Legami tra sicurezza e diritti umani

Privacy ed esigenze investigative: dalla contrapposizione alla complementarietà[1]

di Giuseppe Busia[2]

Troppo spesso sicurezza e tutela dei diritti fondamentali vengono poste in alternativa, e sono raffigurate come obiettivi fra loro inconciliabili e quindi necessariamente contrapposti. Tale schematica impostazione non è però condivisibile: in un sistema che voglia dirsi democratico, infatti, le esigenze di sicurezza non possono che essere perseguite nel quadro del rispetto dei diritti fondamentali della persona. È dunque necessario passare dall'idea di una contrapposizione a quella di una doverosa ed imprescindibile complementarietà fra tali elementi.

Ed è proprio in questa luce che si tenterà di sottolineare come in particolare tale obiettivo possa (e debba) essere perseguito nel rispetto di quell'insieme articolato e complesso di diritti che ormai ricade sotto l'ombrello della protezione dei dati personali.

Diritti che, oltre a trovare una protezione di tipo costituzionale nell'ordinamento interno, come ha più volte affermato la Corte costituzionale, hanno ricevuto una consacrazione espressa anche a livello comunitario con la Carta dei diritti fondamentali dell'Unione europea (artt. 7 e 8). Diritti che, soprattutto, contribuiscono a qualificare il nostro ordinamento come democratico, aiutando a non cadere nella tentazione di credere che tutto ciò che è possibile fare, sia per ciò stesso anche lecito e moralmente accettabile.

---

[1] In corso di pubblicazione negli atti della Conferenza internazionale su CRIME AND TECHNOLOGY: NEW FRONTIERS FOR REGULATION, LAW ENFORCEMENT AND RESEARCH at the initiative of International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme/ ISPAC Centro Nazionale di Prevenzione e Difesa Sociale/ CNPDS, in cooperation with United Nations Office on Drugs and Crime/ UNODC, Vienna - Courmayeur Mont Blanc, 28-30 November (http://ispac-italy.org/pubs/Crime%20and%20Technology%20International%20Conference%20Draft%20Programme.pdf)

[2] Avvocato, giornalista pubblicista, dirige il Servizio Studi e Documentazione del Garante per la protezione dei dati personali ed è Presidente del Comitato di Appello previsto dall'art. 24 della Convenzione Europol.

Nelle pagine seguenti, dopo aver accennato ai rischi per la libertà delle persone legati alle raccolte di dati personali ed all'utilizzo delle nuove tecnologie, si indicheranno alcuni limiti insiti nell'idea che la collazione di più informazioni aiuti necessariamente le attività di indagine. Si ricorderanno quindi le principali garanzie giuridiche previste dalla normativa sui dati personali anche come limite ai trattamenti realizzati a fini di polizia, soffermandosi in particolare su alcune categorie specifiche di informazioni utilizzate in sede investigativa. Infine, ci si soffermerà sull'esperienza internazionale in materia di cooperazione ai fini di sicurezza, che può essere assunta quale valido esempio di come sia possibile bilanciare e far convivere le esigenze di sicurezza e con quelle volte a garantire la protezione dei diritti fondamentali della persona.

1. Il diritto all'oblio come diritto di libertà

Al riguardo, è sempre necessario tenere presente che ogni volta che si raccolgono e conservano dati di una persona, anche per fini certamente meritevoli, quali sono indiscutibilmente la prevenzione del crimine e la tutela della sicurezza, in qualche modo si finisce per comprimere la sua sfera di libertà. Se, infatti, si conosce qualcosa di un altro, egli perde per ciò stesso la possibilità di farlo dimenticare, eventualmente perché ha cambiato professione, comportamenti, attitudini, abitudini, idee, ecc.; perde la possibilità di nasconderlo, magari perché intende ricostruire la propria identità sulla base di un nuovo e diverso sentire (diritto all'oblio). Perde, quindi, una parte della sua libertà di scegliere e di autodeterminarsi.

Essere prigionieri del proprio passato significa non avere più la speranza di cambiare e di migliorarsi: si pensi al caso di quella prostituta -faccio esempi realmente accaduti, anche se ovviamente evito riferimenti personali- che, liberatasi dei propri sfruttatori, aveva cominciato a lavorare nel mondo dello spettacolo, conquistando anche una certa notorietà, e che ogni volta si vedeva rinfacciare il suo passato come ostacolo alla sua carriera. Ed alle tante donne che hanno avuto esperienze simili e per le quali il passato rappresenta più semplicemente un impedimento per trovare un lavoro lontano dai riflettori, far crescere una famiglia, e così ricostruire la propria identità dimenticando e facendo dimenticare un momento poco felice della loro vita.

Si pensi anche a chi ha commesso reati, ha pagato il proprio debito con la società, è riuscito a reinserirsi nel mondo del lavoro e legittimamente desidera non trovare nel proprio cammino di reinserimento -che la società avrebbe il dovere di incoraggiare e di favorire- difficoltà o veri e propri ostacoli dovuti al continuo ripresentarsi del proprio passato. Ebbene, di fronte a questi casi, occorre chiedersi quanto la pur necessaria conservazione e la consultabilità dei dati sui reati commessi favorisca il raggiungimento del fine sotteso a quella bella disposizione costituzionale –una delle più affascinanti perché impregnate di speranza nei confronti della persona- secondo cui la pena deve tendere alla rieducazione del condannato (art. 27).

