello stesso codice, nonché dei delitti previsti dagli artt. 1 e 2, comma 1, della legge 20 giugno 1952, n. 645, e successive modificazioni e dall'art. 1, comma 5, del d.l. 4 marzo 1976, n. 31, convertito nella legge 30 aprile 1976, n. 159, come sostituito dall'art. 2 della legge 23 dicembre 1976, n. 863. Eguale richiesta può essere fatta per la raccolta e l'elaborazione dei dati da utilizzare in occasione delle indagini per gli stessi delitti.
L'autorità giudiziaria può trasmettere le copie e le informazioni di cui al comma precedente anche di propria iniziativa; nel caso di richiesta deve provvedere entro cinque giorni.

Le copie e le informazioni acquisite ai sensi dei commi precedenti sono coperte dal segreto d'ufficio.

Se l'autorità giudiziaria ritiene di non poter derogare al segreto di cui all'art. 307 emette decreto motivato di rigetto ».

La nozione di « ordine pubblico » può comprendere anche la forma istituzionale dello Stato e legittimare raccolte a tappeto di dati sensibili (ordine pubblico in senso costituzionale). Può invece limitarsi alla conservazione del diritto positivo dello Stato, nel qual caso l'ambito di raccolta dei dati è più limitato. Sui problemi sollevati da questi concetti indefiniti ritornerà l'ultimo paragrafo.

c) *La trasmissione di dati personali a polizie straniere*. Il comma 4 e 5 dell'art. 6 entrano nel vivo del flusso trasnazionale dei dati: « [4] Possono essere altresì acquisite le informazioni e i dati di cui all'art. 6 in possesso delle polizie degli Stati appartenenti alla Comunità Economica Europea e di quelli di confine, nonché di ogni altro Stato con il quale siano raggiunte specifiche intese in tal senso. [5] Possono inoltre essere comunicate alle polizie indicate nel precedente comma le informazioni e i dati di cui all'art. 6, che non siano coperti da segreto istruttorio ».

Il testo di legge istituisce anche un Centro Elaborazione Dati (art. 8), che fa capo all'Ufficio di coordinamento previsto all'art. 5, al fine di elaborare i dati indicati all'art. 6, lett. *a*), ed anche di provvedere « alla loro comunicazione ai soggetti autorizzati, indicati nell'art. 9, secondo i criteri e le norme tecniche fissati ai sensi del comma seguente ». Lo strumento tecnico per lo scambio di informazioni è quindi l'elaboratore.

5. Le garanzie sui dati memorizzati.

Delimitato così il campo di che cosa si può raccogliere, dei fini per cui lo si può raccogliere e di chi può esserne portato a conoscenza nelle polizie estere, resta da vedere come viene garantito da abusi interni il cittadino, titolare dei dati memorizzati. Occorre quindi fissare, anche qui tassativamente: *a*) chi può accedere ai dati memorizzati; *b*) quale autorità può svolgere controlli in un settore necessariamente coperto da segretezza; *c*) quali sanzioni sono previste per chi viola la legge, e con quale procedura vengono irrogate.

a) *Chi è autorizzato all'accesso ai dati*. Le forze di polizia, gli ufficiali di pubblica sicurezza ed i funzionari dei servizi di pubblica sicurezza possono accedere ai dati memorizzati, mentre l'autorità giudiziaria può accedervi soltanto « ai fini degli accertamenti necessari per i procedimenti in corso e nei limiti stabiliti dal codice di procedura penale » (art. 9). Fuori da questi casi, è vietata la circolazione dei dati all'interno della pubblica amministrazione[10]. Inoltre « è co-

[10] L'art. 9 vieta la circolazione di queste informazioni « fuori dai casi indicati al comma 1 del presente articolo »; poiché il comma 1 si riferisce a polizie e servizi di sicurezza, mentre il secondo si riferisce ai magistrati, credo che il divieto vada riferito ad entrambi i commi.

munque vietata ogni utilizzazione delle informazioni e dei dati predetti per finalità diverse da quelle previste dall'art. 6, lett. *a* ».

b) *L'autorità di controllo*. La legge italiana fissa precisi limiti ai dati che possono essere raccolti, conosciuti e trasmessi; inoltre prevede esplicitamente lo scambio di dati personali con altre polizie. Ma come è possibile verificare se i funzionari si attengono a queste disposizioni?

In assenza di una legge sulla riservatezza — la quale d'altronde tende ad escludere questi settori dello Stato dal controllo del garante dei dati — l'art. 10 affida il controllo sul Centro Elaborazione Dati al Comitato parlamentare per la vigilanza sui servizi di sicurezza, istituto all'art. 11 dalla legge 24 ottobre 1977, n. 801[11]. Esso può compiere « periodiche verifiche dei programmi, nonché di dati e informazioni casualmente estratti e forniti senza riferimenti nominativi ». Data la natura tecnica di questi controlli, esso « può farsi assistere da esperti scelti tra i dipendenti delle camere o del Ministero dell'Interno ».

