LO SPAZIO EUROPEO DI LIBERTA' SICUREZZA E GIUSTIZIA E LA PROTEZIONE DEI DATI PERSONALI

di Giuseppe Busia

(capitolo V del quaderno di Astrid, di prossima pubblicazione, "***L'Europa dei diritti. Lo spazio europeo di libertà sicurezza e giustizia,*** a cura di Giuliano Amato e Elena Paciotti, ed. Il Mulino)

1. La centralità della protezione dei dati personali per l'attuazione del programma dell'Aia

Il cosiddetto Programma dell'Aia[1], come già osservato nei capitoli precedenti[2], ha evidenziato opportunamente la necessità che lo sviluppo di uno spazio di libertà, sicurezza e giustizia si realizzi – alla luce del Trattato costituzionale- in un quadro di tutela dei diritti fondamentali della persona, badando che questi non siano solamente rispettati, ma anche attivamente promossi. Occorrerà dunque un'opera di promozione attiva, diretta a far sì che la loro tutela divenga elemento fondante di ogni sviluppo delle politiche in questo settore, alla stregua di un ingrediente indispensabile affinché le stesse possano realizzarsi e crescere nel tempo[3].

Certo, queste importanti considerazioni sono state fatte dal Consiglio europeo soprattutto guardando al futuro, al momento in cui il nuovo trattato sarà stato ratificato da tutti i paesi membri e quindi entrato in vigore. E sarebbe stato sicuramente preferibile se i capi di stato e di governo avessero avuto più coraggio, ed avessero anticipato in misura maggiore i contenuti trattato, specie per quanto attiene alla tutela dei diritti fondamentali nel campo della cooperazione giudiziaria e di polizia in campo penale. Tuttavia, limitarsi ad evidenziare i limiti di tali scelte serve a poco, ed può anzi rivelarsi controproducente. Meglio, invece, cercare di dare un'interpretazione in qualche modo "estensiva" e "progressiva" degli impegni dell'Aia, sforzandosi di realizzare quanto ancora manca rispetto al

---

[1] Allegato I alle Conclusioni della Presidenza del Consiglio europeo di Bruxelles del 4/5 novembre 2004 8(14292/04 – CONCL 3)

[2] vedi in particolare il capitolo II

[3] Occorre comprendere quanto sia sbagliata, anche con riguardo alla privacy, la tentazione, purtroppo frequente, di contrapporre sicurezza e tutela dei diritti fondamentali, raffigurati alla stregua di obiettivi fra loro inconciliabili

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).

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.

risultato sperato. Ciò, oltre che attraverso le prassi ed i comportamenti degli altri soggetti coinvolti, in particolare mediante l'opera della Commissione, chiamata a concretizzare gli obiettivi e le priorità del programma dell'Aia in un piano di azione da presentare entro il 2005 nonché del parlamento europeo. Quest'ultimo, coinvolto meno di quanto si sarebbe potuto nel processo di definizione del nuovo quadro giuridico, dovrà conquistarsi lo spazio a cui ha diritto con gli strumenti che oggi ha a sua disposizione, incalzando la Commissione attraverso atti di indirizzo e di controllo e, così, coinvolgendo l'opinione pubblica in un dibattito dal quale non può e non deve restare esclusa.

In tale percorso, la tutela dei dati personali assumerà un ruolo ed un significato assolutamente centrali, in quando gran parte delle attività di cooperazione 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.
Come è noto, la Carta dei diritti fondamentali dell'Unione europea, dopo aver affermato che "ogni individuo ha diritto al rispetto della propria vita privata e familiare" (art. 7 della Carta, ora II-77 del Trattato costituzionale), dedica uno specifico articolo alla protezione dei dati personali (art. 8 della Carta, II-68 del Trattato). 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.

Il Programma dell'Aia evidenzia opportunamente anche il fatto che il Trattato costituzionale (art. I-7) prevede che "l'Unione aderisce alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali", la quale, per prima in ambito europeo, ha riconosciuto in modo completo ed esplicito un diritto alla vita privata (art. 8). La previsione di tale adesione – al di là degli interrogativi suscitati dal valore di una simile affermazione di carattere unilaterale- costituisce un ulteriore indice della volontà dell'Unione di garantire al suo interno il pieno rispetto dei diritti fondamentali e apre la via alla possibilità che la Corte europea dei diritti dell'uomo possa esercitare un ruolo importante per la tutela dei diritti medesimi.

Il fatto che la Carta dei diritti sia stata inserita come parte integrante del Trattato costituzionale, e che quest'ultimo dedichi un'ulteriore disposizione alla protezione dei dati personali (art. I-50) sta a significare che il pieno rispetto di tale diritto deve essere considerato già oggi un vincolo (sebbene non necessariamente presidiato da una completa tutela giurisdizionale) per l'azione dell'Unione anche per quanto attiene alle politiche ed agli organi operanti all'interno del terzo pilastro. Ciò,specie in considerazione del fatto che questi ultimi sono destinati ad essere pienamente comunitarizzati (cfr. art. I-41).