Spesso, attraverso le tracce che lasciamo a causa dell'utilizzo sempre più diffuso degli strumenti elettronici, siamo noi stessi a limitare la nostra libertà ed a mettere gli altri nella possibilità di sapere di noi anche più di quanto noi stessi siamo in grado di ricordare. Si pensi –anche qui il riferimento è ad un episodio realmente accaduto- al giovane che, partecipando ad uno dei tanti gruppi di discussione presenti su Internet, aveva manifestato -per scherzo e senza crederci troppo- alcune opinioni di carattere politico. Ebbene, a distanza di anni

-quando il nostro giovane aveva completato gli studi e probabilmente maturato opinioni diverse- si è trovato a dover sostenere un colloquio di lavoro nel quale il suo esaminatore, oltre ad aver esaminato il *curriculum* che lui stesso aveva inviato, aveva avuto l'idea di consultare un motore di ricerca fra quelli più utilizzati della rete, imbattendosi -attraverso una ricerca basata sul suo indirizzo di posta elettronica- nell'opinione espressa all'interno del gruppo di discussione tanto tempo prima. Prescindendo qui dalla liceità del comportamento dell'esaminatore, questo episodio mostra come la conservazione per lungo tempo di informazioni personali, magari lasciate quasi inavvertitamente, finisce per pesare su elementi decisivi della vita di una persona, la quale, per il fatto stesso che qualcuno abbia la possibilità di accedere a tali dati, vede ridursi lo spettro delle proprie scelte e quindi l'ambito della propria sfera di libertà.

L'ordinamento non sempre può tutelare tali situazioni. A volte le tutela solo in parte, dovendo bilanciare l'anelito verso l'oblio con la protezione di altri diritti riconosciuti in capo ad altri soggetti o alla collettività. Tuttavia richiede a tutti –a cominciare da chi opera al servizio della sicurezza pubblica- di tenere sempre presente che anche la semplice conservazione di un suo può pesare sulla vita della persona a cui si riferisce. E quindi prescrive di raccogliere e conservare informazioni personali solo nel rispetto dei principi di pertinenza, non eccedenza e proporzionalità: solo se, dunque, ciò è effettivamente necessario per il perseguimento di fini ugualmente meritevoli e non è possibile perseguire i fini medesimi senza l'utilizzo di dati personali o mediante trattamenti meno invasivi.

2. Rischi e opportunità legati allo sviluppo delle nuove tecnologie

Lo sviluppo tecnologico aumenta in modo esponenziale la possibilità di raccogliere e conservare informazioni personali dei cittadini. Cresce infatti il *numero di banche* dati e la loro *interconnessione*, sia in ambito pubblico che privato: si pensi, da una parte, alla sicuramente opportuna creazione di una rete unitaria delle pubbliche amministrazioni, al fine di rendere più facili ed efficienti i rapporti con i cittadini. E, dall'altra, al numero crescente di centrali rischi private, nelle quali vengono raccolte le informazioni sui comportamenti debitori dei soggetti che chiedono denaro a prestito o acquistano beni a rate[3].

Cresce contemporaneamente la *capacità di memorizzare* le informazioni raccolte in tali archivi elettronici, rendendo possibile la conservazione di un numero sempre più elevato di informazioni personali per tempi via via più lunghi. Ciò, contemporaneamente alla predisposizione di sofisticati sistemi che consentono di *ricercare ed ordinare* i dati in modo sempre più rapido, aumentando così le possibilità di identificare i soggetti e di conoscere un maggior numero di informazioni su di essi.

Crescono anche le possibilità di raccogliere dati personali *senza che l'interessato ne abbia consapevolezza*: si pensi solo ai *cookies*, i piccoli software che vengono scaricati sull'apparecchiatura dell'utente nel momento in cui visita determinate pagine web. Alcuni di

[3] L'art. 117 del Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196) prevede che i profili legati alla protezione dei dati nella creazione e nella gestione di tali banche dati siano regolati da un apposito codice di deontologia e di buona condotta. Ed è in adempimento a tale disposizione che il Garante ha appunto promosso l'approvazione di un codice di deontologia "per il trattamento dei dati personali effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini della concessione di crediti al consumo o comunque riguardanti l'affidabilità e la puntualità dei pagamenti da parte degli interessati, individuando anche specifiche modalità per garantire la comunicazione di dati personali esatti e aggiornati nel rispetto dei diritti dell'interessato".

essi sono necessari per garantire un utilizzo funzionale dei siti medesimi, ma altri arrivano a raccogliere un gran numero di informazioni su chi naviga in rete, con particolare riferimento ai siti visitati, e quindi ai gusti e agli interessi di tali persone.

Da ultimo, cresce la *convenienza economica* a raccogliere e trattare i dati. Le tecnologie hanno infatti reso meno costose –e, quindi, più diffuse- alcune forme di intrusione nella vita privata altrui: si pensi al riguardo solamente al fenomeno dello spamming, che ha raggiunto dimensioni tali da portare ad interventi legislativi volti a contenerlo anche Paesi come gli Stati Uniti, che fino a oggi avevano ritenuto di potersi affidare unicamente alla "mano invisibile" del mercato per affrontare tali problematiche.

Tutto questo si lega inesorabilmente ad un aumento della nostra vulnerabilità non solo con riferimento alla nascita di nuovi reati, specificamente basati sull'uso di tali tecnologie (si pensi ai cosiddetti *computer crimes*), ma –per quello che qui più interessa- con la via via più ampia diffusione di cosiddetti "furti di identità", legati al fatto che sempre più spesso siamo rappresentati non già dalla nostra immagine reale, ma da codici o segni identificativi trasmessi sulle reti di comunicazione elettronica, che possono però essere duplicati ed utilizzati impropriamente da persone terze rispetto a quella cui si riferiscono e appartengono.

In generale, quindi, si registra un aumento complessivo dei rischi di un uso improprio delle banche dati che si riflette inevitabilmente sulle attività investigative. Ciò, sia per quanto attiene all'utilizzo delle diverse banche dati esistenti per finalità di polizia sia per ciò che riguarda la creazione di appositi archivi elettronici per finalità di sicurezza e repressione del crimine.

Il continuo progresso delle nuove tecnologie rappresenta ovviamente un'opportunità che la nostra società deve sfruttare fino in fondo. La diffusione ed il sempre più ampio utilizzo di esse da parte delle diverse categorie di utenti costituisce quindi insieme un sintomo ed una conseguenza dello sviluppo anche in senso democratico della nostra società.

Anche in questo caso, tuttavia, è necessario tenere sempre presente che, almeno tendenzialmente, quanto più tali tecnologie sono sofisticate e –parallelamente- quanto più sono utili e semplificano la vita quotidiana, tanto più il loro utilizzo implica che chi se ne serve lasci tracce elettroniche: dati che volta a volta indicano quando si è utilizzato quel determinato servizio, per quanto tempo, per quale ragione, dove si era in quel momento, con quali altri soggetti si è eventualmente interagito attraverso lo strumento utilizzato, ecc.