Se in un procedimento giurisdizionale o amministrativo risulta che il centro detiene dati erronei o illegali, l'autorità ne informa il Comitato parlamentare affinché proceda alle opportune correzioni. Se invece — sempre nel corso di un procedimento — è un cittadino ad impugnare dati che lo riguardano, l'istanza di correzione o cancellazione va presentata al Tribunale penale, nel cui circondario si celebra il processo in cui è emerso il dato contestato. Il Tribunale penale ordina l'eventuale cancellazione o correzione con un ordinanza che viene trasmessa anche al Comitato parlamentare e contro cui è possibile il ricorso in Cassazione.

[11] La legge n. 801/1977 è intitolata *Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato*; l'art. 11 è così formulato: « Il Governo riferisce semestralmente al Parlamento, con una relazione scritta, sulla politica informativa e della sicurezza, e sui risultati ottenuti.

Un Comitato parlamentare costituito da quattro deputati e quattro senatori nominati dai Presidenti dei due rami del Parlamento sulla base del criterio di proporzionalità, esercita il controllo sull'applicazione dei principi stabiliti dalla presente legge.

A tale fine il Comitato parlamentare può chiedere al Presidente del Consiglio dei Ministri e al Comitato interministeriale di cui all'art. 2 informazioni sulle linee essenziali delle strutture e dell'attività dei Servizi e formulare proposte e rilievi.

Il Presidente del Consiglio dei Ministri può opporre al Comitato parlamentare, indicandone con sintetica motivazione le ragioni essenziali, l'esigenza di tutela del segreto in ordine alle informazioni che a suo giudizio eccedono i limiti di cui al comma precedente.

In questo caso il Comitato parlamentare ove ritenga, a maggioranza assoluta dei suoi componenti, che l'opposizione del segreto non si sia [sic] fondata, ne riferisce a ciascuna delle Camere per le conseguenti valutazioni politiche.

I componenti del Comitato parlamentare sono vincolati al segreto relativamente alle informazioni acquisite e alle proposte e ai rilievi formulati ai sensi del comma 3. Gli atti del Comitato sono coperti dal segreto ».

c) *Le sanzioni.* Veniamo così alle sanzioni per i comportamenti illeciti. « [1] Il pubblico ufficiale — si legge all'art. 12 — che comunica o fa uso di dati ed informazioni in violazione delle disposizioni della presente legge, o al di fuori dei fini previsti dalla stessa, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a tre anni. [2] Se il fatto è commesso per colpa, la pena è della reclusione fino a sei mesi ». La norma penale è in bianco, dal momento che la determinazione dei reati cui ricollegare le sanzioni dipende dall'interpretazione degli altri articoli di questa legge.

Si delineano due fattispecie. Nella prima, il pubblico ufficiale comunica o fa uso di dati fuori dai limiti tracciati dalla legge (che sono sintetizzati nel già citato art. 6, lett. *a*): « classificazione, analisi e valutazione delle informazioni e dei dati ecc. »). Ad esempio, memorizza dati che gli pervengono da lettere anonime, da intercettazioni telefoniche o postali non riconducibili a nessuna delle attività previste dall'art. 7, che elenca tassativamente le fonti da cui possono provenire le informazioni memorizzate. Ovvero memorizza dati di cui è espressamente vietata la raccolta, come quelli sull'affigliazione politica o sulla razza di una persona.

Nella seconda fattispecie, il reato consiste nel fare uso dei dati nei casi previsti dalla legge, ma per fini diversi. Ad esempio, il funzionario comunica dati legalmente acquisiti nella lotta al terrorismo per informare un partito politico della posizione equivoca, in cui viene a trovarsi un suo iscritto, consentendone così un preventivo allontanamento (che potrebbe poi risultare infondato).

6. Proposte per una legislazione futura.

Una futura regolamentazione dello scambio di dati personali tra polizie deve presentarsi come una normativa che regoli questo scambio, senza ostacolarlo inutilmente. Una normativa eccessivamente garantista (e quindi troppo limitativa per le forze di polizia) nuocerebbe al cittadino in due modi. Da un lato, renderebbe meno efficace l'azione della polizia, che io considero nelle sue grandi linee un grande servizio al cittadino. Dall'altro, potrebbe indurre qualche settore delle polizie a sdoppiare le banche di dati, istituendone una da esibire alla Commissione parlamentare ed un'altra ad usare per i « dirty tricks ». Bisogna essere realisti nel valutare sia le esigenze delle polizie, sia le difficoltà di controllo — tecniche ed organizzative — delle autorità esterne. Cercherò di indicare brevemente alcuni degli elementi fra cui la futura legge dovrebbe cercare un difficile punto di equilibrio.

Anzitutto va distinta la repressione dalla prevenzione. Se il reato è stato commesso e si è in presenza di un mandato di cattura internazionale, pochi dubbi possono esistere sullo scambio di informazioni tra polizie di Stati diversi. Qui esistono regole procedurali già ben definite e collaudate.