Per tale ragione – pur tenendo presenti i limiti sopra evidenziati - appare condivisibile la scelta, operata dal Consiglio europeo di Bruxelles del 4-5 novembre 2004, di incoraggiare ogni azione perché, pur nel quadro del diritto vigente, sia avviato da subito il processo di implementazione delle diverse misure previste dal nuovo trattato, con particolare riferimento ai diritti fondamentali. Tale scelta può

rappresentare una spinta particolarmente opportuna per il difficile percorso di ratifica che attende la nuova "Costituzione" europea: solo se inquadrato in un contesto di adeguata tutela dei diritti fondamentali, infatti, lo spazio di giustizia e sicurezza che l'Unione si è impegnata a garantire ai propri cittadini sarà avvertito da questi anche come un vero spazio di libertà, capace di garantire un reale progresso in termini di civiltà e di salvaguardare nel contempo la specificità del modello di sviluppo democratico che caratterizza il Vecchio Continente.

La decisione di iniziare immediatamente a preparare l'applicazione di queste norme costituisce altresì una condizione necessaria per assicurarne l'immediata operatività non appena il Trattato stesso sarà stato ratificato. Ed infatti, a differenza di quanto accade con altre disposizioni, perché quelle riguardanti i diritti fondamentali ed in particolare la tutela dei dati divengano realmente diritto vivente, non è sufficiente il loro inserimento in un atto normativo giuridicamente vincolante, ma è necessaria la loro progressiva assimilazione nella prassi e nella cultura di coloro che sono chiamati ad applicarle.

2. Creare un circolo istituzionale virtuoso fra Commissione, parlamenti europeo e nazionali, ed autorità garanti

Come accennato, in questo quadro un ruolo specifico dovrà necessariamente essere svolto dal parlamento europeo, che negli ultimi anni ha manifestato una particolare sensibilità nella tutela e nella promozione dei diritti in discorso[4]. Per il futuro, sarebbe auspicabile che tutte le decisioni di principio relative alla tutela dei dati vedano il parlamento europeo realmente partecipe. Occorrerebbe infatti evitare che le scelte attinenti alla tutela dei diritti e delle libertà fondamentali possano essere assunte al di fuori di un ampio dibattito democratico e con procedure che non garantiscano la più ampia trasparenza. In particolare, non è più accettabile, anche sulla base dell'ordinamento vigente, che decisioni dirette ad incidere sui tali diritti possano essere assunte esclusivamente dal Consiglio, con il rischio di pericolosi cedimenti ad una logica emergenziale, foriera di un abbassamento del grado di tutela dei diritti delle persone[5].

In questa fase, l'Assemblea rappresentativa dei cittadini d'Europa in molti casi dovrà limitarsi ad un'opera di controllo e di stimolo. Tuttavia, anche tale attività, se portata avanti in modo sufficientemente costante, può rivelarsi particolarmente preziosa. Per tale ragione, è auspicabile che il parlamento si attivi da subito per tale obiettivo, sia attraverso l'approvazione degli opportuni atti di indirizzo sia chiedendo alla Commissione di riferire costantemente sui lavori di elaborazione del piano.

Per le stesse ragioni, attinenti principalmente alla democraticità delle decisioni da assumere, è parimenti auspicabile che anche i parlamenti nazionali siano coinvolti in tale processo fin dall'inizio, a

[4] Un esempio emblematico si è avuto con riguardo all'accesso diretto alle banche dati delle compagnie aeree europee concesso alle agenzie di sicurezza degli Stati Uniti prima di fatto, poi attraverso accordi più o meno formalizzati a livello amministrativo e, infine, attraverso un accordo fra il Consiglio UE e l'amministrazione USA, che ha visto la ferma opposizione del Parlamento europeo. Con diverse risoluzioni, che hanno accompagnato il lungo negoziato, il Parlamento europeo ha infatti denunciato la violazione delle norme europee che assicurano la protezione dei dati personali – e in particolare dell'articolo 8 della Carta dei diritti fondamentali – e, infine, ha proposto ricorso alla Corte di giustizia contro l'accordo definitivamente concluso contro il suo parere.

[5] Le funzioni disciplinate nel Terzo pilastro dovrebbero prevedere 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 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.

partire dalla cosiddetta “fase ascendente” del processo di elaborazione della nuova normativa. Ciò, al fine di evitare che il loro intervento sia limitato –come troppo spesso accade- al recepimento in sede nazionale di disposizioni già definite a livello comunitario (fase discendente). Sarebbe pertanto particolarmente opportuno che i parlamenti nazionali si attivino in tal senso, principalmente attraverso atti di indirizzo volti ad indicare ai governi le posizioni da assumere in sede di Consiglio al fine di salvaguardare la tutela dei diritti fondamentali. Solo attraverso tale coinvolgimento, sarà infatti possibile garantire un adeguato coinvolgimento delle opinioni pubbliche e così la trasparenza dell’intero processo.

Inoltre, con riferimento alle decisioni assunte nel quadro della normativa appena delineata, che abbiano un impatto sulla protezione dei dati delle persone sarebbe auspicabile fosse assunto l’impegno di richiedere –anche nei casi in cui questo non è previsto normativamente- il parere volta a volta obbligatorio o vincolante delle autorità garanti per la protezione dei dati competenti per il livello istituzionale su cui le decisioni medesime sono destinate ad avere effetto.

