Gruppo sullo spazio europeo di libertà, sicurezza e giustizia

Primissima bozza sulla protezione dei dati personali[1]

(Giuseppe Busia)

1. Introduzione - Per un approccio europeo alla tutela dei diritti fondamentali in un contesto di sicurezza e libertà

1.1 La difesa di un patrimonio di diritti comuni come prerequisito per ogni forma di cooperazione

Lo sviluppo di uno spazio europeo di libertà, giustizia e sicurezza e i diversi istituti che ne costituiscono l'architettura, hanno come presupposto fondamentale il crearsi di una fiducia reciproca fra gli Stati membri, chiamati a riconoscersi nelle decisioni assunte da autorità rette da ordinamenti diversi dal proprio, al di fuori dei confini nazionali. E tale fiducia non può che trovare fondamento in un sostrato comune di diritti fondamentali, che si concretano in altrettante garanzie per i cittadini nonché, più in generale, per la difesa di alcuni valori fondanti e costitutivi della stessa collettività.

Ecco, allora, perché qualunque riflessione sullo sviluppo della cooperazione in materia di giustizia e sicurezza deve necessariamente partire dalla creazione di una base comune di diritti della persona, il cui rispetto, oltre a rappresentare un vincolo giuridico per qualunque azione in questo campo, costituisce un ingrediente indispensabile affinché tali attività possano realizzarsi e crescere nel tempo.

Ecco, quindi, il presupposto da cui muovono le considerazioni che seguono, nelle quali si cercherà in particolare di mettere in luce il ruolo ed il significato che in questo quadro assume la tutela dei dati personali. Un ruolo ed un significato assolutamente centrali, in quando tutte le attività di cooperazione a cui si è fatto riferimento si basano essenzialmente sullo scambio di informazioni (specie per quanto attiene alle attività investigative) o comunque implicano il trattamento di delicatissimi dati personali, dalla cui correttezza dipende in ultima istanza la libertà personale o la protezione dell'incolumità degli individui.

[1] Poiché non si è ancora deciso con precisione quale taglio dare al documento né quale ampiezza dedicare alle singole sezioni, mi sono limitato a stendere alcune idee che dovranno necessariamente essere riviste, integrate o modificate quando sarà più definito il contesto in cui devono essere inserite.

Sulla spinta degli attentati del settembre 2001 e dei tragici avvenimenti che ad essi sono seguiti, si è manifestata nei Paesi occidentali una crescente domanda di sicurezza, che ha indotto tutti i governi a compiere sforzi particolarmente ingenti al fine adottare nuove misure di protezione e di difesa sia sul piano interno che su quello internazionale. Tali avvenimenti hanno mostrato in modo evidente la necessità, per gli stati nazionali, di cooperare fra loro per fronteggiare le diverse forme di criminalità, le quali ormai da tempo prescindono dai confini nazionali e fanno della trasnazionalità delle proprie organizzazioni un punto di forza per eludere o comunque superare le deboli difese approntate da ciascun ordinamento statale.

Per alcuni profili, questi fenomeni hanno apprezzabilmente dato un nuovo impulso alla cooperazione giudiziaria e di polizia (elemento, questo, che tuttavia ha avuto minore evidenza nel nostro Paese, anche in ragione di fattori politici interni) aiutando a creare le basi per significativi progressi in tale campo. Purtroppo, però, molto spesso questa spinta si è presentata anche sotto forma di riduzione delle garanzie fondamentali delle persone, portando all'approvazione di norme eccezionali, capaci di derogare anche a principi e diritti che costituiscono il patrimonio ineliminabile della nostra civiltà ormai da secoli. Ciò, senza tenere in giusta considerazione le conseguenze a lunga scadenza di tali politiche[2].

Tale fenomeno ha avuto maggiore evidenza negli Stati Uniti d'America (si pensi solo ai prigionieri di Guantanamo), il paese sicuramente più colpito ed esposto ai rischi di attacchi esterni. Ma ha avuto preoccupanti manifestazioni anche in Europa, in molti casi, proprio sulla spinta di richieste più o meno pressanti di collaborazione da parte degli Stati Uniti o sotto forma di vere e proprie imposizioni esercitate da tale Paese (si pensi al problema della comunicazione dei dati dei passeggeri aerei, su cui si tornerà più avanti).

