
MARIO G. LOSANO

LA « GIUSCIBERNETICA » DOPO QUATTRO DECENNI

SOMMARIO: I. L'informatica e il diritto da un secolo all'altro. — 1. L'informatica del secolo passato: le origini dell'informatica giuridica in Italia. — 2. L'informatica del secolo attuale: un elenco di problemi. — II. Oggi: privacy e sicurezza nell'era del terrorismo. — 3. Ma oggi il bisogno di privacy è davvero un'esigenza diffusa? — 4. I doveri del giurista informatico di fronte all'emergenza. — 5. Le difficoltà nell'interconnessione fra banche di dati all'interno dello stesso Stato. — 6. La raccolta dei dati per la lotta al terrorismo. — 7. L'interconnessione sovranazionale di banche di dati nazionali. — 8. Echelon: « Dagli amici mi guardi Iddio, che ai nemici ci penso io ». — 9. Verso il groviglio inestricabile.

I. L'INFORMATICA E IL DIRITTO DA UN SECOLO ALL'ALTRO.

1. L'INFORMATICA DEL SECOLO PASSATO: LE ORIGINI DELL'INFORMATICA GIURIDICA IN ITALIA.

La storia dell'informatica è iniziata circa mezzo secolo fa, quando negli anni Cinquanta il computer — nato per esigenze militari durante gli anni di guerra — cessò di essere uno strumento coperto dal segreto e divenne un oggetto commerciale sempre più diffuso. In questo mezzo secolo, l'informatica è stata oggetto di un tale affinamento tecnologico, ha conosciuto una tale diffusione operativa e ha esercitato un tale impatto sociale che oggi senza ironia si può parlare di quella prima informatica come dell'informatica « del secolo scorso », per non dire « del millennio scorso ».

La « giuscibernetica », intesa come applicazione dell'informatica al diritto, risale alla metà degli anni Sessanta: quel nome era il titolo di un mio scritto del 1968¹, seguito l'anno dopo da un libro che contribuì a diffondere il dibattito italiano sulla materia². Nel

* Il testo è l'originale in italiano, con alcuni aggiornamenti, della « Conferencia Inaugural » tenuta al « I Congreso Derecho TICs » (Universitat de València, Facultat de Dret, 2 novembre 2004) con il titolo: *La « giuscibernetica » tras quatro décadas*.

¹ LOSANO, *Giuscibernetica*, in: *Nuovi sviluppi della sociologia del diritto 1966-1967*. A cura di Renato Treves, Edizioni di Comunità, Milano 1968, pagg. 307-325.

² LOSANO, *Giuscibernetica. Macchine*

quadro di una ricostruzione storica delle origini dell'informatica in Italia ho già raccontato questa fase eroica dell'informatica giuridica, che allora si chiamava giuscibernetica³. Anche in Brasile, dove avevo tenuto nel 1973 i primi corsi di informatica giuridica⁴, pubblicai un bilancio dell'evoluzione subita in vent'anni da quella materia⁵. Nonostante i radicali mutamenti intervenuti nei decenni successivi, il nome « giuscibernetica » però è tuttora usato, come si può vedere nell'ampia voce della *Piccola Enciclopedia Garzanti del Diritto*; anzi, il termine sembra addirittura entrato nell'uso comune, dal momento che è registrato nel *Nuovo Zingarelli*⁶ e nel *Dizionario di Italiano* della *Biblioteca di Repubblica* in quattro volumi⁷.

Per puro amore di precisione, e quindi senza alcun intento polemico, vorrei però smentire quanto scrive Enrico Pattaro: « Fu grazie all'originaria presenza e all'originario impulso di Vittorio Frosini che altri studiosi, muovendo dalla filosofia del diritto, si volsero all'informatica giuridica: sia in Italia (per esempio Mario Losano ed io stesso); sia all'estero »⁸. Per quanto mi concerne, giunsi all'informatica giuridica per altre vie, soprattutto attraverso il World Peace Through Law Center di Washington e l'università Humboldt di Berlino (allora Est), nonché attraverso mio padre, che fu tra i primi in Italia a introdurre l'informatica nelle assicurazioni. Gli anni Sessanta furono per me anni di lavoro all'estero e nelle imprese private, che consolidarono il mio approccio soprattutto pratico all'informatica: un approccio quindi diverso da quello, prevalentemente teorico, di Vittorio Frosini. Dopo il 1968 le nostre vie si intrecciarono spesso, ma sempre in totale autonomia scientifica e in totale armonia personale. Il nostro buon rapporto si riflette anche dalle pagine che scrissi subito dopo la sua morte⁹. Quanto al nostro diverso modo di affrontare

e modelli cibernetici nel diritto, Einaudi, Torino 1969, 205 pagg.

³ I primi anni dell'informatica giuridica in Italia, in: FONDAZIONE ADRIANO OLIVETTI (a cura di), *La cultura informatica in Italia. Riflessioni e testimonianze sulle origini, 1950-1970*, Bollati Boringhieri, Torino 1993, pagg. 191-236.

⁴ LOSANO, *Lições de informática jurídica*. Curso de extensão universitária no Departamento de direito economico-financeiro da Faculdade de Direito da Universidade de São Paulo, Seção gráfica do Tribunal de Alçada Criminal, São Paulo 1973, IV-210 pagg.

⁵ LOSANO, *A informática jurídica vinte anos depois*, « Revista dos Tribunais », LXXXIV, maio de 1995, vol. 715, pagg. 350-367.

⁶ Il titolo esatto è: NICOLA ZINGARELLI, *Vocabolario della lingua italiana*, Zani-

chelli, Bologna 1984 (undicesima edizione), purtroppo con una definizione fuorviante: « Scienza che studia il razionale ordinamento enciclopedico dei vocaboli attinenti il diritto ».

⁷ Questo *Dizionario di Italiano*, pubblicato nel 2005, nasce dalle attività lessicografiche delle case editrici Garzanti, Utet e De Agostini. La definizione di giuscibernetica è più accettabile, anche se discutibile perché troppo limitativa: « Scienza che studia la sistemazione e la catalogazione dell'insieme delle norme giuridiche, valendosi di elaboratori elettronici ».

⁸ ENRICO PATTARO, *La filosofia del diritto di fronte all'informatica giuridica*, in ANNA JELLAMO-FRANCESCO RICCONO (ed.), *In ricordo di Vittorio Frosini*, Giuffrè, Milano 2004, pag. 26.

⁹ LOSANO, *Vittorio Frosini (1922-2001)*, « Sociologia del diritto », 2001,

l'applicazione dell'informatica al diritto, basta confrontare le nostre bibliografie¹⁰.

Le attività di studio e le applicazioni pratiche, soprattutto nell'amministrazione pubblica, si cristallizzarono nel 1985-86 nei tre volumi del corso destinato ai miei studenti milanesi¹¹. Per quanto oggi superati dall'evoluzione tecnologica, questi volumi costituivano il più completo panorama disponibile in Europa tanto sull'informatica giuridica quanto sul diritto dell'informatica. Essi erano stati preceduti da varie edizioni ciclostilate, una delle quali venne tradotta anche in spagnolo¹².

Accanto alle banche di dati in linea, il mio interesse andava alle banche di dati fuori linea (cioè ai CD-ROM¹³) e alla legge sulla privacy¹⁴, che l'Italia fu tra gli ultimi Stati nell'Unione Europea ad adottare e alla quale dedicai molti scritti e persino un progetto di legge¹⁵. Ma sulla privacy, oggi, ho anche qualche radicale ripensamento: se ne parlerà in dettaglio nella seconda parte di questo scritto.

Le opere che andavo pubblicando negli anni Settanta e Ottanta tenevano d'occhio due prospettive di ricerca. La prima era storica, legata alla mia formazione e intesa soprattutto a far capire agli studenti come l'elaboratore elettronico fosse il frutto della secolare storia del calcolo automatico. La seconda prospettiva si rivolgeva invece al futuro, perché la rapidità dell'evoluzione dell'informatica poneva inevitabilmente quesiti sui problemi futuri. Così, mentre compivo i primi esperimenti nell'amministrazione regionale lombarda, mi occupai dell'automazione dello Stato giapponese¹⁶: una ricerca che oggi si chiamerebbe di *e-government*. Al

n. 3, pagg. 193-197. Anni prima avevo partecipato a una Festschrift per Frosini con il saggio *L'applicazione delle leggi sulla privacy alle carte di credito*, in DONATO A. LIMONE (a cura di), *Dalla giuritecnica all'informatica giuridica. Studi dedicati a Vittorio Frosini*, Giuffrè, Milano 1995, pagg. 201-216.

¹⁰ *Bibliografia degli scritti di informatica giuridica di Vittorio Frosini*, in DONATO A. LIMONE (a cura di), *Dalla giuritecnica all'informatica giuridica. Studi dedicati a Vittorio Frosini*, Giuffrè, Milano 1995, pagg. 385-396. La mia bibliografia è reperibile nel sito «www.mariolosano.it».

¹¹ LOSANO, *Corso di informatica giuridica*. Vol. I. *Informatica per le scienze sociali*, Einaudi, Torino 1985, XXI-547 pagg.; vol. II. *Il diritto privato dell'informatica*, Einaudi, Torino 1986, XVIII-298 pagg.; vol. III. *Il diritto pubblico dell'informatica*, Einaudi, Torino 1986, IV-348 pagg.