3. Verso la predisposizione di un quadro normativo comune

Sarebbe auspicabile che la Commissione, nella predisposizione del programma a cui si è fatto cenno, prevedesse l’approvazione di una normativa specifica sul trattamento dei dati personali per fini di giustizia e sicurezza pubblica, facendo tesoro, oltre che della normativa elaborata in sede di Consiglio d’Europa, anche degli sviluppi già realizzati nell’ambito del primo pilastro nonché dei principi che costituiscono l’ossatura delle Convenzioni Schengen, Europol, sull’uso dell’informatica nel sistema doganale ed Eurojust, sulle quali si tornerà fra breve. Anche con riguardo a tale normativa, appare infatti cruciale dare immediatamente avvio ai lavori di elaborazione, anticipando quanto previsto dal Trattato costituzionale con riferimento alla piena comunitarizzazione delle politiche qui in esame. Ciò, ancora una volta, col duplice fine di offrire un utile sostegno al cammino di ratifica ed insieme preparare l’immediata operatività delle disposizioni del Trattato non appena queste entrino in vigore.

Come presupposto di tale lavoro, la stessa Commissione dovrebbe dare avvio ad una completa ricognizione delle garanzie sulla protezione dei dati adottate dalle diverse convenzioni di terzo pilastro, nonché dei risultati concretamente ottenuti nella loro applicazione pratica. Sulla base di tale lavoro, sarà possibile individuare regole comuni, possibilmente mirando ad elevare gli standard di protezione. Ciò, anche come misura in qualche modo “compensativa” rispetto agli accresciuti rischi derivanti dal tendenziale aumento del numero e delle categorie di dati conservati all’interno dei sistemi informativi in discorso nonché della crescente possibilità di interscambio di informazioni fra le diverse basi di dati (si tornerà nelle pagine seguenti sui rischi legati a tali sviluppi, e sulla conseguente necessità di adottare opportune cautele al riguardo).

In generale, occorrerà che la normativa predisposta sia sufficientemente dettagliata per quanto attiene alla tutela dei diritti delle persone, non lasciando che il quadro normativo approntato al riguardo possa essere modificato da micro-decisioni prese al di fuori di un adeguato controllo delle istituzioni rappresentative e delle autorità di controllo di settore. La stessa normativa, proprio in nome del pieno rispetto dei diritti fondamentali sopra richiamati, dovrà inoltre evitare che si creino “zone franche” di irresponsabilità per le possibili violazioni dei diritti medesimi, anche sotto forma di privilegi ed immunità garantiti ai soggetti incaricati dello svolgimento delle attività di polizia o giurisdizionali.

4. Alcuni principi generali a cui dovranno uniformarsi le nuove regole sulla protezione dei dati

È indispensabile che le scelte che saranno assunte nel quadro aperto dal programma dell'Aia e in quello del nuovo trattato siano coerenti con alcuni principi cardine in materia di protezione dei dati[6]. 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, è necessario che applichino i principi prima richiamati con particolare rigore.
È dunque necessario che la normativa sulla protezione dei dati utilizzati per fini di sicurezza pubblica non si limiti a ricordare i principi generali sopra richiamati ma detti altresì alcune regole specifiche riguardanti in particolare meccanismi di verifica interna periodica sui trattamenti realizzati, necessari al fine di valutare l'effettiva persistenza delle ragioni che ne avevano giustificato l'inizio nonché la pertinenza e la necessità delle diverse informazioni detenute. Tutto ciò, non solamente al fine di tutelare i diritti degli interessati, ma anche di rendere più efficienti le operazioni di analisi, che vengono invece rallentate dall'eccessivo appesantimento degli archivi con informazioni eccedenti o non aggiornate.
Con riguardo a quest'ultimo profilo è altresì necessario prevedere forme adeguate per l'esercizio dei diritti da parte dell'interessato, con particolare riferimento alla possibilità di accesso, verifica e rettifica dei dati, eventualmente attraverso la mediazione dell'autorità garante, secondo moduli già sperimentati a livello europeo.

I rischi connessi alla conservazione dei dati: l'esempio del casellario giudiziario europeo

[6] 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'autodeterminazione 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.

Poiché anche la semplice conservazione di una singola informazione può pesare sulla vita della persona a cui si riferisce[7], nella predisposizione delle diverse misure previste dal programma dell'Aia tale trattamento dovrà essere consentito solo se sia effettivamente necessario per il perseguimento di fini ugualmente meritevoli e non sia possibile perseguire i fini medesimi senza l'utilizzo di dati personali o mediante trattamenti meno invasivi.
A titolo di esempio, può essere richiamato il progetto di dare vita ad un casellario giudiziario europeo (sul quale si veda anche quanto detto nei capitoli precedenti). Esso può certamente rappresentare un utilissimo strumento per la prevenzione e la repressione del crimine, ed è pertanto opportuno proseguire nella discussione sulla sua istituzione. Tuttavia, è necessario che il raggiungimento di tale obiettivo, da realizzare attraverso l'interconnessione dei casellari giudiziari nazionali, avvenga nel pieno rispetto della normativa sui dati e, magari, sia anche l'occasione per ripensare la disciplina di questi strumenti anche sul piano nazionale, alla luce degli sviluppi della protezione dei dati.