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.

Anzi, di fronte a tali fenomeni, l'Europa, lungi dal cedere di fronte a scorciatoie emergenziali, anche quando queste sembrino trovare appoggio da parte dell'opinione pubblica, deve rivendicare con orgoglio la superiorità del proprio modello in termini di diritto e di civiltà, richiedendo –se mai- all'alleato americano di recuperare al proprio interno la difesa di alcuni diritti fondamentali che proprio negli Stati Uniti hanno avuto origine o sono fioriti[3]. 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.

---

[2] 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.

[3] Risultato, questo, da non dichiarare a priori impossibile da conseguire, come ha dimostrato il confronto realizzato negli ultimi anni proprio in tema di protezione dei dati personali, in occasione sia delle trattative per la stipula dell'accordo fra Stati Uniti ed Europol sullo scambio di informazioni di polizia (2002), sia della più recente discussione relativa alla trasmissione dei dati dei passeggeri aerei. In entrambi i casi, infatti, pur non essendo stato possibile raggiungere gli standard necessari a garantire una tutela adeguata delle persone, si è tuttavia registrata una crescente apertura dell'Amministrazione statunitense di fronte all'idea di introdurre nel proprio ordinamento talune garanzie dirette ad accrescere il livello di protezione assicurato alle persone rispetto al trattamento dei loro dati personali. Ovviamente, il cammino da compiere è ancora molto: tuttavia la strada da perseguire non è certamente quella del nostro adeguamento alle scelte legislative statunitensi ma, al contrario, quella della progressiva "esportazione" del nostro modello di tutela Oltreoceano.

La tutela orgogliosa di tali diritti e del modello di civiltà del quale sono espressione non rappresenta solamente un atteggiamento auspicabile da parte dei diversi organismi dell'Unione europea coinvolti in tale processo (mentre finora solamente il Parlamento europeo si è distinto per il particolare impegno e la coerenza in questo campo), ma anche un preciso dovere giuridico, specie alla luce del nuovo contesto normativo che si va delineando dopo l'accordo raggiunto sul nuovo Trattato che istituisce la Costituzione europea.

Come è noto, infatti, la Carta dei diritti dell'Unione europea, proclamata solennemente dal Consiglio Europeo di Nizza del dicembre 2000 ed ora significativamente inserita come parte integrante dei nuovi Trattati, dopo aver affermato che "ogni individuo ha diritto al rispetto della propria vita privata e familiare" (art. 7), dedica uno specifico articolo alla protezione dei dati personali (art. 8). Quest'ultima disposizione, oltre a sancire espressamente che ognuno ha diritto alla protezione dei dati di carattere personale che lo riguardano, dispone che tali dati devono essere "trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge". Agli interessati è inoltre riconosciuto un generale "diritto di accedere ai dati raccolti che li riguardano" nonché di "ottenerne la rettifica". Di più: la stessa carta precisa che tali regole devono essere "soggette al controllo di un'autorità indipendente", formalizzando così anche in tale sede l'istituzione dei Garanti per la protezione dei dati, chiamati a svolgere un ruolo particolarmente significativo nella tutela dei diritti che qui interessano.

1.2. Dalla contrapposizione alla necessaria complementarietà fra fini di sicurezza e protezione della privacy

Tutto questo porta a comprendere quanto sia sbagliata la tentazione, purtroppo frequente, di contrapporre sicurezza e tutela dei diritti fondamentali, raffigurati alla stregua di obiettivi fra loro inconciliabili: troppo spesso, infatti, si sente affermare che molti problemi legati alla cooperazione giudiziaria in materia penale e fra le forze di polizia sono riconducibili alle difficoltà derivanti dall'applicazione della normativa sulla protezione dei dati personali, che indubbiamente pone dei limiti alla circolazione delle informazioni, anche quando queste riguardano persone sospettate, imputate o condannate per la commissione di alcuni reati (informazioni, che costituiscono la base di tale cooperazione).