Il vero problema è lo scambio di informazioni per la prevenzione di un reato. Qui si indaga su un reato che il controllato non ha ancora commesso, anche se può averne commessi altri. Entrano in gioco valutazioni sulla pericolosità sociale dell'individuo, spesso diverse da Stato a Stato. Se si intende il concetto di ordine pubblico in senso lato (come acennavo al par. 3, lett. *b*), il confine tra libertà di espressione e prevenzione di reati politici diviene labile, e varia da Stato a Stato.

Penso ad uno Stato rigido, come la Germania federale, dove esiste un'applicazione spesso troppo zelante del « Berufsverbot ». Penso all'Italia, Stato non flessibile, ma pantagruelico; e tollerante non per civiltà, ma per debolezza. Lo scambio di dati può dar luogo a malintesi dannosi per il cittadino, specialmente se i « dati » sono in realtà « valutazioni ».

Quest'espressione compare sia nell'art. 2 della legge istitutiva dell'Ufficio Criminale Federale (BKA), e viene espressamente richiamata in uno dei documenti forniti al congresso, sia nell'art. 6, lett. *a*), della legge italiana. Se la comunicazione varca la frontiera recando una valutazione, in un contesto culturale diverso questo può caricarsi di significati diversi da quelli consueti nel paese d'origine. Ma alle differenze culturali si aggiungono anche le differenze giuridiche. Proviamo ad immaginare qualche possibile caso concreto.

Se una polizia straniera chiede a quella italiana un dato personale che non rientra tra quelli legittimamente raccoglibili, la richiesta va respinta. Se il dato venisse — nonostante tutto — raccolto e trasmesso, il funzionario si esporrebbe alla sanzione prevista dalla legge italiana. L'avvocato del titolare del dato dovrebbe far valere questa situazione davanti al tribunale straniero.

Nel caso inverso, potrebbe verificarsi che la polizia italiana ricevesse — tra le altre — anche informazioni incompatibili con la legge nazionale. In questo caso dovrebbe memorizzare soltanto i dati leciti, cancellando gli altri.

Questi casi sono concreti soltanto fino a un certo punto, poiché molte situazioni di fatto inducono a spingere la trasmissione dei dati anche oltre i limiti legali. Nel primo caso, se la polizia italiana opponesse troppi rifiuti di origine legale alle richieste straniere, rischierebbe di provocare un analogo comportamento come ritorsione. E ne soffrirebbe la collaborazione tra le polizie. Nel caso delle informazioni che giungono in Italia e che si rivelano soltanto in parte in armonia con la legislazione interna, il funzionario può non memorizzarle, ma ormai « le sa » (ed è facile che sia tanto cortese da comunicarle al collega interessato).

Sul piano tecnico, poi, bisogna vedere come è organizzato il programma del centro elettronico: ma è certo che ormai l'informazione straniera sempre più spesso arriva per via informatica e passa quindi direttamente da un elaboratore ad un altro. Si pone allora un sottile quesito che lascio volentieri ai penalisti: il reato si con-

suma con l'arrivo nell'elaboratore dell'informazione straniera illecita per il diritto interno? Oppure bisogna attendere che essa venga inclusa nella banca di dati, ammesso che questa sia logicamente separata dal resto? E c'è reato (e di chi?) se i dati attraverso la rete vengono immessi nella banca di dati da un programma apposito, per rendere più rapidamente disponibile il dato a tutti i terminali? Cercare di regolare questi problemi sul piano tecnico mi pare un'impresa disperata.

La soluzione potrebbe invece essere offerta da un migliore coordinamento giuridico. Il Consiglio d'Europa o la Comunità Europea potrebbe ripetere in questo campo l'attività di guida già svolta per le leggi sulla privacy. Se una convenzione determinasse tassativamente i dati trasmissibili da polizia a polizia e, altrettanto tassativamente, le eventuali eccezioni, si potrebbero eliminare le disparità illustrate poc'anzi.

Per alcuni aspetti mi sembra che questo modo di procedere ricalchi lo schema seguito, negli anni passati, dalle leggi sulla privacy. Queste ultime hanno il valore del patto sociale tra lo Stato informatizzato e il cittadino titolare dei dati; e sono state rese necessarie dal numero crescente di banche di dati. Analogamente, in questi anni assistiamo a una crescente collaborazione tra le polizie per la lotta al terrorismo, ai narcotrafficanti e alla criminalità organizzata. Forse è giunto il momento di regolare — tenendo conto di tutte le sue peculiarità — anche quell'ambito della memorizzazione e diffusione dei dati personali che le classiche leggi sulla privacy avevano lasciato da parte.

Il primo passo potrebbe essere una convenzione internazionale, cui aderiscano anzitutto i paesi uniti non tanto dalla geografia economica o politica, quanto dalla geografia del crimine, che segue spesso una sua mappa particolare.