¹² LOSANO, *Curso de informática jurídica*. Traducción de Manuel Atienza y Juan Ruiz Manero, Tecnos, Madrid 1984, 262 pagg.; traduzione del solo vol. I dell'edizione del 1984.

¹³ Le mie esperienze in questo campo sono riassunte in *Diritto e CD-ROM. Esperienze italiane e tedesche a confronto*, a cura di Mario G. Losano e Lothar Philipps, Giuffrè, Milano 1990, pagg. VIII-117.

¹⁴ *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, a cura di Mario G. Losano, Laterza, Roma-Bari 2001, pagg. XX-434.

¹⁵ LOSANO, *Il computer di cristallo. Progetto di legge sulla protezione dei dati personali*, «MicroMega», 1987, n. 1, pagg. 159-177; anche in *Il diritto dell'informazione e dell'informatica*, III, maggio-agosto 1987, pagg. 465-485.

¹⁶ LOSANO, *Stato e automazione. L'esempio giapponese*, Etas Kompass, Milano 1974, pagg. 245.

tempo stesso, mi sorprendevo l'attenzione che i giapponesi e il Sud-est asiatico rivolgevano all'educazione: e — mentre la propensione alla ricerca del Giappone appariva scontata già allora — nel 1972 richiamavo l'attenzione sugli sviluppi universitari del Sud-est asiatico. Allora sembrava una forma di esotismo tecnologico, oggi ne stiamo vivendo le conseguenze¹⁷.

Con il passare degli anni, l'informatica mutava il mondo, ma intanto diveniva una tecnica matura. La frontiera del sapere si spostava verso la biologia, che avrebbe finito per influire anche sull'informatica. Nel 1976 avevo accennato, nella prefazione a una raccolta di articoli nell'edizione italiana di «Scientific American»¹⁸, come per l'innovazione tecnologica il futuro sembrasse sempre più puntare sulla biologia come scienza d'avanguardia, dando invece per ormai acquisita l'informatica. Per esempio, gli animali transgenici diverranno produttori di medicinali a basso costo: ma sarà importante vedere se questi saranno medicinali anche a basso prezzo, oppure soltanto ad alto profitto. Nell'ambito dell'informatica si sta lavorando a creare micro-organismi che assolvano le funzioni di microprocessori.

Infine, tenendo presenti queste prospettive, al cambio del millennio tentai una sintesi e una previsione che forse sono ancora in parte accettabili¹⁹. A fronte di questo tempestoso sviluppo dell'informatica, è sorprendente notare l'immobilismo della facoltà di giurisprudenza, dove per tre decenni ho tentato invano di introdurre l'insegnamento dell'informatica giuridica. Se questa materia poteva sembrare eccentrica negli anni Settanta, non lo era certo più nel decennio successivo. Eppure solo nel nuovo millennio riuscii ad istituire un corso triennale di informatica giuridica nella giovane università del Piemonte Orientale²⁰.

Oggi la prospettiva per il futuro dell'informatica è legata anche agli squilibri fra gli Stati operanti in un mondo globalizzato, il «*computer divide*», da cui discende il quesito più generale: *quale futuro per il Terzo Mondo?* Il principale problema per il futuro dell'informatica è la trasformazione del cosiddetto Terzo Mondo da puro consumatore in produttore: o produttore per delega, gra-

¹⁷ LOSANO, *Le nuove università del Sud-Est asiatico*, «Civiltà delle Macchine», 1972, n. 1-2, pagg. 36-38; LOSANO, *La doppia faccia di Hong Kong*, in «Rivista IBM», VIII, 1972, n. 1, pagg. 28-36.

¹⁸ LOSANO, *Presentazione - Le radici europee dell'elaboratore elettronico*, in *I calcolatori elettronici. Applicazioni e prospettive*, a cura di Mario G. Losano, Le Scienze, Milano 1976, pagg. 7-28.

¹⁹ LOSANO, *La informática jurídica hacia el tercer milenio*, in *Instituto de Derecho Informático de la Universidad de la*

República, Derecho informático. Tomo I. Corresponsable al año 2000, Fundación de Cultura Universitaria, Montevideo 2001, pagg. 81-101.

²⁰ LOSANO, *Un corso universitario triennale di informatica giuridica*, in questa *Rivista* 2003, n. 6, pagg. 1047-1061 (trad. port.: *O curso trienal de informática jurídica na universidade do Piemonte Oriental*, «Prim@ Facie» (João Pessoa, Brasil), III, 2004, n. 4, pagg. 5-19: «<http://www.ccj.ufpr.br/primafacie>»).

zie al *dumping* sociale e salariale, oppure produttore in proprio, grazie alle tecnologie finora appannaggio del cosiddetto Primo Mondo.

Il Giappone moderno ha sempre avuto la tendenza a porsi alla testa dell'innovazione tecnologica. I primi passi verso l'informatizzazione del paese vennero intrapresi già negli anni Settanta, ma solo con Internet (e l'elaborazione grafica degli ideogrammi) si è potuti passare a una fase avanzata. Dal 1994 il Giappone è coperto da Internet ed ora intende proporsi a modello per il resto del mondo — come già avvenne per la costruzione dei computer — anche nella creazione di una società informatizzata. In Europa ci muoviamo verso un e-government (e siamo ai primi passi). Il Giappone si propone oggi una strategia di informatizzazione totale: una « e-Japan Strategy »²¹.

Ma al Giappone si aggiungono oggi l'India, con la sua capacità nel software, e la Cina, con la sua capacità produttiva. I difetti di quei modi di produzione non sono spariti: ma bisogna riflettere sul fatto che lo sviluppo industriale non è incompatibile con la corruzione, né che è facile mettere un limite al *dumping* sociale e salariale, che oggettivamente esiste.

L'informatica è anche lo strumento della globalizzazione economica (cfr. *infra*, § 2, a). Gli Stati e i continenti che ne sono tagliati fuori avranno un destino sempre più separato da quello degli Stati avanzati: è questo il *computer divide*. Infatti oggi prevale il modello « gravitazionale »: si è infatti constatato che è più facile il commercio fra paesi con tecnologia simile che fra paesi troppo diversi. Se fosse decisivo solo il basso costo della mano d'opera, le imprese emigrerebbero in Africa, mentre invece cercano un partner che offra uguale tecnologia a un costo inferiore di quello domestico. Ad esempio, prima di essere montato sulle automobili coreane Kia, il lettore di DVD varca tre volte l'Atlantico verso gli Stati Uniti. Nel mondo globalizzato, infatti, il trasporto può essere un costo trascurabile.

In questo mondo globalizzato e diviso, resta da vedere se e come reagiranno gli Stati e i popoli che il *computer divide* relega tra i perdenti. Una delle risposte sembra essere il terrorismo internazionale, quando lo si interpreta come nato dalla frustrazione dei paesi islamici per non aver raggiunto la soglia del benessere.

Dopo questa ricostruzione del passato e questa previsione del futuro è giunto il momento di esaminare anzitutto i mutamenti introdotti dall'informatica, mutamenti già presenti e destinati ad accompagnarci nell'immediato futuro: ad essi sarà dedicato il prossimo paragrafo, che inevitabilmente dovrà assumere l'aspetto più

²¹ Relazione di VALENTINA MATONE (*e-Japan Strategy: costruire la più avanzata società dell'informazione*) al XXVIII

Convegno di Studi sul Giappone (Aistugia), svoltosi a Milano il 16-18 settembre 2004.

di un elenco che di una trattazione. La seconda parte, invece, si soffermerà più in dettaglio sull'invasione dell'informatica nella nostra vita privata e, soprattutto, sul conflitto che caratterizza l'attuale uso dell'informatica: il conflitto fra la riservatezza individuale e la sicurezza collettiva.

Naturalmente non solo i poteri pubblici, ma anche i privati invadono la sfera individuale: tuttavia non è qui possibile occuparcene. Una rassegna dettagliata è stata pubblicata nel 2003 in Svezia — paese sempre attento a questi problemi — e tradotta nel 2005 in tedesco con il significativo titolo: *La mafia della sorveglianza. Buoni affari con i nostri dati*²². A questo volume rinvio per le informazioni sugli attentati privati alla privacy individuale. Nella seconda parte l'attenzione si concentrerà invece sull'invasione della privacy individuale da parte dei poteri pubblici

2. L'INFORMATICA DEL SECOLO ATTUALE: UN ELENCO DI PROBLEMI.

In questo paragrafo mi limito ad accennare agli aspetti più attuali dell'informatica, senza poterli sviluppare: sono tutti argomenti per un'eventuale, successiva discussione.

a) In generale, l'informatica è lo strumento della *globalizzazione*, di cui oggi si parla tanto: senza la capacità e la velocità degli attuali computers, senza la flessibilità e la complessità dei loro programmi, senza la capillarità e l'attendibilità della rete mondiale, la globalizzazione non esisterebbe. L'informatica ha annullato il tempo e lo spazio, almeno per le attività smaterializzate (come quelle finanziarie); per le altre, ha reso molto più veloce tutta una serie di attività comunicative, giuridiche e finanziarie, ma trova ancora un insormontabile collo di bottiglia nella consegna materiale dell'oggetto. Con la libreria in rete posso cioè concordare un acquisto, stipulare un contratto e pagare il prezzo per Internet, ma qualcuno dovrà poi portarmi a casa il libro così acquistato.

b) L'informatica ha rivoluzionato interi settori dell'attività economica: in particolare, vorrei qui ricordarle la *rivoluzione della stampa*.

