

Giovanni Buttarelli

**Incontro con le Autorità comuni di controllo del cd. Terzo Pilastro
(Schengen, Europol, Eurojust e Dogane)**

Bruxelles, Palazzo Justus Liptius

21 dicembre 2004, ore 15-16

Probabilmente, l'incontro ufficiale di oggi non ha precedenti, almeno nei termini in cui è stato convocato.

Per questo, è anzitutto opportuno ringraziarvi per l'invito che le vs. autorità comuni riunite in seduta congiunta mi hanno rivolto.

Molti di voi hanno potuto seguire le mie audizioni al Parlamento europeo quale candidato commissario.

Avete potuto notare come già in quelle sedi, a nome della Commissione, ho evidenziato le questioni aperte sulla protezione dei dati e la necessità di delineare una strategia europea più coerente per assicurare uno spazio di libertà, sicurezza e giustizia, tutelando più a fondo quel diritto fondamentale alla protezione dei dati personali che è ora sancito in due articoli del Trattato.

Gli impegni che abbiamo preso in quella circostanza caratterizzeranno il lavoro della Commissione: rispetto della Carta e del Trattato, dialogo più stretto con il Parlamento europeo, collaborazione più intensa con le autorità di garanzia.

I rapporti istituzionali tra voi e gli uffici della Commissione erano già buoni. I commissari Vitorino e Bolkestein hanno svolto un'intensa attività.

A volte, si è forse registrato un *gap* nella tempestiva conoscenza del lavoro rispettivamente svolto, come pure qualche difficoltà a comprendere le motivazioni sottostanti alle posizioni degli uni e degli altri.

La mia presenza, oggi, vuole testimoniare la possibilità di lavorare di più, assieme, per perseguire meglio i compiti che abbiamo rispettivamente assegnati.

La Commissione ha di fronte una stagione intensa di lavoro per portare a termine una tra le priorità dell'Unione: intensificare ulteriormente le varie attività di cooperazione giudiziaria e di polizia.

Le convenzioni o decisioni che hanno istituito le vs. autorità comuni di controllo vi assegnano compiti delicati, ma in ambiti specifici, per controllare i complessi trattamenti di dati personali che, caso per caso, si svolgono nell'ambito dei delicati sistemi informativi che sono stati creati.

Questa funzione resta attuale, ma non è forse più adeguata alle esigenze del ns. tempo.

Quali sono, infatti, le sfide del prossimo futuro ?

Quali nuovi bilanciamenti tra *privacy* e sicurezza sarà necessario raggiungere?

Come sarà, a medio-lungo termine, il quadro istituzionale del controllo sulla protezione dei dati a livello europeo ?

Quale ruolo per voi tutti ? Vi attende una funzione solo di controllo o anche un importante ruolo consultivo già nelle fasi preliminari alle scelte politiche ?

Attraverso quanti e quali organi di protezione dei dati a livello europeo ?

Nel breve periodo, quali percorsi possiamo percorrere assieme ?

Per le risposte che dovremo dare a queste istanze credo sia importante partire proprio dalla Risoluzione che le vs. autorità hanno adottato a Wroclaw il 14 settembre scorso.

In particolare, penso alla vs. richiesta di guardare a queste problematiche in modo non frammentato, convenzione per convenzione, ma organico, creando di fatto un innovativo *forum* istituzionale che permetterà finalmente di formulare scelte più strategiche.

Sappiamo tutti che le convenzioni istitutive delle Vs. autorità comuni di controllo sono nate in tempi diversi e che ciascuno dei sistemi informativi europei da esse creati è stato costruito in modo diverso per rispondere a specifiche esigenze: come voi stessi avete più volte evidenziato, ad esempio nei vs. pareri sul SIS II, il Sistema di informazione Schengen (SIS) è stato istituito per finalità “statiche” di documentazione e per consentire l’attuazione della libera circolazione delle persone. Il sistema Europol, in teoria più complesso ed ambizioso (come dimostra il fatto che metà della Convenzione istitutiva è dedicata alla protezione dei dati), aspira invece ad una notevole e mutevole pluralità di archivi, anche di analisi, ai fini di una “elaborazione intelligente” delle informazioni.