Al riguardo non è irragionevole immaginare che, proprio di fronte alle prospettive di interconnessione dei dati detenuti dai paesi membri e, quindi, di un notevole ampliamento dei trattamenti realizzati, si introducano opportune differenziazioni nella circolazione di tali informazioni, ad esempio, a seconda del tipo o della gravità del reato per il quale si è ricevuta una condanna o in funzione del tempo trascorso dalla stessa. Come pure non sarebbe sbagliato immaginare differenti gradi di accessibilità a seconda delle funzioni volta a volta attribuite ai singoli operatori delle forze dell'ordine. Ad esempio, mentre nel caso dell'effettuazione di un fermo o di particolari indagini può essere opportuno rendere immediatamente accessibili dal comando della polizia anche i dati più risalenti e riguardanti i reati meno gravi su un determinato individuo, in modo da rendere più rapide le verifiche necessarie. Potrebbe invece apparire sproporzionato che una persona, magari in vacanza all'estero con la famiglia, si trovi a dover rendere conto di un reato bagatellare commesso in patria tanti anni prima alla pattuglia che intende elevargli una contravvenzione per divieto di sosta, solo perché questa ha un accesso immediato e indiscriminato a tutte le informazioni del casellario attraverso il computer di cui venga dotata la propria autovettura. Ciò, a prescindere dai fastidi, dalle lungaggini e dagli errori (oltre che dai maggiori costi) che possono derivare alle indagini proprio dal fatto di costringere le forze dell'ordine ad analizzare un numero eccessivo di informazioni, naturalmente in larga parte inutili.

Se veramente si vuole che la pena serva alla rieducazione del condannato ed al suo pieno reinserimento nella comunità, è necessario che questi, soprattutto se ha commesso reati di lieve gravità, dopo aver pagato il proprio debito con la società, possa muoversi al suo interno senza il pesante fardello degli errori passati. Anche una circolazione eccessiva e sproporzionata delle informazioni contenute nei casellari giudiziari può oggi pesare quanto una catena alla caviglia o essere fastidiosa quanto una moderna gogna, spingendo chi vorrebbe reinserirsi nella società ad allontanarsene nuovamente, visto che questa continua a considerarlo "diverso".

---

[7] 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.

5. Possibili misure per rafforzare l'azione delle Autorità di controllo sulla protezione dei dati operanti nell'ambito del Terzo pilastro

Uno degli elementi che accomunano i diversi sistemi previsti nell'ambito del Terzo pilastro[8] è quello della presenza, a fianco ai garanti nazionali, di un'Autorità di controllo comune, nella quale siedono i rappresentanti di tutti gli Stati aderenti. Tali organismi hanno finora svolto un ruolo importante per assicurare il rispetto delle disposizioni poste a protezione dei dati personali nonché nel proporre soluzioni innovative tese ad accrescere il livello complessivo di tutela.
Tuttavia, per migliorare la funzionalità e rendere più efficace l'azione di queste Autorità, soprattutto in vista dei probabili sviluppi che interesseranno l'assetto complessivo dei sistemi informativi attualmente inseriti nel terzo pilastro, appaiono opportune una serie di iniziative che in parte sono state avviate e che necessitano in ogni caso di un rinnovato impulso.

---

[8] Fra questi, merita innanzi tutto attenzione la Convenzione Europol, che rappresenta uno dei più organici tentativi di dare alla cooperazione internazionale delle forze di polizia una coerente strutturazione all'interno dell'architettura europea. 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.

Proprio al fine di assicurare una completata protezione dei dati personali, la Convenzione Europol ha previsto una tutela articolata su due livelli: nazionale e sopranazionale, attraverso apposite autorità di controllo.

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 o comunicare i dati a tali soggetti. Procedura, questa, che vede significativamente coinvolta anche l'Autorità di controllo comune.

La convenzione Europol – ma un discorso per molti versi analogo può essere fatto per le altre convenzioni del terzo pilastro sulle quali ci si soffermerà fra breve - contiene disposizioni di principio necessariamente generiche che hanno richiesto l'adozione di una copiosa normativa di attuazione nella quale sono di fatto contenute disposizioni che incidono profondamente sui diritti della persona oltre che sull'assetto complessivo del sistema. Tali disposizioni sono state e continuano ad essere adottate nella maggioranza dei casi con decisioni del Consiglio, al di fuori di un serio controllo democratico. Con riferimento a tutte queste disposizioni, occorre invece che per il futuro sia garantita la piena partecipazione del Parlamento europeo all'adozione delle disposizioni di principio nonché il parare di questo per le decisioni più rilevanti.

Un discorso per molti versi simile a quello fatto con riguardo a Europol 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, denominato 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 (attualmente nel SIS sono contenute informazioni relative a circa un milione di persone).

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'istituzione 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.

1) Uno degli elementi di possibile debolezza del sistema, specie in vista dei suoi probabili sviluppi, è quello della frammentarietà dei controlli, derivante dalla pluralità di autorità presenti nell'ambito del terzo pilastro, a sua volta conseguenza della parcellizzazione della normativa contenuta nelle diverse convenzioni. È ragionevole immaginare che in un prossimo futuro si arriverà all'unificazione di tali autorità (tale sbocco è strettamente legato al crescente interscambio di dati o collegamento fra i diversi sistemi informativi che lo stesso programma dell'Aia sembra prefigurare, forse non tenendo nel dovuto conto i problemi che questo comporta per quanto attiene alla protezione dei dati). Tuttavia, anche prima di tali ormai auspicabili mutamenti dell'assetto complessivo del sistema, è possibile realizzare alcune misure anche di carattere pratico che, pur nella loro gradualità, vanno nella medesima direzione:

a) Occorre intensificare la pratica delle riunioni congiunte fra le diverse autorità di controllo del terzo pilastro al fine di discutere delle problematiche comuni e di coordinare la propria azione[9]
b) Appare opportuno incoraggiare la scelta, già effettuata da molti Stati, di designare le medesime persone come rappresentanti all'interno di più autorità, così da realizzare una prima, parziale unificazione delle autorità medesime, almeno sotto il profilo personale. Ciò, grazie al fatto che esse hanno una composizione molto simile fra loro, sia per quanto attiene al numero dei rappresentanti, sia –soprattutto- per la loro provenienza (nella quasi totalità dei casi riconducibile alle autorità di controllo nazionali).