Non vi è dubbio che alcune volte le disposizioni sulla protezione dei dati siano invocate (strumentalmente) dalle diverse parti coinvolte nelle procedure di cooperazione come pretesto per non fornire agli altri talune informazioni che invece dovrebbero essere oggetto di scambio. Tuttavia, si tratta appunto di strumentalizzazioni, tendenti a coprire resistenze di tipo politico o anche solo piccole rivalità di tipo amministrativo (basti pensare alla rivalità che a volte è possibile riscontrare anche nei rapporti fra i corpi di polizia appartenenti allo stesso Paese).

Occorre pertanto ribadire che in un sistema che voglia dirsi democratico, le esigenze di sicurezza non possono che essere perseguite nel quadro del rispetto dei diritti fondamentali della persona, passando dall'idea di una contrapposizione a quella di una doverosa ed imprescindibile complementarietà fra tali elementi.

Ciò, non solo come ovvio presupposto per qualunque discorso in questo campo, ma proprio come strumento per facilitare cooperazione in ambito comunitario. Non è un mistero, ad esempio, che Europol si trovi ad ricevere meno informazioni di quelle che potrebbe e dovrebbe avere, perché gli Stati membri preferiscono servirsi a tal fine degli accordi bilaterali fra loro e con i Paesi terzi. Accordi, questi, la cui esistenza finisce per rappresentare contemporaneamente un indebolimento per le istanze multilaterali (quali Europol, che

dovrebbero costituire la sede privilegiata di cooperazione) ed un rischio maggiore per la tutela dei diritti della persona, essendo gli stessi molto meno controllati e controllabili sotto tale profilo.

1.3. Il necessario bilanciamento fra sicurezza e protezione dei diritti della persona

Ogni qual volta 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 infatti non avere più la speranza di cambiare e di migliorarsi: si pensi ad esempio 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).

L'ordinamento deve naturalmente farsi carico di trovare un adeguato equilibrio fra le esigenze di sicurezza e la necessità di tutelare la persona nella sua libertà nonché –prima ancora- nella sua dignità, bilanciando l'anelito verso l'oblio con la protezione di diversi diritti riconosciuti in capo ad altri soggetti o alla collettività. Tuttavia tutti –a cominciare da chi opera al servizio della sicurezza pubblica- hanno il dovere di tenere sempre presente che anche la semplice conservazione di una singola informazione può pesare sulla vita della persona a cui si riferisce. Per tale ragione la normativa internazionale come pure quella interna prescrivono 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. L'impatto delle nuove tecnologie sulle attività di indagine

2.1 Rischi e opportunità legati allo sviluppo tecnologico

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 infatti contemporaneamente un sintomo ed una conseguenza dello sviluppo anche in senso democratico della nostra società.

Anche in questo caso, tuttavia, è necessario tenere 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. Dati, questi, che anche quando appaiono esteriori e poco invasivi, dicono in realtà molto delle relazioni intrattenute da una persona. Se poi tali informazioni vengono conservate 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.

Lo sviluppo nuove delle tecnologie, inoltre, 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. 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 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.

Questi sviluppi hanno un impatto almeno duplice per quanto attiene alla tutela della sicurezza e dell'ordine pubblico. Da una parte, infatti, espongono i cittadini a nuovi rischi, ne aumentano la vulnerabilità non solo con riferimento alla nascita di nuovi reati, specificamente basati sull'uso di tali tecnologie (si pensi ai cosiddetti *computer crimes*), ma anche con la via via più ampia diffusione di cosiddetti "furti di identità", legati al fatto che sempre più spesso si è rappresentati non già dalla propria 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.

Dall'altra –per quello che qui interessa maggiormente- crea un bacino di dati personali potenzialmente vastissimo, al quale le autorità giudiziarie e le forze di polizia possono attingere informazioni a fini di prevenzione o repressione dei reati e consente loro di creare con maggiore facilità propri archivi elettronici per le medesime finalità.