Si è passati dalla tipografia « calda » alla tipografia « fredda », anche se il lettore non se ne accorge. La tecnica tipografica tradizionale è divenuta un'attività di nicchia per tipografi-artisti (in Italia, ad esempio, l'editore Tallone). Una significativa innovazione dell'informatica applicata all'editoria è la nascita dei *books on demand*. Si immagazzina nella memoria il testo e se ne produ-

²² PÄR STRÖM, *Die Überwachungs-mafia. Das gute Geschäft mit unseren Daten*, Hanser, München 2005, pagg. XI-340.

cono tante copie quante sono necessarie: scompare quindi l'immobilizzo finanziario legato al magazzino.

Il *book on demand* non si sta diffondendo con la velocità che le sue caratteristiche consentirebbero perché incontra problemi giuridici. Infatti si riesce a produrre un *book on demand* solo se l'editore dispone dei diritti d'autore, cioè se produce un *book on demand* utilizzando una parte di un libro già suo (tanto come diritti, quanto come memorizzazione del testo); in caso contrario, deve predisporre con l'autore un contratto apposito; ma non riuscirà a produrre il *book on demand* se il testo in questione è stato pubblicato da un editore concorrente.

Nonostante questi ostacoli giuridici, si provi a pensare alle potenzialità di questa tecnologia nella didattica universitaria, in quella della scuola secondaria e nella pubblicazione dei risultati di ricerche scientifiche finanziate con il denaro pubblico.

Nell'università, il *book on demand* sarebbe la soluzione ideale per produrre testi universitari adatti all'Espacio Europeo de Educación Superior e al nuovo sistema dei crediti (SETC: Sistema Europeo de Transferencia de Créditos). Esso permette infatti di (ri-) produrre anche *parti di libro* nelle dimensioni richieste dai crediti della specifica materia e nella quantità di esemplari necessari per gli studenti di quell'anno. Questo sistema è già stato sperimentato con risultati soddisfacenti nel corso di informatica giuridica dell'Università del Piemonte Orientale, ad Alessandria.

Nelle scuole secondarie, ogni anno sorgono discussioni sull'aumento del prezzo dei libri e sull'aumento del peso dei libri, anche se il Ministero della Pubblica Istruzione impone limiti di costo e di peso, non sempre rispettati. In particolare, le nuove edizioni ogni anno impediscono di usare i libri stampati nell'anno precedente: e spesso si tratta di «nuove» edizioni che di nuovo hanno veramente poco, salvo il prezzo. La Presidenza del Consiglio dei Ministri italiano ha avanzato una proposta interessante: i libri di testo delle secondarie saranno su Internet e gli studenti li scaricheranno, eventualmente solo per la parte necessaria, a costo pressoché zero²³. Ovviamente gli editori e i librai hanno protestato energicamente: ma siamo sicuri questa proposta sia davvero (come essi dicono) «una norma anti-libro»?

Infine, affrontando il problema dei rapporti fra ricerca pubblica e pubblicazione dei suoi risultati, in Germania il Ministero Federale della Ricerca ha proposto che gli enti che compiono ricerche finanziate con fondi pubblici siano liberi di pubblicare a stampa il testo con un editore di loro scelta, ma che — al tempo stesso — siano obbligati a divulgarlo gratuitamente anche su In-

²³ Gli studenti troveranno i libri di testo su Internet, «Corriere della Sera», 3 luglio 2004, pag. 18.

ternet: infatti, si afferma, i risultati di una ricerca pubblica devono essere pubblici.

c) L'impatto dell'informatica può non essere entusiasmante per tutti: che ne sarà degli *archivi* e delle *biblioteche* nell'era dell'informatica? Ci avviamo verso una società senza memoria? Per ragioni di profitto dei produttori di software, infatti, i nuovi programmi di videoscrittura sono sempre più spesso incompatibili con quelli anteriori, anche se messi in circolazione dallo stesso produttore. Oggi non siamo più in grado di leggere i testi scritti con programmi di dieci anni fa; anzi, non abbiamo neppure più l'hardware per leggerli: chi mai possiede ancora un lettore per dischi magnetici di 5 pollici? Questa situazione genera interrogativi inquietanti:

— Che ne sarà degli attuali archivi magnetici? Diverranno illeggibili, o si smagnetizzeranno, e noi non pubblicheremo mai più carteggi?

— Come faranno gli archivi di Stato a conservare la documentazione che, per legge, devono raccogliere? E come sarà possibile consultarla?

— Le biblioteche catalogano CD, DVD ecc.: come sarà possibile leggerli in futuro?

— Per leggere la massa di dati informatici oggi prodotti, bisognerà disporre dell'hardware, del software di base, del software applicativo e dei relativi manuali d'istruzioni: la futura biblioteca si trasformerà in un ibrido incrocio tra la biblioteca classica e il museo della scienza della tecnica²⁴?

d) Infine si può solo ricordare con un cenno l'impatto dell'informatica sulla *produzione della stampa periodica e dei giornali*, sempre più messa in pericolo dalla televisione e da altre forme di diffusione delle informazioni. Qui l'informatica sembra aver prodotto effetti tanto positivi quanto, a volte, perversi. È positivo il fatto che oggi il giornale composto nelle tipografia fredda conosca una diffusione prima impensabile: esso viene composto, spedito attraverso la rete e stampato in un altro continente; per esempio, il « Corriere della Sera » esce contemporaneamente a Milano, a Buenos Aires e a São Paulo. Ma è preoccupante che la scrittura degli articoli si avvalga di programmi con sofisticati correttori ortografici, e che contemporaneamente nei giornali non si siano mai visti tanti refusi come oggi.

L'informatica viene usata per ridurre i costi e soprattutto il personale, cioè i giornalisti. A mio giudizio, questa tendenza tipica

²⁴ Mi ero occupato di questi problemi in LOSANO, *História contemporânea del derecho y sociología histórica*, « Anuario de Filosofía Jurídica y Social » (Buenos Aires), 1995, n. 15, pagg. 133-173; anche in

« Sociologia del diritto », XXIII, 1996, n. 3, pagg. 13-50, incluso poi nel volume MARIO G. LOSANO (a cura di), *Storia contemporanea del diritto e sociologia storica*, Franco Angeli, Milano 1997, pagg. 13-50.

dell'intera attività economica attuale, invece di migliorare il giornale (rendendolo un « prodotto di nicchia » rispetto agli altri mezzi di comunicazione) ha peggiorato la qualità informativa della stampa periodica: invece di puntare sulla qualità intrinseca, i giornali e i settimanali soprattutto italiani cercano di sostenere le vendite ripiegando sui *gadgets* in omaggio. Il trend informativo è chiaro da decenni a tutti i comunicatori: la radio dà subito la notizia; la televisione ne dà subito l'immagine; il giornale ne dà subito il commento: oggi però preferisce spesso dare un pettine o una sciarpa invece del commento.

e) Il « *Distributed Library Project* » è un caso particolare di simbiosi tra l'informatica e il buon vecchio libro stampato: alcune biblioteche hanno creato un catasto di chi è disposto a prestare un libro o un CD a un'altra persona. L'iniziativa si propone di far nascere una comunità di lettori, anche per la difficoltà di spostare il libro o il CD come oggetto fisico²⁵. Ulteriori informazioni si possono trovare per la California in « www.communitybooks.org » e per l'Italia in « www.babelteka.org ».

f) *La musica in rete*. Infine non si può qui esaminare il fenomeno diffusissimo della musica in rete, che muove interessi giganteschi e crea quindi conflitti giuridici altrettanto giganteschi. Le possibilità tecniche vanno regolate dal diritto, che spesso si rivela un ostacolo inutile. In alcuni casi, si ha l'impressione che il legislatore non si renda conto delle conseguenze della sue azioni, come è avvenuto in Italia con il cd. « Decreto Urbani », dedicato a reprimere lo scaricamento da Internet — fra l'altro — di cinema e musica²⁶.

Nella conversione in legge, la formulazione « a fini di lucro » è stata sostituita con quella « per trarne profitto ». La differenza giuridica è, in Italia, chiarissima: poiché è profitto anche una spesa evitata, le sanzioni della legge si applicherebbero a chi scarica film o musica per uso proprio, in quanto evita una spesa. Le pene previste sono gravi: da 6 mesi a 3 anni di reclusione, aumentati da uno a quattro anni in caso di reato aggravato; a queste pene si aggiungono gravi sanzioni pecuniarie. Se non intervengono mutamenti nel corso dell'iter di conversione in legge, scrive Rossato, « il nostro paese si troverà ad essere il primo, nell'ambito della tradizione giuridica occidentale, ad aver optato per una repressione penale della condivisione on-line, senza fini di lucro, di opere dell'ingegno protette dal diritto d'autore »²⁷. Si rischia così l'incriminazione della tecnologia « peer to peer » (P2P) e il contra-

²⁵ CARLO FORMENTI, *I libri a costo zero, l'ultima sfida online*, in « Corriere della Sera », 29 settembre 2004, pag. 37.

²⁶ Decreto legge del 22 marzo 2004, n. 72, convertito in legge con modifiche

alla Camera dei Deputati il 22 aprile 2004.