PARTE II: ESEMPI DI SCAMBIO DI DATI PERSONALI FRA POLIZIE DELLA COMUNITÀ EUROPEA

7. I DATI DELLA POLIZIA NEL PROCESSO PENALE: LA SITUAZIONE ATTUALE NELLA GERMANIA FEDERALE.

Dopo l'analisi delle norme italiane sul flusso transnazionale dei dati personali, nel precedente paragrafo abbiamo immaginato alcuni possibili casi di applicazione o di violazione delle norme esistenti, al verificarsi di un flusso transnazionale di dati. È giunto ora il momento di passare dai casi possibili ai casi reali.

Mi limiterò ad alcuni casi di flusso transnazionale di dati fra Stati che non hanno una legge sulla privacy e Stati che, invece, l'hanno: può quindi essere utile fare anzitutto il punto della situazione tede-

sca, caratterizzata da una normativa complessa e da una sua applicazione pluriennale. Nel paragrafo successivo risulterà più agevole la lettura dei documenti su alcuni casi relativi al flusso dei dati personali della Germania federale verso l'Italia e la Spagna, dove — non esistendo una normativa organica sulla protezione dei dati personali — le polizie fanno quello che possono e, talvolta, quello che vogliono.

La situazione giuridica tedesca, in questo campo, oscilla fondamentalmente tra due poli: da un lato, la *legge federale per la protezione dei dati* (emanata nel 1977 e già da tempo oggetto di proposte di riforma), che nega al cittadino un diritto a chiedere informazioni sui propri dati memorizzati dalla polizia; dall'altro, la sentenza del Tribunale costituzionale federale del 15 dicembre 1983, che — troncando le controversie sull'ammissibilità o meno di un censimento molto, anzi troppo curioso — stabilisce un « diritto all'autodeterminazione informatica del cittadino »[12]. Nel primo caso, prevale l'attenzione per il lavoro della polizia, mentre nel secondo l'accento è posto sui diritti del cittadino. Il dibattito durante il congresso del 1989 dei penalisti tedeschi tentava di individuare un possibile punto di equilibrio fra queste due esigenze spesso in contrasto. In assenza di una precisa normativa in proposito, anche la giurisprudenza tedesca oscilla a favore ora dell'uno, ora dell'altro principio, pur manifestando negli ultimi tempi una tendenza a favore dell'esclusione del diritto di accesso da parte del cittadino ai propri dati detenuti dalla polizia.

A favore del cittadino si schiera, ad esempio, il tribunale di Francoforte con una sentenza del 1987[13]. Il fatto è il solito: un cittadino chiede alla polizia la cancellazione di suoi dati personali, la quale rifiuta. La massima della sentenza afferma:

« Dopo la "Sentenza sul censimento" del Tribunale costituzionale federale, l'art. 81, lett. *b*), StPO non costituisce più un sufficiente fondamento giuridico per conservare dati (in questo caso, documenti investigativi) con finalità di polizia preventiva.

Poiché nel Land dell'Assia manca una legge locale che autorizzi la conservazione di documenti investigativi a scopo di prevenzione, la conservazione di detti documenti è illecita e, di conseguenza, l'interessato ha diritto alla loro distruzione[14] ».

[12] Se ne veda il testo, ad esempio, in *NJW*, 1984, pp. 419 ss.

[13] Verwaltungsgericht Frankfurt/M., Urteil v. 18 febbraio 1987, in *Der Strafverteidiger*, 1987, p. 336 ss.

[14] *Op. cit.*, p. 336. L'art. 81, lett. *b*), del cod. proc. pen. tedesco-federale dice: « Se è necessario per lo svolgimento del processo *o per finalità di indagine*, possono essere prese impronte digitali e fotografie anche contro la sua volontà, nonché misurazioni e misure analoghe ». Il Tribunale costituzionale federale si riferisce esplicitamente alla seconda alternativa, qui riprodotta in corsivo.

Nel testo della sentenza si osserva che la decisione della Corte Costituzionale non sancisce un diritto illimitato all'autodeterminazione informatica, ma esige che i limiti a questo diritto vengano indicati con precisione da una legge. Ora, al momento della stesura della sentenza (ed ancora oggi) esistono disposizioni interne che possono fornire le linee direttrici per una futura legislazione, ma non esiste ancora la legislazione stessa. Trattandosi di un diritto fondamentale del cittadino — del diritto cioè al libero sviluppo della sua personalità — secondo la magistratura di Francoforte la polizia deve accettare la richiesta di cancellazione dei dati.

Invece una sentenza del tribunale di Colonia, nel 1988, si muove nella direzione contraria, che sembra quella seguita dalla maggioranza dei tribunali tedeschi[15]. In questo processo, la richiesta di accesso ai dati venne rivolta da un cittadino ai servizi di sicurezza (Verfassungschutz), ma la pretesa fu ritenuta infondata per due ragioni: perché la *legge federale sulla protezione dei dati* (BDSG) prevede che gli organi di sicurezza non siano tenuti a fornire queste informazioni (art. 13, comma 2) e perché i dati in questione erano stati raccolti in modo lecito. Il Tribunale di Colonia rimise quindi alla decisione degli stessi servizi di sicurezza la concessione dell'accesso ai dati, dal momento che la BDSG non li obbliga a negare l'informazione. Quest'ultima va obbligatoriamente fornita soltanto se il cittadino ha « un interesse legittimo all'informazione, da provare specificamente. Ciò si verifica quando l'interessato può essere o è stato danneggiato, ovvero limitato nei diritti della sua personalità, dall'uso effettivo o prospettato dei suoi dati ».