Sappiamo ancora che mentre il SIS è forse riuscito meglio a perseguire gli scopi meno ambiziosi fissati dalla Convenzione Schengen originaria, altri sistemi informativi comuni hanno evidenziato lentezze e lacune e che ad esempio per Europol si stanno discutendo in molte sedi le ragioni che rallentano l’afflusso di dati da parte degli Stati membri e che non derivano dalla necessità di tutelare la *privacy*.

Sappiamo infine che tutte queste basi dati europee pongono alcune difficoltà giuridiche ed operative quando dobbiamo verificare se e come le informazioni siano intrecciabili a livello europeo o nazionale, e conosciamo anche i rischi di una parziale sovrapposizione dei sistemi.

A livello nazionale, le Vs. autorità non hanno sempre gli stessi poteri.

Per altro verso, il negoziato Europol sul flusso di dati verso Paesi terzi ha dimostrato che non è facile limitare il numero o la tipologia delle autorità interessate ai dati a fini investigativi.

In tutte queste problematiche, abbiamo quindi corso e corriamo ancora il rischio di scontentare le autorità di polizia e di giustizia (giustamente desiderose di nuovi e più efficienti strumenti contro la criminalità e costrette invece a fare i conti con sistemi da aggiornare costantemente alle tecnologie e non sempre intrecciabili tra loro, malgrado i notevoli costi economici). Ma possiamo scontentare anche le autorità di protezione dei dati (preoccupate del fatto che l'ampliamento degli accessi e delle finalità di uso dei sistemi avvenga senza una precisa base giuridica, o per finalità non sufficientemente determinate o non rispettando regole importanti di protezione dei dati).

Tutto questo ci dice che dobbiamo individuare nuove modalità per intensificare la cooperazione giudiziaria e di polizia e gli scambi di dati. Possiamo dare risposte adeguate alle crescenti domande di sicurezza che ci vengono dai cittadini, anche in riferimento ai fatti di terrorismo che si succedono nel mondo a partire dall'11 settembre. Dobbiamo coinvolgere non solo il Parlamento europeo, ma anche i Parlamenti nazionali, per la catena degli adempimenti collegati con il

quadro normativo dei singoli Paesi: “*fornire ai cittadini un livello elevato di sicurezza in uno spazio di libertà, sicurezza e giustizia*” è, appunto, il mandato che proveniva dall’art. 29 del Trattato di Amsterdam.

Dobbiamo forse individuare assieme una nuova generazione della protezione dei dati.

Non partiamo da zero per questo, visto che dobbiamo restare fedeli ai principi della Carta dei diritti fondamentali inseriti nella futura Costituzione per l’Europa, alla giurisprudenza della Corte europea dei diritti dell’uomo, alla Convenzione n. 108/1981 di Strasburgo e alle Raccomandazioni del Consiglio d’Europa. Vi sono inoltre le esperienze di tutti i Paesi dell’Unione che, trasponendo la direttiva 95/46/Ce, hanno quasi sempre applicato vari suoi principi anche a diversi trattamenti di dati effettuati per finalità di sicurezza, di giustizia e persino alle attività di *intelligence*.

Tutte queste esperienze devono essere ora sviluppate e arricchite in relazione al tempo che viviamo.

Può darsi che tutto ciò richieda nuove norme giuridiche generali a livello europeo, come può darsi che sia sufficiente elaborare solo alcuni principi generali da rispettare nella prassi e nella redazione di future convenzioni.

Quel che conta, è che si completi l’armonizzazione del quadro della protezione dei dati nel III Pilastro.

Le garanzie per i cittadini devono essere mantenute, rispettate e rivalutate alla luce dello sviluppo delle reti, delle tecnologie e dei tipi di

dati impiegati, visto, ad esempio, che potrebbe esserci un uso intensivo della biometria.

Nella protezione dei dati, abbiamo forse bisogno di più attenzione alle garanzie sostanziali, piuttosto che agli adempimenti formali che pure hanno il loro rilievo.

Privacy e sicurezza non sono in antitesi, né si tratta di beni da bilanciare per sacrificare una parte dell'una o dell'altra. Piuttosto, l'una è il presupposto dell'altra e viceversa. Il diritto alla sicurezza ha, come condizione non alienabile, il diritto a veder rispettati -come garanzie di efficienza dell'azione dei pubblici poteri- i diritti e le libertà della personalità.