L'insieme di queste informazioni, anche quando appaiono esteriori e poco invasive, dice in realtà molto delle relazioni intrattenute da una persona. Se poi tali dati vengono conservati per lunghi periodi –come appunto le medesime tecnologie permettono a costi sempre inferiori- allora è possibile ricostruire l'intera rete delle relazioni sociali intrattenute da una persona nel tempo, arrivando in certi casi a ricordare di esse più di quanto gli stessi interessati siano a volte in grado di fare.

Tali considerazioni valgono anche per quei sistemi che sembrano garantire l'anonimato degli utenti, come accade per diversi servizi offerti attraverso le reti di comunicazione elettronica. Servizi che, invece, al di là delle apparenze, consento quasi sempre l'identificazione degli utenti. Ciò, a meno che non si utilizzino accorgimenti o tecnologie particolarmente sofisticate, quali quelle che vengono utilizzate da coloro che hanno ragioni particolari per rimanere anonimi, ad esempio perché stanno commettendo o hanno intenzione di commettere un reato.

3. I limiti insiti nell'idea che la raccolta di più informazioni aiuti necessariamente le attività di indagine

E siamo così ad uno dei diversi paradossi contro i quali sembra scontrarsi chi sostiene raccolte sempre più massive di informazioni personali al fine di prevenire e reprimere i reati: nei grandissimi archivi di informazioni finiscono per confluire i dati di tutti i cittadini… tranne quelli di coloro che più di altri avevano interesse a che ciò non avvenisse, in quanto avevano maggiore interesse a sfuggire a tale raccolta: innanzi tutto chi ha commesso o intende commettere dei crimini.

Occorre inoltre tenere presente che -come sempre più spesso riconoscono anche gli organismi incaricati di tutelare la sicurezza pubblica- le raccolte indiscriminate di dati, oltre ad essere eccedenti rispetto ai fini perseguiti (e quindi realizzate in violazione dei principi cui si è fatto cenno più sopra) non sempre portano un reale giovamento ai fini di polizia. Ed infatti, molto spesso l'eccesso di informazioni riduce la qualità della stesse e finisce per ritardare il raggiungimento degli obiettivi investigativi. Ciò, anche quando tali raccolte indiscriminate di dati non nascondono in realtà carenze nella capacità investigativa.

Infine, è sempre necessario considerare che la raccolta e la conservazione dei dati per lunghi periodi di tempo comporta costi molto elevati che -direttamente o indirettamente- finiscono per ricadere sulla collettività. Questo, sia attraverso gli oneri sostenuti dalle imprese, che li scaricano sugli utenti, sia attraverso i costi addebitati ai soggetti pubblici, che vengono fatti ricadere sui contribuenti.

Per ciò che qui maggiormente interessa, si deve pertanto certamente riconoscere che il progresso nelle tecnologie crea importanti opportunità anche con specifico riferimento all'utilizzo delle tecnologie medesime ai fini di indagine, determinando un aumento quantitativo e qualitativo degli strumenti posti a disposizione di chi opera in tale settore. Si deve però anche evidenziare non solo che tale utilizzo deve sempre mantenersi nei limiti posti dalla normativa sulla protezione dei dati a tutela delle persone, ma altresì che esso, anche a causa delle sua estensione, può veder ridotta la propria efficacia proprio rispetto ai fini perseguiti.

4. La risposta della normativa sui dati personali e gli obblighi posti a carico delle forze di polizia

Contro questi rischi, la normativa sulla protezione dei dati ha approntato una serie di tutele, volte in generale non solo ad evitare che altri si introducano nella vita privata di una persona contro la sua volontà, secondo la tradizionale concezione della privacy, intesa come diritto ad essere lasciati soli. Ma anche a consentire di decidere che uso gli altri possono fare dei dati che li riguardano, scegliendo non solo se un terzo può conoscere una determinata informazione personale, ma anche per quali fini può utilizzarla, per quanto tempo può conservarla, a chi può comunicarla, ecc. La protezione dei dati è divenuta così diritto all'auto-determinazione informativa, raccogliendo sotto il proprio ombrello un numero crescente di diritti che, in nome della tutela della persona e della sua dignità, abbracciano e insieme arricchiscono diritti tradizionali quali quello all'identità personale, all'immagine o alla libertà di manifestazione del pensiero. In tal modo, esso acquista una propria autonomia che è stata consacrata in una serie di testi costituzionali e poi anche dalla Carta dei diritti fondamentali dell'Unione europea.

La normativa comunitaria ed italiana basano innanzi tutto la tutela su alcuni principi fondamentali –ai quali si è già accennato- che trovano piena applicazione anche per i trattamenti svolti dalle forze di polizia e, in generale, da tutti i soggetti comunque impegnati nella tutela della sicurezza. Si tratta dei principi di pertinenza (la polizia può raccogliere e conservare i soli dati che abbiano un significato per le indagini), non eccedenza (non può raccogliere dati eccedenti rispetto a quelli necessari), ragionevolezza e proporzionalità fra il fine perseguito e il trattamento realizzato.

Di più: poiché le forze di polizia, a differenza di quanto avviene per la generalità degli altri soggetti, non sono tenute né ad informare gli interessati del fatto che utilizzano i loro dati né a chiedere loro il consenso, ed hanno inoltre la possibilità di trattare le informazioni personali con molte meno restrizioni (cfr. artt. 53 ss del Codice in materia di protezione dei dati personali, decreto legislativo 30 giugno 2003, n. 196, di seguito anche, Codice privacy), è necessario che applichino i principi prima richiamati con particolare rigore.

Ed infatti, proprio i minori controlli che ogni interessato può effettuare sul loro operato -a causa, fra l'altro, dell'assenza di informativa e della mancata necessità di un consenso dello stesso interessato- impongono un "auto-controllo" particolare sia nella cernita dei dati da raccogliere, sia nella fissazione dei relativi tempi di conservazione, sia, infine, nell'individuazione dei soggetti che volta possono accedere ai diversi insiemi di informazioni volta a volta necessarie.