²⁷ Cfr. il parere pro veritate di Andrea Rossato in « www.istitutocolli.org/materiali/relazioneDecretoUrbani.pdf » (ovvero con suffisso « .html »).

sto con la normativa comunitaria, che esclude le sanzioni per gli utenti in buona fede e senza fine di lucro.

g) L'attuale fusione tra informatica e telefonia e la diffusione dei *telefoni cellulari* ha portato all'uso dei messaggi brevi (sms) per fini pubblicitari. Il 12 febbraio 2004 il garante italiano della privacy aveva autorizzato i messaggi pubblicitari telefonici, purché non registrati su nastro: da allora non si mangia più tranquilli, perché l'ora dei pasti è quella prediletta dai call-center, che sanno di trovare qualcuno in casa. Invece gli sms non sono telefonate dirette e perciò la Corte di Cassazione italiana li ha equiparati non alle lettere, ma alle telefonate moleste, condannando di conseguenza chi ne fa un uso insistente.

Un vasto dibattito politico e giuridico è stato provocato dalla Presidenza del Consiglio italiana in occasione delle elezioni locali del 12 e 13 giugno 2004, quando la coalizione di governo temeva un forte assenteismo. Sentito il Garante della Privacy e autorizzato dal Ministero degli Interni, il Presidente del Consiglio inviò alle società telefoniche un suo messaggio per ricordare agli elettori di andare a votare. Da quelle società il messaggio venne trasmesso a circa 50 milioni di cellulari.

L'opposizione ritenne che questo invio costituisse una forma di propaganda elettorale illecita. La situazione era ancora più tesa a Milano, dove la candidata uscente inviava un sms che era un chiaro messaggio elettorale: « Vota 5 anni di buon lavoro ». Il prefetto di Milano ha ritenuto non corretto questo uso degli sms, perché questo tipo di informazione è ammissibile solo per motivi di ordine pubblico.

Dopo le elezioni la polemica si è dissolta, ma il problema resta e si ripresenterà in futuro, perché l'uso dei sms è previsto in caso di emergenze e per l'ordine pubblico (per esempio, fughe di gas o *black out* elettrici): perciò l'abuso dei sms per fini diversi, afferma un giurista, « può togliere peso e visibilità ai pochi comunicati urgenti emessi dalle autorità »²⁸.

Circa un anno dopo, in occasione del referendum sulla fecondazione assistita, la Chiesa invitò i cattolici ad astenersi da quel voto: in questo modo, gli avversari della fecondazione assistita si appropriavano anche dei voti degli astensionisti « fisiologici » (e col 51% di astensioni il referendum fallisce, come infatti avvenne). Però, negli animati dibattiti che precedettero il giorno del voto, il ricordo delle elezioni dell'anno prima provocava testi ironici in internet. Per esempio: « Sono sicura che il mio presidente del Consiglio, che è onesto, corretto, bravo e buono, provvederà ad inviare un sms a tutti gli italiani per ricordare loro che il 12 e il 13 giugno [2005] si vota per il referendum sulla fecondazione assistita, così

²⁸ FULVIO SCAPARRO, *Sms e allarmi sociali: nuove regole civili*, in « Corriere della Sera », 25 giugno 2004, pag. 1 e 52.

come giustamente fece per le *elezioni europee*. Vero?»²⁹. Ma ovviamente questa volta dal governo non giunse alcun sms che invitasse a votare.

Più in generale, l'uso dell'informatica nelle elezioni — il cosiddetto voto elettronico — evoca necessariamente le vicende della Florida del 2000, quando la prima elezione di George W. Bush si concluse in un modo poco chiaro. Nel 2004, alla vigilia della seconda elezione di Bush, la situazione tecnica del voto elettronico non sembrava migliorata, tanto che un giornale tedesco ne forniva un quadro sotto il titolo *Due più due fa cinque*³⁰.

h) Molti problemi stanno sorgendo dalla diffusione dell'*immagine in rete grazie a telecomunicazioni, web-cam e fototelefoni cellulari*. Per l'immagine in rete si ripropongono tutti i problemi visti per i testi, cui si aggiungono alcuni problemi specifici, come quelli legati alle web-cam e all'uso dei video-telefoni.

Qui si sono verificati numerosi abusi e violazioni della privacy, perché le spesso web-cam sono installate all'insaputa degli interessati (anzi, degli assolutamente-*non*-interessati) nelle cabine di prova dei grandi magazzini, negli spogliatoi, negli hotel o nei bagni. Le immagini abusive vengono cedute a siti Internet e spesso costituiscono oggetto di commercio. La diffusione del fenomeno è tale da aver provocato un'indagine parlamentare in Nuova Zelanda, al termine della quale i risultati paiono essere stati così allarmanti da indurre il Ministro della Giustizia, Phil Goff, a presentare un progetto di legge che prevede tre anni di reclusione per il «voyeur digitale» e un anno per la sola detenzione di questo genere di immagini³¹.

Ma il videotelefono può costituire anche uno strumento per verificare il comportamento elettorale nella compra-vendita di voti e, quindi, nel controllo del territorio da parte della criminalità organizzata. Nelle elezioni locali del 3 aprile 2005, i seggi elettorali italiani esibivano un cartello che vietava di entrare con il videotelefono nelle cabine elettorali: si sarebbe infatti potuto «fotografare» la scheda con il contrassegno di voto per esibire poi la foto all'emissario del candidato disonesto o — ipotesi ancora più inquietante — al boss mafioso che controlla i voti della zona. Divieto sensato, dunque: peccato però che nei seggi elettorali non fosse prevista alcuna forma di controllo dei votanti.

i) *Il sottile confine tra abuso e censura nella rete.*

Nei casi di reati comuni come offerte fraudolente o contrarie alla pubblica morale è comprensibile l'intervento dell'autorità

²⁹ «www.rolliblog.net/archives/2005/06/06/un_sms_per_il_referendum.html», visto il 30 agosto 2005.

³⁰ WOLFGANG KOYDL, *Zwei plus zwei macht fünf*, «Süddeutsche Zeitung», 29 settembre 2004, pag. 2.

³¹ La notizia viene da «punto-informatico.it/p.asp?i=48809» e deve ancora essere verificata.

pubblica sui siti e la loro censura o chiusura. Altrettanto chiari e riprovevoli sono i casi di censura politica preventiva, come avviene con Internet in Cina.

Ma può essere oggetto di discussione la chiusura di un sito per motivi di tipo giuridico-politico. Basti qui ricordare il caso del sito Indymedia, sito libertario sorto dopo l'incontro dell'Organizzazione Mondiale del Commercio a Seattle e fondato sulla totale libertà dei contenuti (*open publishing*)³². Sembra che nell'incontro al vertice di Evian questo sito avesse pubblicato alcune foto di agenti antisommossa svizzeri e che da ciò fosse partita la richiesta di chiudere il sito. Ed effettivamente l'FBI oscurò il sito, affermando di eseguire così una richiesta avanzata da Italia e Svizzera: si voleva tutelare la riservatezza di un agente di polizia o si trattava di un'altra velenosa conseguenza degli scontri fra polizia e no-global al G8 di Genova?

l) La *rapidità dell'innovazione* sta provocando anche un cambio di comportamento nella protezione della propria invenzione. Il procedimento per ottenere un brevetto è lungo e rende nota l'invenzione. Poiché nel mondo dell'informatica e dell'elettronica di consumo — considerate ormai tecnologie mature — l'obsolescenza è rapidissima, si tende a non brevettare più: infatti nell'arco di tre anni il prodotto sarà obsoleto e, nel frattempo, i concorrenti non avranno potuto prenderne conoscenza attraverso la documentazione depositata per il brevetto.

m) Giungiamo infine al quesito su cui è necessario soffermarsi in dettaglio: *privacy e sicurezza sono compatibili?* Quarant'anni fa non esisteva Internet e le embrionali banche di dati allora esistenti permettevano la schedatura di dati personali in un modo soltanto un po' più efficiente della schedatura manuale. Quindi le schedature illegali — tanto manuali quanto informatiche — creavano all'incirca lo stesso allarme politico o sociale.

Con l'aumento della capacità delle memorie e della velocità di elaborazione, con il miglioramento dei programmi e, infine, con l'interconnessione in rete delle banche di dati, il rischio della violazione della privacy allarmò anche il cittadino comune. Nacquero così negli anni Settanta le prime leggi sulla protezione dei dati personali. Negli ultimi anni queste leggi — nate con riferimento alle banche di dati informatici — vennero estese anche alle intercettazioni telefoniche e alla videosorveglianza, giungendo sino a entrare in collisione con il diritto di cronaca.

Bisogna distinguere le restrizioni del diritto individuale alla riservatezza dalle violazioni della riservatezza stessa.

³² Al fatto il « Corriere della Sera » dedica un'intera pagina (10 ottobre 2004, pag. 14). Il sito « indymedia.it » spiega che

è un « network di media gestiti collettivamente per una narrazione radicale, obiettiva e appassionata della realtà ».

Ad esempio, una legittima restrizione alla privacy, anche se oggetto di violente discussioni, è quella contenuta nella « Legge sull'onestà fiscale » tedesca, che consente alle autorità fiscali l'accesso ai conti correnti di ogni cittadino in qualunque momento, senza avvertire né il cittadino né la banca (né tanto meno l'autorità giudiziaria). Forse sarebbe più efficace, ai fini fiscali, controllare non lo stato di un conto corrente, ma il flusso delle rendite finanziarie, cioè gli interessi e i dividendi incassati: ma questa è una discussione sull'efficacia del provvedimento, che comunque si presenta come una legge. In questo caso, la limitazione della privacy è il frutto di una decisione politica, discutibile ma legittima.