Sul piano giuridico non sembra esservi dubbio che i rifiuti della polizia e degli organi di sicurezza sono legittimati dall'assenza di una legge federale o locale sui limiti entro cui la polizia può negare l'accesso al dato personale o rifiutarne la cancellazione. Sino ad oggi, quindi, l'accettazione o il rifiuto della richiesta di un cittadino è affidata alla discrezionalità degli organi di polizia. Questi ultimi, ovviamente, tendono ad avere una visione incentrata più sui propri problemi professionali che sulle esigenze generali della società: ne può derivare una tendenza all'eccessiva accumulazione e conservazione dei dati.

8. Il caso dell'antinuclearista con lo spray.

Questa tendenza all'accumulo di dati si vede bene in un caso concreto, quello del ventenne (al momento dei fatti) che potremmo chia-

[15] Verwaltungsgericht Köln, 6 maggio 1988, riportato per intero in *Neue Zeitschrift für Verwaltungsrecht*, 1988, pp. 85 ss.

mare « A., l'antinuclearista con lo spray ». A. viene accusato di danneggiamento materiale per avere scritto slogans antinucleari sulla facciata di una casa di una cittadina bavarese. La polizia inizia le indagini su A., raccoglie informazioni e le memorizza. Il Tribunale (Amtsgericht) tuttavia lo assolve per insufficienza di prove, dopo un processo che deve essere stato un po' stralunato, almeno a giudicare da come lo descrive l'Ufficio Criminale Bavarese scrivendo all'avvocato di A.:

« Il Suo cliente era concretamente sospettato di aver commesso un danneggiamento materiale motivato politicamente. Anche dopo l'escussione dei testimoni nel corso del dibattimento questo sospetto non potè essere eliminato. Il danneggiato affermò che il Suo cliente, alcuni giorni dopo il fatto, andò da lui e gli disse di essere pentito di quanto aveva fatto e di voler cancellare la scritta. Tuttavia questo testimone non fu in grado di riconoscere con totale sicurezza il Suo cliente. Un'altra teste ha dapprima accusato il Suo cliente, ma, dopo un giorno, ha rilasciato una dichiarazione tutta diversa che lo scagionava »[16].

Come si vede, il buon senso può provocare in una cittadina bavarese gli stessi comportamenti che l'omertà genera in un paese siciliano. Nonostante tutto ciò, la richiesta di cancellare i dati relativi a quel processo (terminato, ripeto, con un'assoluzione per insufficienza di prove) venne respinta, perché, per gli organi di polizia, « è decisivo se il reato di cui è accusato il Suo cliente offra indizi sufficienti [...] per stabilire se egli in futuro commetterà ancora azioni penalmente rilevanti ». Di qui l'esigenza di conservare i dati: « Nei reati penali con motivazioni politiche, in cui le indagini e la raccolta delle prove sono rese tipicamente difficili dal modo di agire del reo, in base all'esperienza criminalistica ci si può in generale aspettare una recidiva. Perciò i dati personali ricavati dalle indagini su accusati in casi precedenti si prestano particolarmente a facilitare il lavoro di indagine della polizia »[17].

Supponiamo ora che una polizia straniera chieda a quella tedesca informazioni su A., fermato all'estero — ad esempio — per un presunto reato-bagatella. Il telex dalla Germania informerà che è stato processato per danneggiamento materiale a un edificio, e per di più con un movente politico: come se, a quella casa, non ci avesse scritto sopra, ma ci avesse messo una bomba sotto. Quel telex lo farebbe accompagnare subito alla frontiera, come si è infatti verificato in casi analoghi.

È a questi ultimi che vogliamo ora dirigere la nostra attenzione.

[16] Questo passo è contenuto nel documento con cui l'Ufficio Criminale Bavarese respinge l'istanza di cancellazione dei dati di A., raccolti durante le indagini: 13. Strafverteidigertag, *Materialheft*, Köln, 1989, p. 15.

[17] *Ibid.*

9. Flusso transnazionale: alcuni problemi aperti tra Germania federale, Italia e Spagna.

Il caso dell'« antinuclearista con lo spray » illustra le ragioni per le quali la polizia continua a tenere nella memoria del computer certi dati personali, anche dopo una sentenza di assoluzione. Ma quali conseguenze producono queste mancate cancellazioni, allorché i dati vengono trasmessi all'estero? Nel poco materiale a mia disposizione si possono individuare tre situazioni diverse:

— nel caso dell'« ecologo irriducibile » si nota che tra le polizie circolano dati contestabili, perché non cancellati presso la polizia d'origine;

— nel caso della « presunta terrorista », invece, la cancellazione dei dati è avvenuta presso la polizia d'origine, ma non presso quella che li ha richiesti;