5. Il regime specifico di alcune categorie di dati personali

Fatte tali considerazioni di carattere generale, conviene soffermarsi sulla disciplina specifica di alcuni tipi di informazioni personali che assumono particolare rilievo e sono spesso utilizzate a fini di indagine dalle forze deputate alla tutela della sicurezza pubblica. Ciò, anche al fine di mostrare come i principi sopra richiamati abbiano trovato esplicazione nel regime particolare di alcune categorie di dati.

5.1 I dati sul traffico

Per il loro rilievo intrinseco nonché per l'acceso dibattito che ha accompagnato la loro regolamentazione, è opportuno partire dai dati relativi al traffico telefonico e telematico. Il Codice privacy, seguendo alla lettera la direttiva n. 58 del 2002 a cui ha dato attuazione, considera dato sul traffico "qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione". Dunque, una definizione estremamente ampia, che discende dall'impostazione fatta propria dalla più recente normativa comunitaria. Quest'ultima, preso atto della crescente convergenza fra strumenti quali i telefoni, i computer ed anche i televisori, ha adottato un approccio "tecnologicamente neutro" e -fatte salve alcune specificità- tende a prevedere una disciplina comune per tutte le comunicazioni elettroniche, indipendentemente dal terminale volta a volta utilizzato per effettuarle.

Per questo, nella nozione di dati relativi al traffico rientrano non solo le telefonate su terminali fissi o mobili (attraverso cui si realizzavano "chiamate", cioè le connessioni che consentono una comunicazione bidirezionale in tempo reale: cfr. art. 4, comma 2, lett. *b)*, d.lgs. 196/2003), ma anche gli altri tipi di comunicazione elettronica, quali in particolare, i fax, gli sms, gli mms e le e-mail.

Prima di descriverne la disciplina, occorre, però, un chiarimento di base: i dati sul traffico non riguardano il contenuto delle conversazioni o dei messaggi, ma solamente alcune

informazioni "esteriori", quali i numeri o gli indirizzi di posta elettronica fra i quali interviene la comunicazione ed il momento in cui la stessa è avvenuta. E allora –si dirà- quali rischi potrà mai comportare la loro raccolta e conservazione? In realtà, mettendo insieme le informazioni sui numeri chiamati da un soggetto è possibile ricostruire la rete delle sue relazioni personali e sociali. Verificando se le telefonate fra due persone sono più o meno frequenti, se durano poco o molto, e se vengono effettuate in ore serali piuttosto che in orari d'ufficio, si riesce ad intuire che tipo di rapporti esistono fra i due interlocutori.

Per tale ragione, la Corte costituzionale, ben prima dell'entrata in vigore della normativa sui dati personali, aveva inequivocabilmente ricordato come "l'ampiezza della garanzia apprestata dall'art. 15 della Costituzione alle comunicazioni… è tale da ricomprendere non soltanto la segretezza del contenuto della comunicazione, ma anche quella relativa all'identità dei soggetti e ai riferimenti di tempo e di luogo della comunicazione stessa" (sent. n. 81 del 1993).

Per la medesima ragione, come accennato, queste informazioni sono regolate da una serie di disposizioni specifiche sia nelle direttive comunitarie sia nella legislazione italiana che ha dato loro attuazione. Il Codice privacy prevede infatti, in generale, che i dati sul traffico devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione elettronica (art. 123). Tuttavia, il fornitore dei servizi è autorizzato a trattare le informazioni strettamente necessarie ai fini della fatturazione e dei pagamenti per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale. È poi consentito un ulteriore trattamento nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, ma solo dietro consenso dell'abbonato o dell'utente, che possono revocarlo in ogni momento. Tutto ciò, con specifiche garanzie riguardanti sia l'informativa da fornire agli interessati sia alcune limitazioni all'accesso a tali informazioni da parte dei soggetti che lavorano per conto del fornitore di servizi[4].

Oltre ai trattamenti necessari alla gestione del contratto, il Codice privacy aveva previsto –per quel che qui maggiormente interessa- che i soli dati relativi al traffico *telefonico* (con esclusione, quindi, di quelli riguardanti le altre comunicazioni realizzate sulle reti telematiche) potessero essere conservati per due anni e mezzo dal fornitore ai fini di accertamento e repressione dei reati. Ciò, secondo modalità da individuare attraverso un decreto ministeriale adottato su parere conforme del Garante (art. 132).

Nel tentativo di ampliare i confini di quest'ultima disposizione, ritenuta troppo limitativa per le esigenze di indagine, alla vigilia dell'entrata in vigore del Codice privacy il Governo aveva approvato un decreto legge (n. 354 del 2003), con cui era stato previsto un allungamento fino a cinque anni dei tempi di conservazione dei dati sul traffico telefonico ed un'estensione delle medesime regole anche per le comunicazioni su Internet, nonché una proroga -addirittura fino al 2006- della vecchia normativa (il d.lgs. 171 del 1998), che invece avrebbe dovuto cessare di essere applicata dal primo gennaio scorso. Con ciò, riducendo

[4] A questo riguardo, può essere utile ricordare che il Gruppo dei garanti europei previsto dalla direttiva n. 95/46/CE, occupandosi di "the storage of traffic Data for billing purpose", ha concluso i lavori, affermando che "reasonable interpretation of the directives is that this should ordinarily involve a routine storage period of maximum 3-6 months, with the exception of particolar cases of dispute where the data may be processed for a longer period".

notevolmente le garanzie di libertà di ciascun cittadino, seppure per l'encomiabile fine di reprimere i reati.

Tali tempi di conservazione erano ben superiori a quelli previsti in altri Paesi europei, che pure hanno dovuto fare fronte all'emergenza del terrorismo dopo gli attentati del 2001 e che incontrano notevoli difficoltà ad introdurre tempi di conservazione anche molto più ridotti. Ciò, anche a causa della resistenza opposta non solo delle organizzazioni che tutelano i diritti civili ma, in generale, di tutti i soggetti che sono abituati a prendere sul serio disposizioni quali quelle previste a protezione della vita privata nella Carta dei diritti fondamentali dell'Unione europea (si vedano i già richiamati articoli 7 e 8).