In altri casi, invece, enti pubblici o semi-pubblici possono violare la privacy infrangendo la legge. Esempio è stata la polemica legata alle elezioni locali italiane del 3 aprile 2005, quando — per concorrere alla presidenza della Regione Lazio — Alessandra Mussolini presentò una lista alternativa di destra in concorrenza con il presidente uscente, che era anche il candidato ufficiale della destra. Per presentare una nuova lista occorre un certo numero di firme: e proprio alcune centinaia di queste firme si rivelarono falsificate. Dunque, la candidata aveva commesso un reato. Però la denuncia di questo reato era avvenuta in modo illecito.

La società informatica della Regione Lazio (non insensibile quindi al presidente uscente e candidato ufficiale della destra, in concorrenza con Alessandra Mussolini) confrontò *senza alcuna autorizzazione* la lista delle firme presentata da Alessandra Mussolini con l'anagrafe del Comune di Roma (retto dal centro-sinistra), scoprendo così le irregolarità. Ne seguirono polemiche feroci e tentativi di far sparire le tracce informatiche dell'incursione nel computer dell'anagrafe del Comune, seguiti dalla sospensione della lista e dallo sciopero della fame di Alessandra Mussolini. Quello che qui importa rilevare non è tanto la vicenda politica, quanto l'abuso informatico di enti ufficialmente preposti alla gestione di dati pubblici.

Questo allarmante caso di abuso informatico da parte del potere politico ha avuto una strana conseguenza: il dibattito si concentrò sulla violazione informatica, mentre nessuno parlò più delle firme false e la lista causa della polemica partecipò alle elezioni regionali, sia pure senza successo.

Infine giungiamo ai casi più inquietanti: i controlli e gli abusi sui dati personali compiuti da quegli *enti clandestini ma non illegali* che sono i servizi segreti. La lotta alla criminalità organizzata e, ora, al terrorismo internazionale ha offerto un pretesto politico eccellente per l'estensione dei loro poteri incontrollati: questi enti agiscono quindi non solo con una copertura giuridica, ma anche per una « nobile causa ».

Lo Stato — che ha emanato le leggi sulla privacy, ma anche quelle sulla lotta al terrorismo e alla criminalità organizzata — si trova così di fronte al compito contraddittorio di dover tutelare

tanto la riservatezza quanto la sicurezza dei cittadini. Ma spesso le due tutele si rivelano incompatibili: sui problematici rapporti fra sicurezza e riservatezza conviene ora soffermarsi ulteriormente.

II. OGGI: PRIVACY E SICUREZZA NELL'ERA DEL TERRORISMO.

3. MA OGGI IL BISOGNO DI PRIVACY È DAVVERO UN'ESIGENZA DIFFUSA?

Oggi assistiamo a una specie di schizofrenia rispetto alla privacy. Da un lato, il bisogno individuale di riservatezza sembra essersi fortemente ridotto: bastino come esempi l'uso fin troppo disinvolto del telefono cellulare nei luoghi pubblici, oppure le trasmissioni televisive dove le coppie si rimproverano particolareggiate vicende d'alcova. Dal lato opposto, i fautori della protezione della privacy premono per una crescente limitazione dell'uso delle tecnologie disponibili, dal momento che queste ultime divengono sempre più potenti e raffinate: bastino come esempi le discussioni infinite sulla videosorveglianza e sul tempo per cui può essere conservata la cassetta con l'immagine di chi, ad esempio, accede a una banca. Il caso limite di eccesso di tutela mi sembra essere una sentenza del 2004 della Corte di Cassazione tedesca (*Bundesgerichtshof*), che vieta di fermare i passanti per fare pubblicità a un prodotto telefonico³³. All'estremo opposto, un caso limite di violazione della privacy è il sistema spionistico Echelon, che verrà esaminato più a fondo nel § 8.

La legislazione sulla privacy sembra ormai essersi definitivamente distaccata dall'informatica per occuparsi di ogni aspetto della vita di relazione, dalle banche di dati personali al diritto di cronaca.

Le esigenze di tutelare la privacy si scontrano anche con le crescenti esigenze di combattere una criminalità organizzata sempre più sovranazionale. Le polizie nazionali e le loro banche di dati operano in condizioni di inferiorità rispetto a una criminalità che agisce senza difficoltà al di sopra delle frontiere, anche grazie al trattato di Schengen che ha abolito i controlli di confine tra gli Stati dell'Unione Europea. La caduta della Cortina di Ferro, la permeabilità delle frontiere fra gli Stati dell'Europa centro-orientale, il fenomeno delle migrazioni dai paesi del Terzo Mondo (controllata spesso dalla criminalità organizzata), infine il fenomeno del terrorismo internazionale hanno aumentato le esigenze di controllo. La richiesta di banche sovranazionali di dati personali e di scambi internazionali di dati su criminali reali o potenziali è og-

³³ Aktenzeichen: BGH I ZR 227/01; «Süddeutsche Zeitung», 7 luglio 2004, informazione riassunta, per esempio, in pag. 18.

getto di dibattiti almeno dagli anni Ottanta³⁴. Le esigenze delle polizie sono state negli ultimi tempi rafforzate dall'immigrazione clandestina (in cui le stesse persone fanno uso di più identità false) e, infine, dal terrorismo internazionale. Oggi è proprio dalla lotta al terrorismo che vengono le più forti richieste di limitazioni della privacy.

Vorrei sottolineare che, nell'emergenza provocata dal terrorismo, è inevitabile che certe tutele avanzate della privacy vengano limitate o sospese almeno temporaneamente. Tuttavia è indispensabile che la lotta al terrorismo non diventi un alibi per annullare anche quelle tutele della privacy che non hanno rilevanza per quella lotta. Non dobbiamo dimenticare che, anche nell'emergenza, bisogna tutelare lo Stato di diritto: e non sempre è facile armonizzare le esigenze investigative con le esigenze dello Stato di diritto.

Con l'aggravarsi della criminalità e del terrorismo, la linea di frontiera tra la protezione della privacy e l'agilità investigativa si sta trasformando in una linea di frontiera fra la tutela di un diritto « di lusso » (come quello della riservatezza) e la tutela di un diritto essenziale (come quello della protezione della società), cioè, in ultima analisi, in una linea di frontiera tra la tutela dell'individuo e la tutela della collettività. Questo ha portato al radicalizzarsi delle posizioni tanto dei fautori quanto degli avversari della tutela della privacy e al sorgere di un manicheismo sulla gestione dei dati personali: non solo sulla gestione informatica, ripeto, ma su ogni forma della loro raccolta e gestione legata a una tecnologia.

4. I DOVERI DEL GIURISTA INFORMATICO DI FRONTE ALL'EMERGENZA.

Credo che oggi i giuristi informatici abbiano un duplice, preciso dovere: da un lato, ricordare ai fautori del « law and order » o della « tolleranza zero » che anche le più fondate esigenze di controllo devono rispettare i diritti individuali fondati sulle costituzioni e sui trattati internazionali; dall'altro, individuare le forme giuridiche con cui limitare quei diritti per comprovate esigenze di sicurezza nazionale, e costruirle in modo che le limitazioni siano limitate nel tempo. Ad esempio, una delle possibili tecniche legislative è quella delle leggi a termine (o *sunset laws*): queste leggi

³⁴ MARIO G. LOSANO, *Datenbanken, Datenschutz und der Kampf gegen das organisierte Verbrechen*, in MARIA-THERES TINNEFELS-LOTHAR PHILIPPS-KURT WEIS (a cura di), *Die dunkle Seite des Chips. Herrschaft und Beherrschbarkeit neuer Technologien*, Oldenbourg, München-Wien

1993, pagg. 117-135. Traduzione in catalano: *Bases de dades, vida privada i lluita contra la delinqüència organitzada*, in ANGEL SAN MARTÍN (a cura di), *Fin de segle. Incerteses davant un nou mil·leni*, Universitat de València, Ajuntament de Gandia, Valencia 1994, pagg. 287-300.

hanno una durata predeterminata, allo scadere della quale un organo parlamentare decide se sussiste ancora l'esigenza di quella limitazione e, in caso positivo, rinnova la norma per un ulteriore periodo predeterminato³⁵. In questo modo vengono contemperate le esigenze del controllo individuale legate alla lotta alla criminalità organizzata o al terrorismo internazionale, con quelle del controllo democratico sulla permanenza di leggi limitative della riservatezza individuale.

In questo momento storico, il giurista informatico non può limitarsi all'esegesi del diritto positivo, ma deve anche formulare proposte di politica del diritto assumendo, quando è necessaria, una posizione critica rispetto alle proposte legislative e al diritto positivo. Questo dovere, in realtà, dovrebbe essere proprio di ogni giurista che voglia far parte della società in cui vive, e non isolarsi da essa chiudendosi nella torre eburnea delle leggi. Tuttavia questo dovere è doppiamente perentorio per il giurista informatico, perché egli possiede anche le conoscenze tecnico-informatiche per valutare gli argomenti tecnici con cui vengono presentate alcune proposte che limitano la privacy e i diritti fondamentali: argomenti che prospettano possibilità o impossibilità tecniche inesistenti, per far accettare limitazioni altrimenti inaccettabili.