— nel caso del « cineasta indesiderato », infine, non risultano dati presso la polizia del paese d'origine, né si sa quali siano quelli in possesso della polizia locale.

a) *L'ecologo irriducibile.* Il tedesco B. acquista nelle vicinanze di Granada una vecchia caserma della Guardia Civil e un po' di terreno al suo interno. Dopo qualche tempo si scopre che una ben maggiore estensione di terra era stata ceduta ad una società immobiliare, che aveva creduto di acquistare anche la vecchia caserma e, con essa, il diritto di edificare. Essendo l'acquisto di B. giuridicamente ineccepibile, la società immobiliare tenta in tutti i modi di indurlo a vendere la sua porzione di terreno. B. rifiuta offerte sempre più vertiginose, perché vuole preservare dall'edilizia quella parte di natura; anzi, la posizione strategica del suo terreno gli consente di creare di fatto una ben maggiore oasi naturale, dal momento che l'immobiliare non può costruire.

Ben presto si passa dalle offerte di danaro alle azioni giudiziarie, nel corso delle quali viene ottenuta dalla Germania una serie di dati personali su B. Questi dati non si riferiscono alla causa in corso, ma ad eventi risalenti anche ad una ventina d'anni prima, ovvero a situazioni che non dovrebbero neppure essere memorizzate. Eccone l'elenco completo, contenuto in una lettera — si noti — del 1987:

1966: furto in un negozio;

1968: indossa senza autorizzazione un'uniforme;

1969: lesioni colpose;

1971: sospetto di truffa; si ignora la conclusione del procedimento;

1977: sospetto di furto d'auto; indagini sospese perché non si tratta di furto.

Questi dati sono anomali: dei più vecchi non esiste traccia nel casellario giudiziale tedesco, dal quale sono stati cancellati per decorrenza della durata prescritta; le ultime due annotazioni, invece, sono in contrasto con i principi sanciti anche dalla giurisprudenza tedesca, in quanto non si riferiscono a comportamenti riferibili con certezza al soggetto.

Le regole interne da seguire in questi casi sono fissate con chiarezza: « I. L'accesso agli atti è consentito ai tribunali, agli uffici del pubblico ministero, nonché agli uffici più elevati della Federazione e del singolo Stato. II. Altri uffici ed enti pubblici possono accedere su loro richiesta agli atti, se dimostrano un loro legittimo interesse. Nei casi in cui: *a*) il processo sia stato « eingestellt »; *b*) l'accusato sia stato assolto; *c*) la registrazione della condanna sia stata cancellata dal Casellario Giudiziale Federale; *d*) la condanna non sia stata iscritta ed un ufficio chieda di vedere i documenti, su cui il Casellario non può dare informazioni in base agli artt. 41 e 61 della Legge Federale sul Casellario Giudiziale (BZRG), a meno che non siano trascorsi più di tre anni dal passaggio in giudicato della sentenza — viene negato l'accesso agli atti, se all'interesse di chi chiede l'accesso si contrappone un interesse superiore dell'interessato, e cioè quello della sua risocializzazione. In caso di dubbio nel concedere l'accesso agli atti, si deve valutare la possibilità di fornire un'informazione desunta dagli atti stessi »[18].

Sulla base delle informazioni sopra riportate, B. venne espulso dalla Spagna.

I suoi avvocati chiesero conto al BKA delle ragioni che l'avevano indotto a trasmettere quei dati. La risposta del BKA del 25 novembre 1988 è formalmente esemplare e può valere la pena di darne il testo per intero, poiché in esso risulta chiaramente tanto il fondamento giuridico della trasmissione all'estero di certi dati personali, quanto l'ambito di discrezionalità entro cui opera un organismo della polizia, nonché i limiti e le salvaguardie di cui la polizia deve tenere conto:

« In base all'art. 2 della sua legge istitutiva, il BKA — nella sua qualità di ufficio centrale — deve "raccogliere e valutare tutte le notizie e i documenti per la lotta contro la criminalità".

In base all'art. 1 della stessa legge il BKA è anche l'ufficio centrale nazionale dell'Interpol per la Germania federale. Di conseguenza, la trasmissione di informazioni della polizia criminale sul Suo cliente all'Interpol di Madrid ebbe luogo legalmente, nell'ambito della collaborazione internazionale fra polizie.

Prima della trasmissione delle informazioni, un nostro controllo accertò che la richiesta dell'Interpol di Madrid era fondata ed accettabile e che quindi ad essa si doveva rispondere fornendo nella misura richiesta tutte le informazioni sul Suo cliente.

[18] Art. 185, I e II delle *Richtlinien für das Strafverfahren und für das Bußgeldverfahren* (RiStBV).

Inoltre, tenendo conto della normativa sulla protezione dei dati personali, in aggiunta al primo telex all'Interpol di Madrid si fece seguire un richiamo alla finalità vincolante cui erano soggette le informazioni fornite.

Oltre all'indicazione del vincolo a questa finalità, il BKA non ha altre possibilità di influire sulla loro ulteriore utilizzazione all'interno dello Stato destinatario.