Con riguardo alla possibilità di ripensare la struttura ed il funzionamento delle Autorità in vista di una loro ipotizzata unificazione, appare utile assumere come modello -anche per quelle previste dalle altre convenzioni- l'autorità istituita dall'art. 24 della Convenzione Europol. Ciò, sia con riferimento alle più avanzate disposizioni in materia di indipendenza di tale organo (incompatibilità, procedure di designazione e garanzie sulla durata del madnato), sia –in particolare- con riferimento all'avvenuta istituzione al suo interno di un Comitato di appello, composto da un rappresentante per ogni stato membro, incaricato di esaminare e decidere in via definitiva sui ricorsi presentati dai cittadini in ordine al mancato rispetto dei loro diritti da parte di Europol. L'attribuzione di un potere decisorio sui ricorsi presentati dai cittadini, analogamente a quanto avviene in ambito nazionale, costituisce infatti un fondamentale completamento delle attribuzioni di questi organismi di garanzia, indispensabile per consentire loro di svolgere pienamente la propria funzione istituzionale.

2) Un altro degli obiettivi da raggiungere consiste nel rendere più continuativa l'attività delle autorità comuni di controllo, superando quel tanto di discontinuità che ancora oggi ne caratterizza l'azione (ciò, soprattutto a causa del fatto che i loro componenti non svolgono questa attività a tempo pieno, essendo impegnati principalmente dai loro incarichi nazionali di garanti o di dirigenti delle autorità nazionali). A tal fine, prima di pensare ad incarichi aventi i caratteri dell'esclusività e dell'impegno a tempo pieno, è possibile muoversi nella direzione sotto indicata.

a) Appare necessario rafforzare il Segretariato comune delle ACC Europol, Schengen e per il controllo sul SID, la cui istituzione ha contribuito in misura notevole a migliorare e rendere più rapida l'azione di questi organismi;
b) Sembra altresì particolarmente opportuno incentivare la possibilità di costituire, all'interno di dette autorità, comitati o gruppi di lavoro in grado di svolgere, in nome e per conto dell'Autorità medesima, funzioni dalla stessa delegate. Ciò, in considerazione della maggiore facilità con cui tali comitati possono riunirsi ed operare, e ferma restando la necessità che l'autorità nel suo

[9] Il primo incontro di questo tipo ha avuto luogo il 28 settembre 2004 ed altri sono seguiti successivamente.

plenum sia volta a volta chiamata non solo a definire puntualmente le azioni delegate, ma anche a verificarne lo svolgimento nonché a ratificare le stesse, una volta che siano completate.

c) Occorre garantire a *tutte* le autorità un'adeguata autonomia finanziaria: attualmente, infatti, solo quella prevista dalla Convenzione Europol gode di un capitolo di bilancio autonomo, nonostante l'esistenza di un simile elemento giochi un ruolo fondamentale sia per garantire l'effettiva autonomia di questi enti, sia per consentire loro di intensificare la propria attività ove le esigenze di tutela lo richiedano

3) Al fine di rafforzare l'indipendenza di questi enti, è necessario prevedere requisiti personali più rigidi per la nomina dei rappresentanti degli Stati, stabilendo specifiche incompatibilità con gli incarichi di tipo governativo e richiedendo una maggiore formalizzazione delle designazioni nonché e fissando regole sufficientemente garantiste per assicurare una tendenziale inamovibilità dei soggetti designati, salvi casi di gravi violazioni o gravi mancanze nello svolgimento dei propri compiti.

4) Sembra opportuno creare un più stretto raccordo istituzionale fra le autorità di controllo ed il Parlamento europeo, prevedendo che le relazioni predisposte periodicamente dalle autorità siano non solamente trasmesse a tale organismo, ma anche discusse nelle loro linee essenziali in occasione di audizioni dei componenti delle autorità medesime. Ciò, anche al fine di consentire al Parlamento di ricevere elementi utili per la propria azione normativa e di controllo nei confronti del Consiglio. Tali relazioni, come è prassi in alcuni Stati, dovrebbero essere inoltre allegate a quelle dell'Autorità nazionale di controllo (i garanti nazionali) assicurando così alle stesse adeguata pubblicità e attenzione, specie da parte dei parlamenti dei singoli Stati membri. In ogni caso, sarà opportuno prevedere sistemi atti a garantire una maggiore pubblicità sia delle relazioni al Parlamento che delle decisioni assunte dalle Autorità (ad esempio istituendo una raccolta ufficiale delle stesse, analogamente a quanto accade per i Bollettini dei Garanti nazionali). Fra le deliberazioni delle Autorità comuni di controllo di sicuro interesse parlamentare, occorre ricordare i pareri che l'autorità di controllo Europol è chiamata ad esprimere sull'avvio dei negoziati e sul testo finale degli accordi per il trasferimento di dati verso gli stati e gli organismi terzi: sarebbe particolarmente utile se tali pareri -in considerazione dell'indubbio rilievo per l'architettura complessiva del sistema- venissero sempre trasmessi al Parlamento, che potrebbe così utilizzarli per intervenire su decisioni altrimenti riservate al solo Consiglio.