Nel 2003 avevo organizzato a Montevideo, per conto della Fondazione Alexander von Humboldt di Bonn, un congresso latino-americano dedicato a *La función mediadora del derecho como ciencia universal en una época de globalización y de lucha contra el terrorismo*. Mi permetto di ricordare un passo della mia relazione introduttiva:

Dopo il settembre 2001 a New York e l'ottobre 2002 a Mosca [ma oggi dovremmo aggiungere anche il marzo 2004 a Madrid e l'ottobre 2004 a Beslan in Cecenia] il terrorismo ha finito di essere un dramma interno — dramma che gli europei e i latino-americani, purtroppo, conoscevano bene da decenni — ed ha assunto una forma universale, legata anche a risentimenti religiosi e a sentimenti nazionalisti.

Già in passato il terrorismo interno aveva condotto a limitare anche profondamente le libertà civili dei singoli Stati contro il « proprio » terrorismo interno.

In seguito si svilupparono forme bilaterali o plurilaterali di lotta al terrorismo, dal momento che le sue radici economiche avevano tratto vantaggio dalla globalizzazione economica. Infine, da pochi mesi [ma oggi sono ormai più di tre anni] tre continenti si trovano coinvolti nella maggior impresa bellica intrapresa dopo la Seconda guerra mondiale: prima l'Afghanistan, poi l'Iraq furono oggetto di una guerra informale perché ritenuti basi del terrorismo mondiale. Ed è probabile che le « guerre preventive » non si limiteranno a questi Stati.

³⁵ Nel 2002 avevo formulato questa proposta nella conferenza di chiusura dell'anno accademico del master in informatica giuridica dell'Università di Hannover (Eulisp): *Terrorismus Bekämpfung und/oder Datenschutz*, tuttora inedita. Preciso

fin d'ora che, quando si parla di « scambio » di informazioni, si intende ormai quasi esclusivamente l'interconnessione o, almeno, l'autorizzazione all'accesso di banche di dati personali.

Ora, che cosa può dire o fare il diritto in questa situazione di conflitto non soltanto sociale e interno, ma anche militare e internazionale?³⁶

Quel congresso cercava risposte *giuridiche* alle misure *di fatto* che, sempre più spesso, venivano presentate come indispensabili per la lotta al terrorismo e, quindi, come insindacabili. In questo scritto, invece, vorrei accennare alle misure informatiche e informatico-giuridiche che vanno prendendo forma e sulle quali sarebbe opportuno che la società civile fosse dovutamente informata e che i giuristi informatici formulassero precise proposte di contenimento.

5. LE DIFFICOLTÀ NELL'INTERCONNESSIONE FRA BANCHE DI DATI ALL'INTERNO DELLO STESSO STATO.

Dopo l'11 settembre 2001, la Germania sta discutendo sulla creazione di una banca con i dati dei fondamentalisti islamici³⁷. La situazione è resa più complessa anche dalla natura federale della Germania, in cui la polizia e i servizi segreti hanno strutture statali e federali³⁸. Inoltre in Germania lo scambio di dati è ulteriormente ostacolato dalla netta separazione tra polizia e servizi segreti, alla cui attenuazione molti sono contrari. Questa separazione ha in Germania un fondamento storico: durante il nazional-socialismo, l'unione dei poteri dei servizi segreti con quelli della polizia aveva portato alla creazione della Polizia segreta di Stato (*Geheime Staatspolizei*, o Gestapo). Nella attuale realtà tedesca, le due strutture hanno funzioni diverse e sottostanno a controlli diversi e rigorosi. Per evitare una loro collaborazione diretta (che richiederebbe profonde modificazioni legislative) si è progettato un centro comune (*Lage- und Analysezentrum*) in cui far convergere le informazioni, ma anche su questa soluzione di compromesso le discussioni non sono ancora terminate.

Inoltre si discute anche sul contenuto di questa futura e indispensabile banca di dati. I fautori della privacy vorrebbero che contenesse solo l'indicazione dell'esistenza di informazioni, ma non il loro contenuto: insomma, una specie di indice delle banche

³⁶ LOSANO, *Europa y América Latina. El « viejo Occidente » y el « otro Occidente »*, in MARIO G. LOSANO-FRANCISCO MUÑOZ CONDE (org.), *El derecho ante la globalización y el terrorismo*. « *Cedant arma togae* », Actas del Coloquio Internacional Humboldt, Montevideo abril 2003. Tirant lo Blanc, Valencia 2004, pagg. 17-30.

³⁷ JOCHEN BITTNER-MARTIN KLINGST, *Von Polizisten und anderen Spionen*, « Die Zeit », 23 settembre 2004, pag. 10.

³⁸ Per esempio, le indagini a tappeto (*Rasterfahndung*: consistenti, per esempio, nel controllo di tutti gli automobilisti che transitano per una certa strada, anche se non sospetti) sono riservate ai Länder, ma il governo tedesco vorrebbe ora renderle possibili anche al Bund (cioè all'Ufficio Criminale Federale, Bundeskriminalamt, BKA), eventualmente con una modifica della Costituzione.

di dati esistenti. Altri ministri di Land sostengono invece che, in quel centro, devono confluire i dati veri e propri, cioè le informazioni complete: « La protezione dei dati, — spiegano, — non deve condurre al chiudersi di un'istituzione rispetto alle altre ». Il garante federale dei dati si è dichiarato contrario all'unione dei dati senza precise regole. Insomma, le difficoltà sono tali, che il presidente del sindacato della polizia concludeva: « Speriamo solo che il terrorismo internazionale abbia un occhio di riguardo per la precisione tedesca »³⁹.

6. LA RACCOLTA DEI DATI PER LA LOTTA AL TERRORISMO.

Per quanto difficili da interconnettere, le banche di dati vanno alimentate e il pericolo del terrorismo islamico costringe le polizie a sorvegliare anche settori prima marginali rispetto alle indagini, o addirittura esclusi da esse. Inoltre questo terrorismo è diffuso e imprevedibile: esige quindi una vasta raccolta di dati a scopo preventivo. Su questo punto è in corso in Germania una polemica che coinvolge non solo gli organi di polizia e di sicurezza, ma anche gli ordini professionali. È in questo contesto che stanno cambiando i limiti ormai trentennali delle leggi sulla privacy.

Da tempo esisteva una legge detta della « Grande Intercettazione » (*Grosser Lauschangriff*), che il 3 marzo 2004 era stata criticata in vari punti dal Tribunale Costituzionale Federale (*Bundesverfassungsgericht*): le intercettazioni dovevano essere autorizzate soltanto nei casi di reati particolarmente gravi e andavano eseguite seguendo precise procedure. Nell'estate del 2004 — dopo la tragedia di Madrid, quindi — il governo federale (una coalizione di socialdemocratici e di verdi) presentò un progetto che teneva conto delle osservazioni del Tribunale Costituzionale Federale, ma aggiungeva un punto inatteso e particolarmente controverso: tra le persone assoggettate alle intercettazioni vengono inclusi anche coloro che esercitano professioni soggette al segreto d'ufficio, cioè « medici, avvocati, consulenti fiscali, esperti in terapie antidroga, psicologi e giornalisti »: persone che hanno il diritto di rifiutarsi di prestare testimonianza su fatti conosciuti per motivi professionali. Si tenga conto che queste intercettazioni sarebbero possibili sulla base non di prove, ma soltanto di un fondato sospetto: e sulla fondatezza del sospetto deciderebbe, ovviamente, l'organo che esegue l'intercettazione.

Il corposo documento governativo (un *Referentenentwurf* di 48 pagine) precisa che negli uffici di questi professionisti possono es-

³⁹ « Süddeutsche Zeitung », 9 luglio 2004, pag. 6. Queste discussioni ebbero luogo a Kiel, durante la Conferenza dei Mi-

nistri dell'Interno tanto dei Länder quanto del Bund.

sere installate microspie se « questa misura e l'uso delle informazioni sono rese eccezionalmente necessarie da irrefutabili esigenze di un efficace perseguimento dei reati, nel rispetto del principio della proporzionalità (*Verhältnismässigkeit*) dell'intervento ». Quindi anche un parroco nel confessionale o un avvocato a colloquio col suo cliente potrebbero essere ascoltati attraverso microspie, « se vi è il sospetto di correttezza, di vanificazione della pena o di ricettazione »⁴⁰. Lo stesso vale per i parenti stretti di un indagato, benché il Tribunale Costituzionale Federale avesse dichiarato intangibile la sfera della vita privata.

In realtà, questo progetto rovescia la sentenza del Tribunale Costituzionale Federale ed è in netto contrasto con la passata politica dei socialdemocratici e dei verdi: essi infatti nel 1998, all'opposizione, avevano lottato in parlamento proprio per ottenere l'esclusione di quei gruppi professionali dalle intercettazioni. La spiegazione di questo radicale mutamento di posizione si spiega solo con la pressione che la lotta al terrorismo islamista oggi esercita su ogni forza politica non solo tedesca, ma europea.

Qualunque sia l'esito di questo progetto di legge, esso è un chiaro indice della tendenza generale — non solo tedesca, dunque — a ridurre al minimo la protezione dell'ambito privato, in contrasto con la legge sulla protezione dei dati, quando non addirittura con la costituzione.

7. L'INTERCONNESSIONE SOVRANAZIONALE DI BANCHE DI DATI NAZIONALI.

Fin qui si è parlato della difficoltà di interconnettere le banche di dati dello stesso Stato e delle tecniche di raccolta dei dati *al suo interno*. Ma ormai la delinquenza comune, la criminalità organizzata e il terrorismo sono realtà sovranazionali. Come è possibile giungere a uno scambio *internazionale* dei dati raccolti e memorizzati nei singoli Stati nazionali? Iniziamo con un caso legato alla criminalità comune.