Fortunatamente, però, dopo una mobilitazione di istituzioni e cittadini, il Parlamento ha imposto un deciso cambiamento di rotta. Così la legge di conversione del decreto ha limitato nuovamente l'ambito di applicabilità dell'art. 132 del Codice privacy ai soli dati telefonici, e ne ha previsto inizialmente la conservazione per due soli anni (invece che i due e mezzo previsti dal provvedimento di necessità e di urgenza). Decorso tale periodo, le stesse informazioni possono essere conservate per altri due anni (invece che altri due e mezzo) esclusivamente per finalità di repressione dei soli delitti di cui all'art. 407, comma 2, lett. *a)*, c.p.p. (per i quali il termine di durata delle indagini è superiore a quello ordinario) nonché di quelli in danno di sistemi informatici o telematici.

[*A differenza del testo originario del Codice, il provvedimento di necessità e urgenza aveva disciplinato nel dettaglio pure le modalità di acquisizione dei dati. Ed anche in tale ambito la legge di conversione ha provveduto ad introdurre una serie di modifiche tendenti ad offrire maggiori garanzie, stabilendo in particolare che sia sempre il giudice (e non anche il pubblico ministero) a disporre l'acquisizione dei dati d'ufficio o su istanza di una delle parti. Inoltre, decorsi i primi due anni, il giudice può autorizzare l'acquisizione solo se vi sono indizi sufficienti con riguardo ai delitti prima richiamati. Da ultimo, il Parlamento ha anche deciso di affidare al Garante (invece che al Ministro della giustizia) la definizione -attraverso un provvedimento emanato ai sensi dell'art. 17 del Codice privacy- delle misure e degli accorgimenti a garanzia dell'interessato, così accrescendo le garanzie a tutela della riservatezza.*

Oppure, in sostituzione del capoverso in corsivo sottolineato qui sopra:

Da ricordare inoltre che, mentre il Codice privacy, nella sua stesura originaria, non aveva regolato le procedure attraverso cui i dati sarebbero stati conservati ed acquisiti, limitandosi a rinviare ad decreto del Ministro della giustizia (da emanarsi su parare conforme Garante), il dl 354 prima e la legge di conversione poi hanno invece dettato una disciplina dettagliata al riguardo. Ed anche qui, le novità introdotte dal Parlamento si rivelano particolarmente rilevanti ed opportune.

Il decreto legge aveva infatti previsto -almeno per il primo periodo di conservazione, relativo all'accertamento di tutti i reati- che i dati potessero essere acquisiti anche dal pubblico ministero senza l'autorizzazione del giudice (era infatti richiesto solamente un "decreto motivato dell'autorità giudiziaria" che, durante le indagini preliminari, può essere emanato anche dal PM). Inseguito alla conversione in legge, invece, proprio in ragione della particolare delicatezza rivestita anche dai dati sul traffico, ai fini dell'acquisizione degli stessi, è sempre richiesto (anche per i primi due anni) un decreto motivato del giudice, al quale possono indirizzare le proprie istanze il pubblico ministero, il difensore dell'imputato,

della persona sottoposta alla indagini, della persona offesa e della altre parti private. Regole per molti versi analoghe si applicano anche al secondo periodo di conservazione (i successivi due anni): tuttavia, in questo caso, al giudice è richiesta una valutazione più stringente sull'effettiva sussistenza di "sufficienti indizi" dei particolari delitti a cui si è fatto riferimento più sopra.

Si deve altresì sottolineare che, per il primo periodo di conservazione dei dati, il difensore dell'imputato o della persona sottoposta alle indagini può richiedere direttamente al fornitore i dati relative alle utenze intestate al proprio assistito con le modalità proprie delle indagini/investigazioni difensive). Tale precisazione, che non riguarda il pubblico ministero, non può essere ricondotta esclusivamente ad una svista derivante dal modo disordinato con cui si è proceduto ad approvare emendamenti e contro emendamenti durante l'iter di conversione, ma trova giustificazione sia come esplicazione del diritto di difesa di cui all'art. 24 Cost., sia in rapporto al generale diritto di ogni persona di accedere alle informazioni che la riguardano quando queste siano detenute da terzi (art. 7, Codice privacy). Informazioni fra le quali, come ha più volte chiarito il Garante per la protezione dei dati personali, rientrano anche i dati delle chiamate telefoniche effettuate. Il riferimento qui è alle chiamate in uscita, mentre per quelle in entrata, vige il limite di cui all'art. 8, comma 2, lett. f) del Codice privacy, opportunamente richiamato dalla legge di conversione (che consente comunque l'accesso nel caso in cui dalla mancata conoscenza dei dati possa derivare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 397 del 2000).

Da ultimo, occorre notare che la legge di conversione ha opportunamente affidato al Garante (e non più a un decreto ministeriale, come stabiliva il dl 354) il compito di individuare le misure e gli accorgimenti posti a garanzia delle persone a cui si riferiscono i dati sul traffico (da prescriversi sulla base delle regole relative al cosiddetto prior checking di cui all'art. 17 Codice privacy), in parte delineate direttamente dal legislatore (si veda il nuovo art. 132, comma 5 del Codice privacy). Tale sottolineatura assume rilievo anche perché lo stesso legislatore ha voluto collegare la fine del regime transitorio (che proroga le vecchie disposizioni prevedendo di fatto la conservazione dei dati per cinque anni) non già ad un termine troppo lontano nel tempo -il 31 dicembre 2005- secondo quanto inizialmente previsto dal decreto legge, ma all'emanazione del provvedimento del Garante appena richiamato (cfr il nuovo comma 6-bis introdotto nell'art. 181 del Codice privacy dall'art. 4 della legge di conversione). In tal modo, si è giustamente voluto far sì che le nuove disposizioni entrino in vigore non appena sarà completato il quadro della disciplina, senza indugiare in un poco garantista regime transitorio, ormai privo di ogni plausibile giustificazione].