5) Da ultimo, occorre valorizzare ed intensificare le relazioni con la Commissione europea, anche al di là del compito specifico ad essa assegnato, di predisposizione del piano d'azione previsto dal programma dell'Aia. Al riguardo, merita sicuramente di essere continuato il cammino cominciato in occasione della riunione congiunta delle Autorità di controllo di terzo pilastro che ha avuto luogo il 21 dicembre 2004 e che ha visto la partecipazione anche del commissario europeo Franco Frattini. In tale occasione, infatti, il neo-commissario ha manifestato l'intendimento di valorizzare il ruolo delle autorità di controllo comune, come interlocutore privilegiato della Commissione per quanto attiene all'elaborazione delle politiche aventi ricadute sulla protezione dei dati. Tutto questo, al fine di creare un circuito istituzionale virtuoso, a presidio dei livelli di tutela dei diritti fondamentali.

6. Le problematiche legate all'interconnessione fra i diversi sistemi informativi

Con riferimento ai diversi sistemi informativi previsti nell'ambito del terzo pilastro, 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. Tale tendenza sembra aver trovato piena conferma nel percorso di rafforzamento della sicurezza

tracciato dal Programma dell'Aia, in base al quale, a partire dal 1 gennaio 2008, lo scambio di informazioni dovrebbe uniformarsi al "principio di disponibilità". Sulla base di esso, in tutta l'Unione, quando un ufficiale di un servizio di contrasto di uno stato membro avrà bisogno di informazioni nell'esercizio delle sue funzioni, potrà ottenere le stesse da un altro stato membro, essendo i corrispondenti servizi di quest'ultimo tenuti a trasmettergliele per i fini dichiarati.

Questo lascia presagire un notevole incremento degli scambi di dati all'interno dell'Unione e richiede adeguate garanzie per quanto attiene alla tutela dei dati personali. 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.

Opportunamente il programma dell'Aia ha voluto enunciare alcune condizioni fondamentali che la Commissione dovrà osservare nella predisposizione delle proposte relative all'attuazione del principio di disponibilità. Si tratta naturalmente solo di principi generalissimi, in qualche caso posti secondo un ordine del quale è difficile cogliere la logica. E tuttavia appare opportuno enfatizzare e valorizzare tali condizioni, al fine di far sì che gli annunciati sviluppi non finiscano per comportare un pericoloso abbassamento di tutela dei diritti fondamentali.

Al riguardo, occorre innanzi tutto ricordare che lo scambio potrà avvenire solo ai fini dell'esecuzione di compiti stabiliti dalla legge. Occorrerà dunque che le decisioni riguardanti i possibili scambi siano assunte attraverso procedure adeguatamente trasparenti e meditate, evitando di agire sull'impulso di situazioni emergenziali, senza un'opportuna riflessione sulle possibili conseguenze di ogni scelta e lontano dal controllo dell'opinione pubblica.

Inoltre, le procedure dovranno garantire che sia mantenuta l'integrità dei dati oggetto di scambio, evitando così che gli stessi possano subire manipolazioni o trasformazioni, tali da esporre l'interessato al rischio di dannose conseguenze anche sul piano della libertà personale o dell'incolumità fisica, prima ancora che su quello della protezione dei dati.

A tale vincolo si lega anche la previsione secondo cui le persone devono avere il diritto di chiedere la correzione dei dati errati, aiutando così a salvaguardare un elevato livello di qualità degli stessi, sempre indispensabile per qualunque trattamento, ma che acquista un rilievo del tutto particolare con riferimento ai settori che qui maggiormente interessano (il programma dell'Aia si pone tale obiettivo anche al fine di assicurare la migliore funzionalità di Europol).

Ed ancora, oltre a doversi garantire la "riservatezza" dei dati in ogni fase dello scambio e successivamente, sarà necessario disciplinare l'accesso alle informazioni attraverso nome e standard tecnici comuni Sarà quindi necessario prevedere una rigorosa regolamentazione, evitando ad esempio che i dati trasmessi ad una determinata unità di polizia, vengano automaticamente posti nella disponibilità di tutta la polizia dello stesso paese. Ogni stato dovrà regolare nel dettaglio le modalità di accesso ai dati da parte degli incaricati della sicurezza pubblica, in modo di far sì che lo stesso abbia luogo solo nel caso sussistano specifiche esigenze con riferimento ad indagini o ad altre attività in corso.

Occorrerà, inoltre, prevedere che ogni richiesta di dati sia corredata da una precisa indicazione delle ragioni per le quali gli stessi sono richiesti, così da consentire al soggetto che li possiede, di selezionare e trasmettere solo quelli effettivamente rilevanti. In tal modo, inoltre, sarà più facile controllare che il soggetto che li riceve, li usi solo per tale finalità, evitando ogni ulteriore trattamento. Inoltre, le disposizioni che regoleranno la materia, dovranno farsi carico di definire i tempi di conservazione, prevedendo altresì la cancellazione dei dati nel caso in cui gli stessi non siano necessari ai fini delle indagini in corso.