Le informazioni sul Suo cliente relative agli anni 1969, 1971 e 1977 ci vennero trasmesse con telex dell'ufficio XXX.

Si ritiene necessaria l'ulteriore conservazione/memorizzazione dei documenti/dati personali nell'ambito del BKA. Se ne prevede la distruzione/cancellazione per il 28 ottobre 1996 ».

Stando così le cose, è probabile che l'ecologo irriducibile avrà difficoltà ad entrare in Spagna per quasi una decina d'anni.

b) *La presunta terrorista*. Verso il 1980, un'indicazione anonima portò ad identificare la libraia bavarese C. con la terrorista Susanne Albrecht, ancor oggi ricercata. L'equivoco venne ben presto chiarito, anche perché tra le due persone non vi è neppure una somiglianza fisica; tuttavia le conseguenze di quell'equivoco non sono state eliminate sino ad oggi. Nell'autunno del 1981, mentre C. è in vacanza a Vicenza, tre carabinieri la prelevano di notte dall'albergo e la portano in commissariato. Nel giugno 1982, altro arresto a Vicenza, questa volta di giorno e per la strada. Infine, nel 1988, nuova azione di polizia a Grosseto. Un giornale conclude: « Le può ricapitare in ogni momento, come le ha detto chiaramente la polizia italiana »[19].

Dal canto suo, la libraia non è stata con le mani in mano. Dopo il primo arresto a Vicenza, attraverso un suo legale ottenne dal BKA le seguenti informazioni: tutte le indagini sul suo conto erano cessate; i dati di C. erano stati cancellati da tutti gli archivi del BKA; « le autorità italiane vennero invitate con un telex a cancellare il nome della Sua cliente da tutte le banche di dati ». Eppure, anche dopo questo telex, a Vicenza ed a Grosseto ebbero luogo ancora i due già ricordati arresti di C.

Il BKA non poteva far altro che segnalare l'erroneità dell'informazione fornita originariamente e chiederne la distruzione presso gli archivi delle polizie straniere cui l'aveva trasmessa. Tuttavia sono passati otto anni e pare che la polizia italiana non abbia ancora provveduto alla cancellazione dei dati su C.: contro questa trascuratezza sembra non esservi rimedio giuridico.

c) *Il cineasta indesiderato*. Un dirigente di una casa cinematografica di Monaco di Baviera, che chiameremo D., ha frequenti occasioni di visitare l'Italia per motivi di lavoro o per le vacanze. Tutta-

[19] BÖGEL, *Unschuldig - aber stets im Polizeigriff*, « Abendzeitung » (München), 3 gennaio 1989, p. 4.

via nel 1987 la polizia di frontiera italiana del Brennero gli vietò l'ingresso in Italia. Lo stesso divieto gli venne opposto nell'agosto del 1988: giunto a Bari su un traghetto proveniente dalla Grecia, D. non potè neppure sbarcare e dovette tornare in Grecia con il medesimo traghetto, per poi rientrare in Germania evitando l'Italia. In nessuno dei due casi la polizia italiana seppe indicare a D. la ragione della misura presa nei suoi confronti.

Dopo il secondo divieto di ingresso, D. si rivolse ad un avvocato di Monaco per chiarire ed eliminare la causa dell'inspiegabile provvedimento. Infatti né in Italia, né in Germania federale risultava pendente alcun procedimento a carico del cineasta. Inizia così una pratica, tuttora non conclusa, che illustra esemplarmente tanto un tipico caso di flusso transnazionale dei dati, quanto lo stile di lavoro di due ben diverse burocrazie (basta guardare le date delle lettere citate).

Il 4 ottobre 1988 l'avvocato scrisse all'Ambasciata italiana di Bonn, al Ministero degli esteri tedesco ed all'Ufficio Criminale Federale (BKA) di Wiesbaden. A quest'ultimo ufficio specificava che « circa 15 anni fa, in connessione con un procedimento penale, vennero raccolte informazioni sul nostro cliente. Poiché ogni registrazione in proposito nel Casellario giudiziale federale è da tempo cancellata, La prego di comunicarmi se le informazioni sono ancora esistenti o se, nel frattempo, sono state distrutte ».

L'11 ottobre il Ministero tedesco degli esteri risponde di aver trasmesso la pratica all'ambasciata tedesca a Roma, affinché « verifichi presso le autorità italiane le ragioni del ripetuto divieto d'ingresso opposto dal Suo cliente ». Il 13 il BKA risponde di non aver in memoria alcun dato su D.; d'altra parte deve aver trasmesso copia della richiesta alla Direzione della polizia criminale di Monaco, che il 24 ottobre risponde di non avere né documenti né dati memorizzati su D. Insomma, in Germania non risulta che D. sia stato condannato, né che vi siano indagini in corso su di lui.

Il 26 ottobre l'Ambasciata italiana di Bonn risponde che, « trattandosi della rappresentanza di interessi di un cittadino tedesco », è necessario rivolgersi all'ambasciata tedesca a Roma ». E così fa l'avvocato, con una lettera del 28 ottobre.