5.2. I dati sulla localizzazione

Fra le informazioni più delicate e insieme più preziose ai fini dello svolgimento delle indagini di polizia, occorre anche ricordare i dati relativi all'ubicazione, ossia le informazioni che indicano la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica. Questi dati non solo consentono la localizzazione del soggetto, ossia di individuarne con estrema precisione la latitudine, la longitudine, l'altitudine e la direzione di movimento, ma possono contemporaneamente offrire uno spettro significativo della personalità del soggetto medesimo. Il loro trattamento è infatti generalmente connesso alla fornitura dei cosiddetti servizi "a valore aggiunto", quali, ad esempio, la descrizione dei

luoghi circostanti, l'indicazione di dove si trovano gli esercizi commerciali di una determinata categoria che si stanno cercando, o il controllo a distanza di veicoli, animali o persone.

Si vanno inoltre diffondendo servizi che consentono la localizzazione di soggetti terzi, diversi da quello che ha richiesto l'informazione: sono infatti già offerti commercialmente sevizi diretti a localizzare tutte le persone di cui si possiede il numero di telefono mobile, purché queste ultime mantengano il proprio terminale acceso e si siano iscritte ad un'apposita lista. Lista, che potrebbe essere costituita da un gruppo di amici o di familiari (nel cui ambito tale trattamento può comunque creare problemi molto delicati, nonostante le cautele previste dalla legge, sulle quali ci si soffermerà fra breve). Ma che non è escluso possa scivolare verso forme di controllo dei dipendenti da parte del datore di lavoro, a dispetto dei divieti relativi al controllo a distanza dei lavoratori.

Per dare un'idea della rapida diffusione di tali servizi, basti pensare che, fino a pochi mesi fa, si è discusso anche animatamente sulla legittimità dell'utilizzo di "braccialetti elettronici" per controllare i movimenti dei detenuti in libertà vigilata. L'estate scorsa uno strumento per molti versi analogo è stato usato nelle spiagge dalle mamme apprensive, al fine di evitare che i propri bambini si allontanassero troppo…

È di tutta evidenza il fatto che la conoscenza di tali informazioni offre la possibilità di ricostruire con precisione le diverse azioni compiute (si pensi al caso in cui sia stato chiesto dove si trova il benzinaio o il ristorante più vicino) o gli interessi (ogni volta in cui sia stata richiesta una data informazione sul luogo in cui ci si trova) della persona che ha fruito o è stata oggetto del servizio, fino a delinearne con precisione la personalità. È inoltre chiaro che la conoscenza di tali dati diviene tanto più significativa -e quindi pericolosa per la tutela degli interessati- quanto più a lungo gli stessi vengono conservati, magari con il fine apparentemente utile di personalizzare meglio il servizio offerto: d'altra parte, è proprio questa la logica dei servizi a valore aggiunto.

In ragione dei rischi specifici connessi al loro trattamento, il Codice privacy, coerentemente con quanto previsto dalla direttiva n. 58 del 2002, dedica a queste informazioni una disciplina specifica rispetto ai dati relativi al traffico sui quali ci si è appena soffermati. Più in particolare, i dati sull'ubicazione possono essere trattati solo se resi anonimi o se l'utente o l'abbonato hanno manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto. Anche dopo la manifestazione del consenso, inoltre, l'utente e l'abbonato conservano il diritto di richiedere, gratuitamente e mediante una funzione semplice, l'interruzione temporanea del trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni (art. 126).

Il fornitore del servizio, prima di richiedere il consenso, è altresì tenuto ad informare gli interessati sulla natura dei dati che saranno sottoposti al trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che gli stessi siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto.

Infine, come ulteriore cautela, il Codice privacy ha previsto che il trattamento di queste informazioni sia consentito unicamente ad incaricati del trattamento che operano sotto la diretta autorità del fornitore del servizio di comunicazione elettronica o, a seconda dei casi, del fornitore della rete o del terzo che fornisce il servizio a valore aggiunto. In ogni caso, il trattamento deve essere limitato a quanto è strettamente necessario per la fornitura del servizio e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

5.3. Videosorveglianza e rilevazioni biometriche

Particolarmente rilevanti ai fini delle attività di polizia sono anche le informazioni personali ricavabili attraverso gli impianti di videosorveglianza, il cui crescente utilizzo a fini di protezione delle persone o della proprietà, pur trovando spesso giustificazione in esigenze di sicurezza, comporta un'intrusione sempre più penetrante nella sfera privata degli individui.

Con frequenza crescente, inoltre, tali sistemi vengono in vario modo combinati con sofisticati strumenti diretti a garantire l'identificazione delle persone attraverso "rilevazioni biometriche" (geometria del volto, dell'iride, ecc…), che consentono di porre a confronto le informazioni rilevate con quelle preventivamente memorizzate.

Nessuno mette in dubbio l'utilità ed a volte l'indispensabilità dell'uso di tali tecnologie per garantire la sicurezza dei cittadini. Tuttavia è chiaro che anche in questo caso è necessario garantire un adeguato bilanciamento fra tali esigenze e quelle legate al rispetto dei diritti fondamentali delle persone, che non possono essere condannate a vivere sotto il perenne controllo altrui, anche quando questo fosse effettuato a loro vantaggio.

Gli organismi preposti alla tutela dei dati personali si sono pronunciati più volte su tali problematiche, sia in sede di Consiglio d'Europa che in sede comunitaria. Ed anche il Garante italiano, oltre ad aver predisposto un apposito decalogo sull'uso di tali strumenti, si è trovato ad intervenire innumerevoli volte per contenerne utilizzi eccedenti o comunque non consentiti. Anche in questo caso, i principi-guida sono quelli sopra richiamati della pertienza, della non eccedenza e della proporzionalità, che vietano le raccolte generalizzate di informazioni personali non riconducibili a situazioni di concreto rischio legate a circostanze obiettive.

Principi, questi, che devono improntare non solo la fase di raccolta delle informazioni (ad esempio, evitando di istallare un numero eccessivo di telecamere, tenendole accese solo quando sono realmente necessarie, orientandone la direzione in modo da non riprendere dati eccedenti, ecc.). Ma anche –ed è sicuramente l'elemento più rilevante per gli impieghi effettuati a fini investigativi- la fase successiva della conservazione dei dati.