Tali considerazioni sono particolarmente attuali per quanto attiene al dibattito che si è sviluppato intorno alla modifica del sistema Schengen, destinata a riflettersi anche sugli altri organismi appena descritti. Il riferimento è alla creazione del Sistema di informazione Schengen SIS II, sia al fine di consentire l'accesso alle informazioni da parte di altri soggetti, sia per fare fronte all'allargamento dell'UE, grazie anche all'adozione di una nuova architettura tecnologica.
Finora, però, il cammino verso l'introduzione di tali trasformazioni non è stato accompagnato da una definizione sufficientemente chiara degli obiettivi perseguiti nonché del regime a cui dovrebbero essere sottoposte le singole informazioni contenute nel nuovo Sistema. Ciò, nonostante le sollecitazioni in tal senso rivolte dal Parlamento europeo al Consiglio[10].
Purtroppo, il programma dell'Aia non sembra fare passi significativi nel senso di una maggiore ponderazione su tali profili mentre apre la via ad una crescente interoperabilità fra i sistemi di informazione dell'Unione da effettuare sulla scorta di una comunicazione della Commissione sull'interoperabilità tra il SIS II, il Sistema di informazione visti (VIS)[11] ed EURODAC da realizzare nel 2005. Opportunamente lo stesso programma sottolinea però la necessità di conseguire il giusto equilibrio tra tali obiettivi e la tutela dei diritti fondamentali dell'individuo. Pertanto, anche sulla scorta di tale doverosa apertura, diventa indispensabile procedere con rapidità alla fissazione di specifiche garanzie, seguendo altresì quanto già segnalato dalle autorità di controllo competenti.
Innanzi tutto, l'accesso a banche dati istituite sulla base di un diverso quadro giuridico e per finalità differenti dovrà pertanto essere consentito soltanto se necessario e proporzionato, e non semplicemente perché le nuove architetture informatiche lo rendono tecnicamente possibile. Dovranno quindi essere chiarite preventivamente le specifiche finalità perseguite nonché i rapporti che intercorrono fra i singoli soggetti autorizzati all'accesso o allo scambio di informazioni, definendo con precisione i limiti all'utilizzabilità dei diversi dati.
Appare inoltre indispensabile che i soggetti abilitati ad accedere a sistemi diversi da quello proprio siano almeno tenuti a rispettare gli stessi standard di protezione dei dati previsti nel sistema a cui hanno accesso.
Con riferimento alla possibilità che nelle banche dati siano aggiunte nuove categorie di dati (per quanto attiene al SIS II si è previsto l'inserimento di identificatori biometrici, quali impronte digitali o scansioni dell'iride) occorrerà infine evitare il rischio del crearsi di pericolose duplicazioni fra i sistemi informativi previsti nell'ambito del terzo pilastro, con il conseguente aumento dei rischi per la protezione dei dati.
Il programma dell'Aia fa esplicito riferimento, oltre all'accesso reciproco o all'interoperabilità di basi di dati nazionali, anche all'accesso diretto (on-line), anche per l'Europol, alle basi di dati centrali dell'Ue già esistenti, quali appunto il SIS. A questo riguardo, occorre sottolineare che la connessione diretta fra sistemi, rispetto al semplice diritto di consultare alcune informazioni, accresce in modo particolarmente rilevante il pericolo che i dati vengano utilizzati per finalità differenti rispetto a quelle per le quali era stata immaginata la raccolta, fino a modificare la natura stessa delle diverse basi di dati.

---

[10] Tutto questo ha finito per impedire ai soggetti istituzionalmente deputati al controllo su tali sviluppi – lo stesso Parlamento nonché le autorità garanti di settore - di esercitare adeguatamente le proprie funzioni, con l'evidente rischio di decisioni poco rispettose dei diritti della persona.

[11] Il programma dell'Aia ha sottolineato l'importanza di una celere attuazione del VIS, che inizia incorporando, tra l'altro, i dati alfanumerici e le fotografie, al più tardi entro il 2006, e i dati biometrici, al più tardi entro il 2007 (su quest'ultima categoria di dati, si veda anche quanto detto più oltre).

A ciò si aggiunga il fatto che l'interconnessione comporta quasi sempre la messa a disposizione di un gran numero di informazioni non pertinenti ed eccedenti rispetto alle finalità perseguite, con conseguente violazione dei principi sopra richiamati. Per tale ragione, è ancora una volta indispensabile che questi cambiamenti siano condizionati alla predisposizione di un quadro adeguato di garanzie, volto ad assicurare il rigoroso rispetto dei richiamati principi di pertinenza, proporzionalità, e non eccedenza.

7. L'impatto delle nuove tecnologie sulle attività di indagine

Rischi e opportunità legati allo sviluppo tecnologico

Con riferimento al richiamato "principio di disponibilità" ed allo scambio di dati fra i diversi soggetti operanti nel quadro della cooperazione giudiziaria e di polizia, il programma dell'Aia prevede giustamente che si debbano "sfruttare appieno le nuove tecnologie". Al riguardo, dal punto i vista che qui maggiormente interessa, occorre ricordare che lo sviluppo tecnologico[12] ha un impatto almeno duplice per quanto attiene alla tutela della sicurezza e dell'ordine pubblico. Da una parte, infatti, espone i cittadini a nuovi rischi, ne aumenta 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

[12] 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 delle nuove 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.

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).
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: come già ricordato, 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.

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

Se 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.
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.