In generale, le richieste di limitare o sospendere alcune garanzie giuridiche vengono avanzate in momenti di intensa commozione nazionale per specifici eventi criminosi, come ad esempio nell'estate del 2004, quando in Germania scoppiò il caso del *serial killer* belga Michel Fourniret, accusato di almeno una decina di omicidi di bambini in Belgio, Francia e Germania. Il suo caso rivelò una grave mancanza di circolazione di informazioni fra le polizie dei

⁴⁰ « Süddeutsche Zeitung », 7 luglio 2004, pag. 1, in cui si citano i passi tratti dal progetto governativo (il « Referentenentwurf » di 48 pagg., ricordato nel te-

sto). Un duro commento è a pag. 4 nell'articolo intitolato *A ciascuno la sua microspia*.

tre paesi e portò alla richiesta di creare « un registro europeo dei pregiudicati. Vi si dovrebbero registrare i condannati e dovrebbe essere accessibile a tutti gli Stati europei » (così il giornale olandese « De Telegraaf »)⁴¹.

Di fronte a queste richieste, in Germania il Ministero Federale della Giustizia aveva fatto presente la difficoltà (se non addirittura l'impossibilità tecnica) di unificare le banche di dati delle polizie dei 25 Stati dell'Unione Europea in un « archivio penale centrale dell'Unione Europea ». Comunque, aveva aggiunto, era indispensabile giungere a un più efficiente scambio di dati fra le polizie dei vari Stati coinvolti. In entrambi i casi — archivio centralizzato o scambio fra polizie — si dovrebbero superare gravi problemi di conflitto fra le leggi che istituiscono gli archivi o che autorizzano gli scambi e le singole leggi nazionali sulla privacy. Per la Germania si aggiungeva poi la rigida divisione, già ricordata, fra polizia e servizi segreti. « Se in futuro la polizia può servirsi come vuole dei dati dei servizi segreti, — osservava un giornale tedesco, — allora si può fare a meno dei controlli propri dello Stato di diritto previsti per le intercettazioni telefoniche da parte della polizia. [...] Già oggi si possono scambiare alcune informazioni. Chi chiede di più, mina una colonna dello Stato di diritto »⁴².

Se questo sommovimento è stato suscitato da un reato gravissimo, ma riconducibile a un solo individuo, è facile immaginare quale pressione politica e psicologica possano esercitare gli attentati terroristici degli ultimi anni.

8. ECHELON: « DAGLI AMICI MI GUARDI IDDIO, CHE AI NEMICI CI PENSO IO ».

Fin qui ci siamo mossi sul piano del rispetto delle regole formali nell'ambito della raccolta e della diffusione dei dati, nonché delle discussioni anche aspre che suscita la limitazione o riformulazione di queste regole. Ma un grave problema a livello internazionale — anzi, mondiale — si è posto a partire dal 2000 con la raccolta illegale di dati da parte di un gruppo di Stati occidentali.

L'indicazione della data è importante. Nel 1989-91 si era formalmente dissolto il blocco comunista, e il gigantesco apparato spionistico degli Stati Uniti in Europa era praticamente disoccupato. Secondo il giornale danese « Ekstra Bladet »⁴³, già dall'otto-

⁴¹ « Süddeutsche Zeitung », 7 luglio 2004, pag. 4; 8 luglio 2004, pag. 4 e pag. 6; « Frankfurter Allgemeine Zeitung », 9 luglio 2004, pag. 7.

⁴² « Süddeutsche Zeitung », 9 luglio 2004, pag. 4.

⁴³ « www.politrix.org/foia/echelon/

echelon-de-spy.htm »: riporta l'articolo di « Ekstra Bladet » del 6 marzo 2000: Bo ELKJAER-KENAN SEEBURG, *German Spies: Echelon Exists. For 18 months now, Germany's intelligence service has issued warnings against Echelon's industrial espionage*. Nella parte finale, contiene an-

bre 1998 i servizi segreti tedeschi (*Verfassungsschutz*) metteva in guardia le imprese tedesche contro la « rete illegale di spionaggio ». Il 6 settembre 2001 il Parlamento Europeo prendeva ufficialmente posizione contro l'uso a fini di spionaggio economico del preesistente sistema militare mondiale di intercettazione dei messaggi elettronici. Nasceva lo scandalo « Echelon », di cui allora si parlò poco e su cui, oggi, è calato il silenzio.

Mi limiterò a citare alcuni documenti, avvertendo che la parola « Echelon » in Internet provoca un diluvio di informazioni, sulla cui attendibilità è necessaria la massima prudenza: ben più che per altre informazioni presenti sulla rete. Per questo userò soltanto fonti ufficiali o testi giornalistici non contestati e tratti da pubblicazioni notoriamente attendibili. Per accertare se e come vi sia stato spionaggio industriale vi sono le commissioni presso il Parlamento Europeo: nel presente scritto, Echelon è rilevante perché dimostra come ormai la tecnologia sia in grado di violare in modo globale e sistematico la riservatezza delle persone fisiche e giuridiche, indipendentemente dalla singole legislazioni nazionali (e anche sovranazionali, per quanto concerne l'Unione Europea).

Una descrizione sintetica viene da « El País »⁴⁴, che riporta il comunicato del Parlamento europeo dei 6 settembre 2001:

Echelon nacque durante la guerra fredda. Ne fanno parte gli Stati Uniti, la Gran Bretagna, l'Australia e la Nuova Zelanda. Conta 120 satelliti-spia e la sua capacità tecnica include l'intercettazione di tutti i tipi di messaggio — telefonici o elettronici — trasmessi per satellite: una capacità che non può essere digerita da alcun servizio segreto, formato, in fin dei conti, da essere umani limitati. A quest'argomento è ricorsa alcune volte la Commissione Echelon per tranquillizzare l'opinione pubblica e la grande industria europea.

Tuttavia, oltre alla testimonianza di persone che ebbero occasione di operare in quella rete, alcune industrie europee hanno denunciato di nutrire fondati sospetti sul fatto di essere state spiate. Il caso più noto è quello dell'impresa costruttrice dell'Airbus, che assicurò di aver perduto un contratto di sei miliardi di dollari con il Governo Saudita perché quest'ultimo preferì il gruppo statunitense Boeing e McDonnell Douglas grazie alle informazioni ottenute per mezzo di Echelon.

Ma nel 2001 ci si doveva limitare soprattutto a supposizioni, data la segretezza del progetto. In quello stesso articolo infatti si leggeva:

Echelon esiste. È stato asserito che forse ha la capacità tecnica di intercettare tre milioni di comunicazioni al minuto. Probabilmente gli Stati Uniti hanno spiato grandi imprese e intercettato messaggi privati d'ogni tipo. L'Europa deve perciò sviluppare non soltanto dei sistemi che tutelino la riservatezza delle sue comunicazioni, ma anche un proprio servizio di spionaggio più coordinato.

che un rinvio al testo dell'*intelligence* tedesca (*Verfassungsschutz*).

⁴⁴ « www.ciberpais.elpais.es/d/200110913/cibersoc/soc1.htm »: GABRIELA

CAÑAS, *La Eurocámara reconoce que Echelon espía a Europa y quiere montar una red similar*.

Queste sono, a grandi linee, le conclusioni approvate la scorsa settimana dal Parlamento Europeo, dopo un anno di indagini. Ma i risultati di queste ultime sono stati così scarsi, che alcuni deputati sostengono ironicamente: « Echelon è come Dio: crediamo che esista, ma non abbiamo prove della sua esistenza ».

Per l'Unione Europea lo spionaggio di Echelon riveste una duplice gravità. Sul piano economico, danneggia l'economia comunitaria e altera la concorrenza internazionale. Sul piano politico, a questa azione destabilizzante partecipa uno Stato membro dell'Unione, anche se sempre al margine di essa: la Gran Bretagna. Questo spiega perché, all'inizio della polemica, sia stata addirittura negata l'esistenza di Echelon.

La notizia iniziò a circolare tra i paesi scandinavi, sempre attenti ai problemi della privacy, e la Germania, che tuttora (credo) ha a Francoforte uno dei grandi centri di ascolto del sistema detto Echelon. Un giornalista svedese elencava nel 1999 i casi a lui noti di manipolazioni della concorrenza internazionale e concludeva:

« The obvious question is naturally if this controversial information is true, and how the European Parliament will handle it. According to the press spokesman of the European Parliament, there is no decision on whether the Parliament really shall process the factual information of IC 2000 and take a stand of it is true or not »⁴⁵.

La Commissione europea negò l'esistenza di Echelon⁴⁶. Solo l'insistenza della stampa e dei ricercatori obbligò infine la NSA (U.S. National Security Agency) ad ammettere l'esistenza di Echelon⁴⁷.

La NSA, l'Agenzia statunitense per la Sicurezza Nazionale, ha reso pubblici alcuni documenti finora segreti che gettano luce sulla nascita del maggior programma di spionaggio noto fino ad oggi. Secondo questa informazione, il mega-progetto consiste in una rete internazionale dedicata all'intercettazione indiscriminata d'ogni tipo di comunicazione elettronica: telefonia, fax, Internet ecc.