Proprio in virtù del complessivo accrescimento dei rischi legati ad un uso improprio dei dati nonché delle potenzialità dischiuse dall'utilizzo delle tecnologie a fini di polizia, alcuni legislatori e talune autorità amministrative si sono spinti a consentire alle forze incaricate della tutela della sicurezza pubblica, da un lato, un accesso quasi illimitato ai dati che

vengono lasciati dai cittadini spesso inconsapevolmente. E, dall'altro, sempre grazie all'utilizzo delle nuove tecnologie, la raccolta di un gran numero di ulteriori dati a fini investigativi (si pensi solo alle informazioni raccolte attraverso l'ancora misterioso sistema Echelon).

Se è certamente vero che le complesse investigazioni che oggi si devono affrontare richiedono –probabilmente più che in passato- la raccolta e l'analisi di un gran numero di informazioni. È altrettanto vero che un accesso o una raccolta indiscriminata di questi dati rappresenta un'inaccettabile compressione della libertà personale, che non può trovare giustificazione in generiche emergenze vere o presunte.

Occorre dunque opporsi a facili scorciatoie che, da un lato, dimenticano che non sono accettabili violazioni di diritti fondamentali –come quello alla protezione dei dati personali- neanche per finalità certamente meritevoli, quali la tutela sicurezza pubblica. E, dall'altro, fanno eccessivo affidamento sulle massicce raccolte di dati, e pretendono di individuare un'inesistente relazione diretta fra il numero di informazioni personali raccolte ed i risultati investigativi conseguiti. Ciò, non considerando che invece troppe volte la realtà si è incaricata di mostrare anche tragicamente quanto tale assioma sia privo di fondamento: basti pensare al fatto che l'esistenza di sistemi sofisticati quali il già citato Echelon non sono riusciti a segnalare la preparazione di attentati della portata di quello dell'11 settembre 2001.

2.2. Il falsi miti legati all'idea che la raccolta di più informazioni aiuti necessariamente le attività di indagine

Proprio l'ultima considerazione fatta invita a riflettere sugli aspetti pratici e concreti delle tecniche investigative eccessivamente basate sulla raccolta dei dati personali, anche al di là –dunque- della richiamata inderogabilità dei diritti fondamentali dal punto di vista del diritto positivo. Al riguardo, occorre rilevare che, mentre è certamente vero che l'utilizzo delle reti di comunicazione elettronica rende alcune informazioni personali potenzialmente conoscibili da terzi. È altrettanto vero che chi ha ragioni particolari per voler rimanere anonimo, ad esempio perché sta commettendo o ha intenzione di commettere un reato, può oggi utilizzare sistemi che consentono di mantenere celata la propria identità (es. carte telefoniche prepagate anonime o accessi alla rete in locali aperti al pubblico ma privi di sistemi di identificazione dei clienti) e così rendere poco significative, ai fini delle indagini sulla propria persona, le raccolte di dati –quali quelli sul traffico telefonico o telematico- che molti pretenderebbero di generalizzare e accrescere nella durata proprio in ragione del loro utilizzo a fini di indagine.

Quanto appena detto consente di evidenziare il primo 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: molte volte 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, e miravano invece a sfuggire a tale raccolta: innanzi tutto, appunto, 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.

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.

3. I contenuti specifici della normativa sui dati personali e gli obblighi posti a carico delle forze di polizia

3.1. Dal diritto ad essere lasciati soli all'autodeterminazione informativa

Le moderne legislazioni sulla protezione dei dati prevedono una serie di garanzie volte 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 alla persona a cui i dati si riferiscono, di decidere che uso gli altri possono fare degli stessi, scegliendo sia se un terzo può conoscere una determinata informazione personale, sia 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 nazionali fino alla già richiamata Carta dei diritti fondamentali dell'Unione europea (e che ha trovato spazio nel nostro ordinamento con l'art. 1 del Codice in materia di protezione dei dati personali - decreto legislativo 30 giugno 2003, n. 196, di seguito anche, "Codice privacy").

3.2. I principi fondamentali in materia di tutela dei dati

La normativa comunitaria e quelle nazionali si 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. Innanzi tutto, il principio di finalità, che costituisce la proiezione più diretta della libertà, riconosciuta ad ogni persona, di decidere non solo quali informazioni possono essere utilizzate dai terzi, ma anche quale uso può essere effettuato delle stesse. In base ad esso –come regola generale- i dati raccolti per un determinato fine (ad esempio per scopi commerciali) non possono poi essere utilizzati per scopi diversi (anche per quelli di tutela della sicurezza pubblica) se non in casi eccezionali, specificamente determinati dalla normativa. Ad esso si affiancano i principi di pertinenza (in base al quale, ad esempio, 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 generalmente 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 (per quanto attiene al nostro diritto interno, si possono vedere gli articoli 53 ss. del 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.