Per maggior sicurezza, due giorni prima aveva incaricato un collega italiano di svolgere analoghe ricerche. Erano così partite due richieste alla Questura di Bolzano (7 novembre) e al Ministero italiano degli interni (22 novembre).

Il 10 novembre, intanto, era giunta una risposta dall'ambasciata tedesca a Roma, che — informata anche attraverso il Ministero tedesco degli esteri — « ha già pregato il Ministero italiano degli esteri di comunicare le ragioni del ripetuto divieto d'ingresso opposto al signor D. al confine italiano. Stando all'esperienza di questa Ambasciata — aggiunge prudentemente la lettera — non bisogna far troppo affidamento su una risposta sollecita ».

Facile profezia. Il 6 febbraio 1989, e poi ancora il 17 maggio, l'ambasciata tedesca scrive all'avvocato di aver sollecitato invano il Mini-

stero italiano degli esteri. Finalmente ai primi di agosto, arriva una tautologica nota verbale della Farnesina, che non spiega perché D. sia stato respinto, ma si limita a parafrasare il quesito: « Gli organi competenti — dice — confermano le misure dirette a impedire l'ingresso ». L'ambasciata tedesca ha riscritto, e tutto sta ricominciando da capo.

10. La libera circolazione comunitaria e la criminalità organizzata.

Nel dibattito al congresso dei penalisti tedeschi richiamai l'attenzione sulla necessità di non allargare troppo le maglie della prevenzione, perché viviamo in una fase storica di espansione del crimine organizzato. Mi pare infatti che i colleghi tedeschi tendano a garantire soprattutto il libero sviluppo della personalità degli individui. Condivido questa esigenza, che tuttavia mi sembra condizionata dalla visione di uno Stato moderno e efficiente (anche troppo, obietterà qualcuno) come la Germania federale.

A questa visione sento il bisogno di contraporre quella che nasce in uno Stato decrepito e inconcludente, come quello italiano. All'estero riesce quasi impossibile separare l'efficienza dell'economia privata italiana dallo sfacelo dell'apparato pubblico. Questa schizofrenia nazionale è stata finora una male cronico dell'Italia, ma — con il processo di integrazione europea che inizierà nel 1993 — anche gli altri Stati comunitari dovranno fare i conti con essa. Dovranno fare i conti, cioè, con uno Stato che non soltanto non è riuscito a sconfiggere la mafia in Sicilia, la camorra in Campania e la 'ndrangheta in Calabria, ma che di fatto ha perso il controllo di queste tre regioni.

Il dominio della criminalità organizzata nel Sud e la sua massiccia infiltrazione nel Nord dell'Italia possono prefigurare un futuro sviluppo a livello europeo, se non vengono prese contromisure adeguate. Queste contromisure esigono un'opera di prevenzione poliziesca ed il coordinamento dei servizi di sicurezza di più Paesi.

Non è possibile qui affrontare il tema della diffusione della criminalità organizzata nella società civile italiana ed europea. Basti tuttavia osservare che, a mio giudizio, i colleghi tedeschi che hanno partecipato alla discussione mi sembravano avere una visione folkloristica e metaforica della mafia. Infatti, quando si usa il termine « mafia » per indicare qualsiasi gruppo di pressione, si usa una metafora che spesso preclude la comprensione della realtà. Oggi il commercio della droga e delle armi attribuiscono al crimine organizzato un potere economico senza precedenti. Da anni non siamo più in presenza della mafia agraria di stampo ottocentesco, né di quella della speculazione edilizia de « Le mani sulla città » di Rosi. È una criminalità organizzata che comporta partecipazioni azionarie in grandi imprese e procura voti ai partiti politici: può così mettere i propri uomini nei consigli di amministrazione e negli organismi legislativi, esecutivi e

giudiziari. Questa potenza corruttrice, dopo il 1993, si riverserà con maggior facilità sugli altri Stati comunitari. Ancora una volta, invito a non sottovalutare la forza di queste organizzazioni criminose.

Dalla primavera del 1989 (quando ebbe luogo il congresso di Colonia) all'estate dello stesso anno, lo Stato italiano ha dovuto inviare l'esercito in Calabria (senza per questo risolvere il problema dei sequestri di persona); l'Associazione Bancaria Italiana ha imposto alle banche di identificare tutti i clienti che compiono operazioni di rilievo, per cercare di arginare il riciclaggio del danaro sporco; lo stesso invito è partito dalle associazioni degli agenti di cambio e degli agenti di borsa, poiché per queste vie passa l'inquinamento mafioso dell'economia sana.

Tutti i dati raccolti passano ai computer delle polizie italiane, pur riferendosi nella maggioranza a cittadini incensurati. Sono il primo a sostenere che questi dati personali esigono una precisa protezione legislativa. Tuttavia, nell'individuare i limiti da imporre all'attività di prevenzione svolta dalle polizie, sarebbe un errore pericoloso sottovalutare la sgradevole realtà del crimine organizzato.