Al riguardo, vige la regola secondo cui le riprese devono essere cancellate non appena non risultino più necessarie per le finalità perseguite, mentre l'accesso alle stesse può in certi casi essere consentito unicamente alle forze di polizia nel caso di compimento di un evento criminoso. Tutto questo esclude che i sempre più diffusi impianti di videosorveglianza possano condurre alla conservazione sistematica delle riprese nel tempo, essendo questa consentita solo se giustificata dal verificarsi di particolari eventi. Ciò, nonostante si abbia consapevolezza dell'utilità che tali riprese possono rivestire e concretamente hanno rivestito nelle indagini relative a diversi delitti.

Con specifico riferimento alla videosorveglianza, occorre infine ricordare che la materia troverà più completa e organica sistemazione in un apposito codice di deontologia e di buona condotta "per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini", che dovrà prevedere specifiche modalità di trattamento e forme semplificate di informativa all'interessato al fine di garantire la liceità e la correttezza dei trattamenti (cfr. art. 134 Codice privacy).

5.4. I dati genetici

I principi generali sopra descritti trovano un'applicazione evidentemente più stringente per quanto attiene a dati particolarmente delicati quali quelli genetici, sempre più spesso

utilizzati a fini identificativi nell'ambito delle indagini di polizia. Fra i dati idonei a rivelare lo stato di salute, le informazioni genetiche costituiscono infatti quelle più intime, potendo fra l'altro esporre ai maggiori rischi di discriminazione. Ciò, sia in quanto rappresentano un elemento permanente, non modificabile da parte dell'interessato; sia perché contengono informazioni riguardanti, oltre che la persona a cui si riferiscono in via diretta, anche i suoi congiunti. Sia, infine, perché consentono di guardare non solo alla sua storia passata, ma anche a quella futura. È questo, ad esempio, il caso delle tecniche della "medicina predittiva", capaci di individuare eventuali malattie ad insorgenza tardiva e, quindi, di prevedere passaggi della vita futura che si potrebbe avere interesse a non conoscere o, sicuramente, a non rivelare.

In ragione di queste loro caratteristiche, il trattamento dei dati genetici, da chiunque effettuato, è consentito nei soli casi previsti da un'apposita autorizzazione rilasciata dal Garante, sentito il ministro della salute, il quale deve a tal fine acquisire il parere del Consiglio superiore di sanità. È stato inoltre previsto che tale autorizzazione dovrà contenere, fra l'altro, l'indicazione degli elementi da inserire nell'informativa, con particolare riferimento alla specificazione delle finalità perseguite e dei risultati conseguibili in relazione a notizie inattese che possono essere conosciute per effetto del trattamento dei dati nonché al diritto di opporsi al medesimo trattamento per motivi legittimi (art. 90, Codice privacy).

6. La cooperazione internazionale in materia di sicurezza

Il fatto che le esigenze connesse alla tutela della sicurezza e quelle legate alla protezione dei dati personali possano e debbano convivere, trova conferma nell'esperienza dell'Unione europea. In tale ambito, infatti, attraverso una serie di accordi internazionali, si è dato vita a diversi organismi che, da un lato, mirano a garantire la sicurezza pubblica dei cittadini dell'Unione; e, dall'altro, improntano la loro azione al rispetto del diritto alla riservatezza dei soggetti volta a volta interessati.

In questo contesto, merita innanzi tutto attenzione la convenzione Europol (ratificata in Italia dalla legge 23 marzo 1998, n. 93), che rappresenta uno dei più organici tentativi di dare alla cooperazione internazionale delle forze di polizia una coerente strutturazione all'interno dell'architettura europea. Essa mostra in tal modo anche come -ben prima che il terrorismo internazionale manifestasse le sue potenzialità offensive con l'intensità degli ultimi anni- fosse già presente a tutti l'importanza di tali modalità di collaborazione. Ciò, soprattutto al fine di combattere le diverse forme di criminalità che sempre più spesso traggono forza proprio dalla loro capacità di operare attraverso i confini nazionali.

Ebbene, tale convenzione, in analogia a quanto accade per altre forme di regolamentazione del settore, dedica uno spazio amplissimo alla tutela dei dati personali, ed evidenzia in tal modo come sia possibile –oltre che doveroso- ottenere buoni risultati in campo investigativo ed insieme assicurare elevati livelli di garanzie per la protezione dei diritti fondamentali della persona.

Il primo e generalissimo vincolo disposto all'azione di Europol attiene alla necessità di rispettare i principi della convenzione del Consiglio d'Europa del 28 gennaio 1981 e della raccomandazione R(87)15 del 17 settembre 1987 del Comitato dei ministri del Consiglio d'Europa.

Inoltre, proprio al fine di assicurare una completata protezione dei dati personali, la Convenzione Europol ha previsto una tutela articolata su due livelli: nazionale e sovranazionale.

A livello nazionale, ciascuno Stato membro ha designato un'autorità di controllo nazionale (in Italia, il Garante per la protezione dei dati personali: cfr. art. 4, comma 2, legge n. 93/1998), con il compito di accertarsi, in modo indipendente e nel rispetto della legislazione nazionale, che l'introduzione, la consultazione e la trasmissione all'Europol di dati personali, da parte dello Stato membro, avvengano in modo lecito e che non siano lesi i diritti delle persone. Inoltre, è stato conferito ad ogni cittadino il diritto di chiedere alla stessa 'autorità di controllo nazionale di verificare la legittimità dei trattamenti che lo riguardano.

A livello sovranazionale è stata invece istituita un'Autorità di controllo comune, con il compito di vigilare sull'attività di Europol per accertarsi che i trattamenti dei dati da esso realizzati non ledano i diritti delle persone. Tale organismo è composto da due rappresentanti per ogni Stato membro e, nelle more dell'adesione dei dieci nuovi Paesi membri, i rappresentanti di questi ultimi vi hanno partecipato nella veste di osservatori.