Sono d'accordo con voi quando, a gran voce, richiamate l'attenzione sul principio di proporzionalità e sulla necessità che le scelte nel c.d. III Pilastro siano valutate preventivamente in termini di impatto sui diritti dei cittadini, evitando possibili lacune, frammentazioni e sovrapposizioni tra iniziative europee e soluzioni nazionali.

La Commissione è disponibile a lavorare ancora più intensamente sotto questo profilo e a svolgere con cura il ruolo che i Trattati le hanno affidato.

Già da vari anni, l'obiettivo definito dal Consiglio europeo di Tampere, volto ad assicurare il pieno sviluppo di un'area di libertà, giustizia e sicurezza all'interno dell'Unione europea, ha evidenziato la necessità di un piano di azione coerente per favorire l'accesso alle basi di dati disponibili e lo scambio di informazioni tra le autorità competenti.

Dobbiamo essere consapevoli che quelli che vengono considerati ostacoli di *privacy* derivano a volta da politiche non interamente

coerenti, dall'eccessiva diversità di alcuni contesti nazionali e, soprattutto, dal fatto che l'intensità e la successione delle iniziative normative sinora adottate non ha permesso una riflessione globale sul modo con cui i sistemi possono dialogare tra loro a livello centrale e nazionale, senza duplicazioni e senza eludere il principio delle finalità determinate del trattamento che ora è ribadito ad alto livello dall'art. II—68 della Costituzione per l'Europa. Queste difficoltà sono aumentate quando a livello europeo sono state promesse alcune azioni *ad hoc* legate ad esempio agli scambi di dati tra polizie in occasione di vertici internazionali o violenze presso stadi.

Da ciò le recenti proposte motivate dalla necessità di combattere in primo luogo il terrorismo, che mirano a rendere il più possibile comunicanti tra di loro i vari sistemi esistenti a livello europeo ed anche gli archivi nazionali, nonostante le diversità di legislazioni tuttora presenti.

Il programma dell'Aja, che prosegue per il prossimo quinquennio quello di Tampere, introduce a questo proposito il principio della disponibilità: le forze di polizia e gli organi giudiziari potranno accedere agli archivi degli Stati membri ed ottenere le informazioni che sono necessarie per perseguire gli obiettivi assegnati.

Sono consapevole delle preoccupazioni che avete sinora espresso riguardo alle proposte volte ad incrementare gli scambi di informazioni: vi siete dichiarati consapevoli della necessità di farlo, ma avete espresso perplessità per come le proposte sono formulate e per far rispettare il principio di proporzionalità.

Il dossier SIS II è certamente centrale, al riguardo.

Il Parlamento europeo ha recepito molti dei vs. suggerimenti a proposito delle proposte spagnole di modifica della Convenzione Schengen e credo, in particolare, che la presidenza italiana e, poi, olandese, dell'ACC Schengen abbiano svolto un buon lavoro, rappresentando la difficoltà di prevedere nuove funzioni intelligenti, oppure nuovi accessi da parte di Europol ed Eurojust e nuove finalità, senza cambiare al tempo stesso l'impianto "statico" complessivo di Schengen, basato solo su una risposta "Si/No" alla domanda sulla presenza o meno di dati su una certa persona.

Ora, dobbiamo dare finalmente uno sbocco equilibrato agli interrogativi che i garanti europei hanno posto non solo nell'ambito delle autorità comuni di controllo, ma anche del Gruppo Art. 29, a cominciare da quelli riguardanti l'inserimento dei dati biometrici nei visti e nei passaporti, anche nella prospettiva della creazione del VIS e del SIS II.

I problemi derivano anche dal fatto che nel I Pilastro esiste già una disciplina armonizzata che garantisce un buon livello di tutela, mentre nel III Terzo Pilastro si è interrotto il percorso che, a partire dalla nota iniziativa italiana del 1999, poi ripresa dalla presidenza portoghese dell'Unione e da contributi del servizio giuridico del Consiglio, era stato intrapreso per elaborare un decalogo di principi-guida della protezione dei dati, appunto, nel III Pilastro.