L'insieme di satelliti e di sistemi informatici — facenti capo ai servizi segreti di Stati come gli USA, la Gran Bretagna e il Canada — è dedicato all'intercettazione dei messaggi su ogni canale di trasmissione. Si controllano così tanto gli utenti privati e le imprese, quanto gli uffici governativi. Gran parte di questo dispiegamento su scala mondiale usa come punti di ascolto le basi che gli USA hanno negli Stati associati a Echelon. In seguito questi dati vengono trasmessi alla NSA affinché li analizzi.

⁴⁵ « jya.com/echelon-se2.htm »: GÖRAN ANDERSSON, *U.S. Industrial Spionage is Confronted*, originalmente in « *Datateknik* » del 10 giugno 1999. Il documento IC 2000 menzionato nell'articolo è il rapporto *Interception Capabilities 2000*, che rende conto anche degli altri Stati che praticano forme simili di spionaggio elettronico.

⁴⁶ « www.politrix.org/foia/echelon/echelon-de-spy.htm »; cfr. la parte finale del già citato « *Ekstra Bladet* » del 6 marzo 2000.

⁴⁷ « www.hispasec.com/unaaldia/ 469 »: ANTONIO ROMÁN, *Documentos desclasificados confirman la existencia de « Echelon »*; corsivo mio.

Oltre alla supposta finalità militare, *tutto pare indicare che questa forma di spionaggio venga utilizzata anche a fini puramente economici*. Questo aspetto parte dalla notizia recentemente confermata della doglianza formale del Parlamento europeo contro i governi associati a Echelon per il sospetto che questa rete sia stata utilizzata per favorire le imprese nordamericane, a danno di quelle europee, nella conclusione di accordi impresariali nel mercato sudamericano.

Questi documenti sono venuti alla luce grazie soprattutto all'ostinazione dimostrata dai ricercatori della George Washington University, che fecero appello alla legge sulla libertà di informazione vigente negli USA.

Infine, il Parlamento europeo ammise l'esistenza di Echelon con un cauto comunicato⁴⁸:

La Camera ha accolto l'informativa della commissione *pro tempore* sul sistema di intercettazione Echelon con 367 voti a favore, 159 contrari e 34 astensioni. Il testo asserisce che non vi sono dubbi sull'esistenza di un sistema di intercettazione mondiale delle comunicazioni, del quale fanno parte gli USA, la Gran Bretagna, il Canada, l'Australia e la Nuova Zelanda. Sembra che questo sistema sia stato designato per qualche tempo con il nome in codice di « Echelon ».

Non v'è dubbio, continua il comunicato, che la finalità del sistema è l'intercettazione delle comunicazioni private ed economiche di natura non militare. Esso tuttavia precisa che le capacità tecniche del sistema sono probabilmente inferiori a quelle annunciate dai mezzi di comunicazione. Inoltre, nonostante le affermazioni secondo cui il sistema venne usato per ottenere vantaggi competitivi a favore delle imprese nazionali [degli Stati associati a Echelon], « non esistono prove » che questo sia stato il motivo che portò alla creazione del sistema di intercettazione. La Camera richiede inoltre agli Stati membri di impegnarsi a includere nel Trattato una clausola che proibisca lo spionaggio industriale.

Questa presa di posizione creò un grave imbarazzo, e la giornalista Gabriela Cañas commenta:

Alcuni membri della Camera, come l'indipendente italiano Maurizio Turco, chiesero una condanna della Gran Bretagna. Gli eurodeputati britannici non solo non risposero, ma neppure parteciparono al dibattito. Alcuni mezzi di comunicazione hanno asserito che Echelon ha intercettato anche milioni di e-mail di cittadini europei, al che la Commissione ha risposto che predisporrà una campagna informativa affinché la gente impari a crittografare i propri e-mail.

Però ancora una volta in quello stesso articolo si legge come la lotta al terrorismo fosse usata dal Parlamento Europeo come uno strumento per giustificare, almeno in parte, la violazione della privacy di persone giuridiche e fisiche:

Il comunicato del Parlamento deplora lo spionaggio industriale e chiede che lo si proibisca, denuncia inoltre come uno Stato membro [dell'Unione Europea] si sia prestato alle sue operazioni e, al tempo stesso, chiede una più stretta cooperazione con gli Stati Uniti per difendersi e anche per disporre di un proprio ser-

⁴⁸ « www.lainsignia.org/2001/septiembre/cyt_004.htm »: Comunicado del Parlamento Europeo, 6 de septiembre [2001], *El*

parlamento Europeo considera probada la existencia de Echelon.

vizio di *intelligence* che sia più efficiente e utile nella lotta contro il terrorismo o il narcotraffico. Insomma, delle proposte che, nel dibattito parlamentare, alcuni deputati definirono « ipocrite » e « incoerenti ».

Il silenzio che seguì a queste prese di posizione del 2000/2001 non significa che questo sistema di intercettazioni — qualunque sia il nome con cui lo si indica — sia terminato. In certi casi, esso può svolgere persino funzioni umanitarie. Così, durante il rapimento delle due volontarie in Iraq (le « due Simone »), una conferma della loro esistenza venne dalla loro voce, captata da un satellite americano sullo sfondo di un'altra conversazione: è la tecnica usata per individuare la presenza dei super-ricercati che non userebbero mai il telefono o l'e-mail. I giornali si sono prodigati in spiegazioni della tecnica « Sigint » (Signal Intelligence)⁴⁹. Dunque, nel settembre 2004 questi sistemi di spionaggio erano — comprensibilmente — in piena funzione sull'Iraq: ma è difficile escludere che non siano in funzione anche sull'Europa, specie dopo l'attentato di Madrid.

Inoltre è difficile credere che non fossero in funzione il 4 marzo 2005 in Iraq, nella strada antistante l'aeroporto, dopo il passaggio dell'ambasciatore statunitense Negroponte: il punto più sorvegliato, anche elettronicamente, di tutto l'Irak. Tanto sorvegliato che una pattuglia americana sparò sull'auto che riportava all'aeroporto la giornalista Giuliana Sgrena, appena liberata dopo il rapimento, uccidendo un agente italiano e ferendo la giornalista. I comandi americani sostengono di non essere stati avvertiti. Tutti ammettono però che da quell'auto erano partite numerose telefonate satellitari verso i vertici politici e militari italiani, per dare notizia della liberazione: è possibile che « Sigint » non avesse percepito nulla? O all'ottimo controllo delle comunicazioni è seguita una pessima comunicazione del controllo? O gli Stati Uniti — che rifiutano le trattative coi rapitori e disapprovano chi le accetta, come l'Italia — hanno voluto manifestare il loro disappunto per quella liberazione?

9. VERSO IL GROVIGLIO INESTRICABILE.

I dati raccolti con o senza il consenso degli interessati entrano dunque nella banche di dati nazionali e circolano a livello internazionale, anche se questo è vietato dai trattati internazionali e dalle leggi dello Stato di origine o di destinazione.

⁴⁹ Il sistema d'ascolto è descritto nell'articolo *Le due ragazze, segnale captato da un satellite. L'intelligence americana intercetta la voce di una delle italiane. Po-*

che parole sullo sfondo di un'altra conversazione: così il titolo a tutta pagina del « Corriere della Sera », 28 settembre 2004, pag. 3.

La lotta al terrorismo ha incrementato la raccolta legale dei dati personali. Dal 1 ottobre 2004, anche i cittadini dei 27 Stati europei finora esentati dall'obbligo di visto di entrata negli USA vengono schedati alla frontiera degli Stati Uniti con fotografia e impronte digitali. Questi dati confluiranno in una banca centrale e verranno aggiornati a ogni ingresso negli USA. William James, responsabile del «US Visit» (il programma per la schedatura dei 27 paesi VWP, Visa Waiver Program) assicura: «Il diritto dei cittadini alla riservatezza viene tutelato in modo ferreo: i dati elettronici non sono accessibili a estranei». Non è però precisato chi sia «estraneo» al programma di lotta al terrorismo e all'immigrazione illegale. E quindi possibile immaginare intrecci di dati raccolti legalmente (come quelli appena menzionati) con altri raccolti in modi non ortodossi. In teoria, la tecnica informatica consentirebbe sempre di risalire alla fonte del dato, ma in pratica quella fonte può essere fittizia (basti pensare agli hackers, che si installano in computers altrui e di lì inviano virus e worms) oppure può mancare la volontà di risalire alla vera fonte. In un futuro vicino sembra inevitabile la commistione tra dati d'ogni origine.

Echelon, Sigint e altre sigle ancora ignote non annunciano un futuro roseo per la privacy: ma almeno serviranno effettivamente nella lotta al terrorismo?

* *

Abbiamo così percorso tutta la gamma degli atteggiamenti attuali rispetto alla privacy: dal divieto di rivolgersi in strada a un passante per fare pubblicità fino al controllo indiscriminato di ogni comunicazione per via elettronica. Controllo eseguito non solo da Echelon. Quest'ultimo abuso è venuto alla luce perché coinvolge molti Stati democratici con un forte controllo parlamentare: ma il già citato rapporto del servizio segreto tedesco ricorda che strutture simili sono all'opera anche in Stati poco democratici e in «Stati canaglia».

La giusta lotta contro il terrorismo internazionale sta divenendo una giustificazione per rendere sempre meno trasparenti le azioni dei servizi segreti e sempre più frequenti le violazioni della privacy e dei diritti fondamentali. I giuristi informatici dovrebbero chiedersi quali revisioni delle leggi in vigore sono veramente indispensabili e quali misure vanno adottate per limitare allo stretto necessario le incontrollate azioni di controllo.