Ciascuno degli Stati membri è inoltre chiamato a designare, nell'ambito dei componenti dell'ACC, un proprio rappresentante presso il Comitato di appello previsto dall'art. 24 della Convenzione. Tale Comitato ha il compito di decidere in via definitiva sui ricorsi presentati dai cittadini contro le eventuali violazioni della normativa addebitabili ad Europol. Chiunque, infatti, ha il diritto di chiedere all'autorità di controllo comune di verificare la legittimità e la correttezza dell'eventuale memorizzazione, rilevamento, trattamento ed utilizzazione di dati di carattere personale che lo riguardano, effettuati presso l'Europol.

La Convenzione Europol ha inoltre tenuto presente l'esigenza che la cooperazione si estenda anche a Stati che non sono membri dell'Ue: è stata infatti positivamente prevista un'articolata procedura per la stipula di accordi bilaterali con Stati e organismi terzi, nei quali sono disciplinate le modalità attraverso cui Europol può ricevere (cfr. l'Atto del Consiglio del 3 novembre 1998 (OJ C 26, 30.01.99) o comunicare i dati a tali soggetti (si veda l'Atto del Consiglio del 12 marzo 1999 (OJ C 88, 30.03.99). Procedura, questa, che vede significativamente coinvolta anche l'Autorità di controllo comune, chiamata ad esprimere sia un parere sull'adeguatezza dell'ordinamento dello Stato o dell'organismo terzo ai fini dell'avvio delle negoziazioni. Sia un parere definitivo sull'accordo, prima della sua conclusione.

Fino ad oggi l'Autorità ha formulato il proprio parere su numerosi accordi, fra i quali è qui utile richiamare almeno quello con Interpol e quello con gli Stati Uniti d'America, il cui iter era stato avviato in seguito agli eventi dell'11 settembre 2001 ed è giunto a conclusione con la firma nel dicembre 2002. Iter che, in considerazione delle particolari condizioni che si erano create dopo tali eventi, nonché dell'assoluta specificità della regolamentazione adottata dagli USA in materia di protezione dei dati, ha visto alcuni rappresentanti dell'ACC prendere parte direttamente a diversi incontri con i rappresentanti USA sia presso L'Aia che a Washington, sebbene con il ruolo di osservatori. Ciò, ancora una volta a significare il peso assolutamente determinante che la disciplina sulla protezione dei dati assume in tale ambito.]

Un discorso per molti versi simile si può fare per quanto attiene all'Accordo di Schengen, firmato il 14 giugno 1985 e la relativa Convenzione di applicazione, siglata il 19 giugno 1990 (cd. "Sistema Schengen"). Come è noto, grazie a tali strumenti è stato creato uno spazio di libera circolazione delle persone, con la conseguente abolizione dei controlli alle frontiere interne degli Stati membri, sostituiti da un controllo unico al momento dell'ingresso nell'area Schengen. Il venir meno dei controlli alle frontiere dei singoli Paesi aderenti

comportava necessariamente una riduzione del livello generale di "sicurezza" ed è stata pertanto compensata attraverso la creazione di un sistema integrato di scambi di informazioni fra gli Stati membri, denomino SIS. Si tratta in sostanza di un grande archivio comune di tutti i Paesi aderenti, dove sono raccolte informazioni relative sia alle persone che agli oggetti ricercati.

Al fine di mantenere un adeguato bilanciamento fra le esigenze di sicurezza e di tutela della riservatezza, la creazione di tale archivio ha imposto la previsione di idonee misure di protezione della vita privata delle persone, che sono state indicate nell'adozione, in ogni Stato membro, di una legge sulla protezione dei dati personali (per noi, inizialmente la legge n. 675 del 1996 ed ora il Codice in materia di protezione dei dati personali) e nell'isituzione di un'Autorità di controllo.

Da ultimo, si devono ricordare Eurodac, un sistema per il confronto delle impronte digitali dei richiedenti asilo; la Convenzione sull'uso dell'informatica nel settore doganale, per la cooperazione tra le amministrazioni doganali dei Paesi dell'Unione europea, in particolare attraverso lo scambio di dati personali, con la conseguente creazione di un sistema informativo automatizzato comune (Sistema doganale SID) testo a facilitare la prevenzione, la ricerca ed il perseguimento delle infrazioni alle leggi nazionali, nonché, da ultimo, il sistema Eurojust, per la cooperazione in ambito giudiziario.

Con riferimento a tali banche dati internazionali si assiste oggi ad una sempre più accentuata tendenza alla loro riunione o al loro collegamento, al fine di mettere a disposizione dei soggetti incaricati della sicurezza pubblica un più elevato numero di informazioni. Al riguardo, occorre sottolineare che, se è certamente vero che questi incroci di dati possono a volte essere utili per scopi investigativi; tuttavia la sistematica interconnessione dei dati in esse contenute rischia di produrre raccolte di informazioni personali eccedenti rispetto alle finalità volta a volta perseguite, nonché di violare il principio di finalità sopra richiamato.

7. Per garantire la sicurezza delle persone, non si possono calpestare i diritti che le rendono tali

Il clima internazionale e interno innescato dagli attentati dell'11 settembre 2001 e dai tragici eventi successivi fino ai nostri giorni, ha spinto tutti i Paesi occidentali all'adozione di misure particolarmente rigide in materia di sicurezza pubblica.

Purtroppo, dietro la spinta emotiva di tali eventi, si è assisto all'adozione di misure non sempre rispondenti ai principi ed ai criteri sopra richiamati. Misure che, troppo spesso, non prendevano in giusta considerazione le conseguenze a lunga scadenza di tali politiche (si veda al riguardo il Parere 10/2001, approvato il 14 dicembre 2001 dal Gruppo dei garanti europei previsto dall'art. 29 della direttiva n. 95/46/CE).

È probabilmente vero che tale irrigidimento ha rappresentato una risposta in parte inevitabile di fronte alle diverse situazioni di emergenza in cui si sono trovati i governi e gli organi incaricati di garantire la sicurezza dei cittadini. Tuttavia, anche tali condizione estreme non possono mai giustificare una compressione eccessiva dei diritti fondamentali.

Ciò perché, al di là di ogni altra considerazione, tali diritti sono anche lo specchio di quei valori che chi attenta alla sicurezza mira a mettere in discussione ed a distruggere.