Alla luce di queste considerazioni, e sulla base di quanto la legislazione nazionale di alcuni Paesi ha già cominciato a fare, appare innanzi tutto necessario disciplinare attraverso la normativa comunitaria il regime di alcune grandi banche dati private dalle quali gli organi di polizia sono soliti attingere informazioni per le indagini (si pensi a quelle detenute dagli operatori telefonici sul traffico realizzato dai diversi utenti), stabilendo termini certi di conservazione dei dati, derogabili solo per i casi nei quali le informazioni in esse contenute siano acquisite dagli organi di polizia per specifiche esigenze e comunque sotto il controllo dell'autorità giudiziaria.
Occorre inoltre prevedere che i dati raccolti per altre finalità possano essere resi disponibili alle forze di polizia solo per lo svolgimento di specifiche indagini, sulla base di regole definite in via generale con disposizioni di rango legislativo che vedano un intervento del Parlamento europeo nonché seguendo una procedura autorizzatoria, riguardante anche categorie uniformi di trattamenti, che preveda il coinvolgimento delle autorità garanti nazionali o europee.
Ciò, anche in considerazione della facilità con cui tecnologie pensate per un determinato uso vengono poi adoperate per altri impieghi, con un conseguente accrescimento del numero di dati raccolti e potenzialmente utilizzati per le più diverse finalità (solo un esempio: i cosiddetti "braccialetti elettronici", in ordine ai quali si è discusso animatamente con riferimento al loro possibile utilizzo ai fini di controllo e localizzazione delle persone sottoposte a provvedimenti restrittivi della libertà personale, pochi mesi dopo sono stati offerti sulle spiagge per consentire alle madri apprensive di controllare che i figli non si allontanassero troppo …).

8. I rischi legati all'utilizzo dei dati biometrici

Il programma dell'Aia prevede che la gestione dei flussi migratori e la lotta all'immigrazione clandestina, anche ai fini di prevenzione e contrasto del crimine, siano rafforzate con una serie di misure di sicurezza basate su soluzioni armonizzate in materia di identificatori e dati biometrici. In questo quadro, al Consiglio, alla Commissione ed agli stati membri è stato dato il mandato di proseguire gli sforzi per integrare gli identificatori biometrici nei documenti di viaggio, nei visti, nei permessi di soggiorno e nei passaporti.
I dati biometrici presentano diversi vantaggi per quanto attiene alla possibilità di identificare con certezza e univocità le persone[13]. Tuttavia, bisogna rifuggire dalla tentazione di affidarsi incondizionatamente alle potenzialità delle rilevazioni biometriche, essendo stata ampiamente dimostrata l'esistenza di margini di errore significativi nell'identificazione delle persone nonché la possibilità di riprodurre e falsificare taluni dati biometrici senza che l'interessato ne sia informato o anche contro la sua volontà.
In ogni caso, proprio per la loro natura, tali dati possono comportare notevoli rischi per la vita privata delle persone. Per tale ragione, occorre che il progettato inserimento di queste informazioni nei documenti avvenga in un quadro di garanzie sufficiente e che, soprattutto, non apra la via ad una raccolta sistematica di dati biometrici a fini identificativi. Dal punto di vista della protezione dei diritti delle persone, infatti, il grado di rischio è più contenuto se i dati biometrici inseriti nei documenti sono utilizzati esclusivamente al fine di verificare l'identità già nota di chi presenta il documento (limitandosi a conservare i dati all'interno del documento). Mentre i pericoli si moltiplicano nel caso in

[13] I tipi di dati biometrici che possono essere utilizzati sono numerosi e vanno dalla forma del viso o dell'orecchio alle impronte digitali, dal palmo della mano, alle caratteristiche dell'iride, della retina o della voce.

cui si immagini di arrivare alla creazione di una grande banca dati contenente le informazioni biometriche al fine di individuare un soggetto di cui non si conosce preventivamente l'identità.
L'inserimento dei dati in documenti quali i passaporti, implica il fatto che gli stessi possano essere rilevati e probabilmente archiviati anche in paesi esterni all'Unione, quando i cittadini li portano con loro proprio per recarsi in tali paesi (è infatti questa la funzione di questi documenti). Ed è ben noto il fatto che in molti di tali stati non vengono rispettati standard di protezione dei dati paragonabili a quelli europei, con la conseguente esposizione dei cittadini detentori di tali documenti a rischi anche particolarmente rilevanti. Ciò, anche a prescindere da ogni considerazione relativa al caso in cui siano proprio tali paesi a richiedere l'inserimento dei dati biometrici nei documenti al fine di garantire la propria sicurezza interna, come è sostanzialmente accaduto per gli Stati Uniti.
Inoltre, anche all'interno dei dati biometrici, occorre poi distinguere quelli la cui raccolta deve avvenire necessariamente con la collaborazione - e, quindi, nella consapevolezza - dell'interessato, da quelli per i quali tale consapevolezza può non esservi (si pensi ai sistemi di rilevazione basati sulla forma del viso ovvero sul timbro della voce). Dal punto di vista che qui interessa, è chiaro infatti che questi ultimi dati sono quelli che lasciano intravedere maggiori pericoli sia per quanto attiene alle raccolta degli stessi all'insaputa degli interessati, sia per il gran numero di informazioni collezionabili, proprio a causa della facilità e all'ampiezza con cui è possibile arrivare alla raccolta. Attraverso una raccolta generalizzata di questi ultimi dati, sarebbe infatti relativamente semplice arrivare alla costituzione di uno smisurato database attraverso il quale si potrebbe risalire alle abitudini di una persona sia nella sfera pubblica che in quella privata, giungendo a forme di profilazione estremamente invasive.
Per tutte queste ragioni è dunque necessario che, con riguardo a tale categoria di dati, i principi di pertinenza, non eccedenza e proporzionalità sopra richiamati siano applicati con estremo rigore, evitando la raccolta o il trattamento di tali dati in tutte le circostanze nelle quali ciò non sia assolutamente indispensabile.