3.3. Le regole sulla protezione dei dati per 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 rappresenta anche il presupposto dell'architettura istituzionale di alcuni organismi nati nel contesto 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 legislazione sulla 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.

4. Alcuni spunti di riflessione in vista degli sviluppi futuri

[Ci si limita qui ad un semplice accenno a tali temi, in quanto gli stessi probabilmente costituiranno la conclusione generale del documento e non solo della sezione dedicata ai dati personali]

Come detto, la prevista "costituzionalizzazione" della Carta dei diritti fondamentali attraverso il suo inserimento all'interno dei nuovi Trattati rappresenta certamente un elemento importante per l'affermazione dei principi che prima si sono richiamati anche per tutte attività istituzionali che fino ad oggi ricadevano nel cosiddetto Terzo pilastro.

Tuttavia, la strada da compiere è ancora tanta, come mostrano alcune resistenze all'adozione di standard comuni di protezione dei dati fra i Paesi membri, che si frappongono al realizzarsi di un'effettiva cooperazione fra le autorità giudiziarie e le forze di polizia europee e che evidenziano paradossi per cui alcuni trattamenti (quali l'accesso i dati sui passeggeri dei voli aerei) non sono normalmente consentiti alle autorità di sicurezza dei paesi membri ma si accetta possano esserlo da parte delle corrispondenti agenzie statunitensi, nonostante gli standard di protezione assicurati da queste siano molto inferiori rispetto a quelli europei.

Inoltre, come accennato, le tante emergenze verificatesi in questi anni, unite alle possibilità aperte dallo sviluppo tecnologico, hanno spinto i governi ad intensificare la raccolta di dati e le forme di controllo sui cittadini: si pensi solo all'inserimento dei dati

biometrici nei documenti di identità o all'uso delle tecnologie biometriche in connessione con i sempre più pervasivi impianti di videosorveglianza, al fine di identificare e schedare tutti i soggetti che transitano in determinati luoghi.

Alcune di queste scelte mostrano quanto sia importante che le decisioni che incidono sui diritti fondamentali non siano lasciate ai soli esecutivi degli Stati membri, necessariamente più sensibili alle pressioni dell'opinione pubblica o dei governi alleati. Per tale ragione, è importante che la pur auspicabile "comunitarizzazione" delle funzioni disciplinate nel Terzo pilastro non si risolva nel semplice affidamento delle stesse agli esecutivi, ma richieda necessariamente, oltre che uno stringente controllo della Corte di giustizia sul rispetto dei principi e dei diritti codificati nella Carta dei diritti fondamentali, anche forme di partecipazione qualificata da parte del Parlamento europeo. Quest'ultimo organismo, infatti, come ha dimostrato in occasione dei dibattiti che si sono sviluppati negli ultimi anni, rappresenta un presidio fondamentale per la tutela dei diritti, anche in virtù del suo carattere più direttamente rappresentativo e della maggiore trasparenza delle procedure interne. Un suo più ampio coinvolgimento appare inoltre particolarmente urgenze in ragione del fatto che il pur opportuno venir meno del sistema delle convenzioni comporta l'emarginazione dei parlamenti nazionali, i quali invece, attraverso le procedure di ratifica potevano svolgere un controllo democratico nei termini ora indicati

Eventuali approfondimenti[4]

[4] **OVE LO SI RITENESSE OPPORTUNO (MA PROBABILMENTE ESULA DAL TIPO DI DOCUMENTO CHE SI INTENDE REDIGERE), ALLE CONSIDERAZIONI GENERALI CONTENUTE NEL TESTO, POTREBBERO ESSERE AGGIUNTE ALCUNE NOTE DIRETTE AD ILLUSTRARE LA 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.

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 .

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 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.

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.

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 e, da ultimo, un nuovo e più ampio provvedimento generale, 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).

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).