Il programma dell'Aja perfeziona gli obiettivi di Tampere e contiene alcune aperture, in particolare richiedendo alla Commissione di presentare proposte entro il 2005 che tengono conto della necessità di osservare alcune condizioni fondamentali in materia di protezione dei dati (liceità del trattamento, integrità dei dati, garanzie di confidenzialità,

regole per gli accessi, diritti degli interessati, necessità di una supervisione).

La DG Jai sta portando avanti una riflessione al riguardo e l'occasione sembrerebbe ormai matura per introdurre adeguati generali principi in materia, a cominciare dagli *standard* comuni per il flusso di dati verso Paesi terzi, compreso Interpol.

Sarà molto utile conoscere il parere delle autorità di protezione dei dati che sono state invitate per un primo scambio di idee l'11 gennaio prossimo sugli aspetti legati agli scambi di informazione e all'introduzione del principio della "disponibilità" dei dati.

So anche che nel corso di una riunione all'Aja convocata per il 28 gennaio discuterete questi temi e potrete forse adottare poi qualche importante decisione in occasione della Conferenza europea di aprile in Polonia.

Tutto ciò è utile perché il vs. ruolo potrà essere rivalutato. Dobbiamo già giudicare positivamente il fatto che le vs. autorità comuni abbiano anticipato le future riflessioni ottenendo la creazione di un segretariato comune, mandando qui a Bruxelles gli stessi rappresentanti nelle varie riunioni e cominciando da alcuni mesi a riunirsi congiuntamente, dando anche una risposta responsabile ai problemi di *budget* che vi affliggono nel difficile rapporto tra le esigenze di economicità e l'esigenza di ribadire la vs. autonomia quando dovete procedere a missioni e ispezioni.

Tenendo conto delle disposizioni introdotte in materia dal Trattato, il vs. ruolo di consulenza potrebbe essere valorizzato andando oltre il mandato specifico di ciascuna autorità comune di controllo, per

costituire un quadro coerente di riferimento in analogia con quanto avviene nel I Pilastro con il Gruppo Art. 29.

Del resto, la vicenda del trasferimento negli USA dei dati dei passeggeri dei voli aerei dimostra che la distinzione tra I e III Pilastro si fa sempre più sottile e che i diritti e le libertà vanno ora esaminati con un approccio orizzontale.

Ci sono in conclusione molti punti da approfondire. Ad esempio, la praticabilità:

- 1- di un nucleo di principi–guida per il trattamento dei dati personali nel III Pilastro, eventualmente con la possibilità di adattare i principi applicabili a seconda delle finalità perseguite: ad esempio, per gli scambi di informazioni i principi individuati nel programma dell'Aja (pag. 22) potrebbero essere una base di partenza sufficiente, mentre per la creazione di basi di dati a livello europeo andrebbero previsti ulteriori principi;
- 2- di una reale valutazione preventiva della proporzionalità delle future misure da introdurre, guardando all'impatto della proposta sui diritti fondamentali, compreso il diritto alla protezione dei dati personali, andando oltre gli omaggi formali di solito a volte contenuti nei preamboli delle iniziative presentate;
- 3- di una contestualità tra l'adozione delle nuove forme di cooperazione di polizia e giudiziaria e l'adozione dei principi di protezione dei dati: la *deadline* per questi ultimi non figura nel programma dell'Aja e dobbiamo

- valutare il problema anche in riferimento ai lavori normativi in corso;
- 4- di un coinvolgimento più incisivo delle autorità di protezione dei dati nella predisposizione dei principi, in forme opportune da individuare, chiarendo anche il ruolo che la Commissione può svolgere per valorizzare questi contributi;
 - 5- di un'attenzione particolare nell'individuare le possibilità di avvalersi del principio di disponibilità introdotto dal programma dell'Aja;
 - 6- della previsione di regole specifiche per trasferire i dati a Stati ed organismi terzi, inserendo un principio che regoli la possibilità di trasmettere ulteriormente i dati ricevuti con il previo consenso della parte che li invia;
 - 7- di una riflessione sull'attuale e futuro assetto delle autorità chiamate a svolgere un controllo indipendente.

Il coinvolgimento delle autorità di protezione dei dati fin dall'inizio è il valore aggiunto da ricercare e per questa opportunità non posso che tornare a ringraziarvi, convinto che cercheremo entrambi di dare concretezza alla collaborazione che vogliamo incrementare.