CENTRO STUDI SUL FEDERALISMO

ALCUNE PRIME CONSIDERAZIONI SUI SISTEMI DI SCAMBIO DI INFORMAZIONI NELLO SPAZIO DI LIBERTÀ, SICUREZZA E GIUSTIZIA: SECURITIZATION, FUNCTION CREEP E TUTELA DEI DIRITTI

Lucia Musselli

Maggio 2013

Research Paper

ISSN: 2038-0623
ISBN 978-88-96871-43-0

Copyright © Centro Studi sul Federalismo 2013

Tutti i diritti sono riservati. Parti di questa pubblicazione possono essere citate nei termini previsti dalla legge che tutela il diritto d'autore e con l'indicazione della fonte.

All rights reserved. Quotations from this paper can be made according to copyright law, providing information on the source.

ABSTRACT

Il venir meno delle frontiere fisiche all'interno dell'Unione europea ha determinato nel corso del tempo la creazione di "frontiere" tecnologiche rappresentate da database di larga scala, principalmente utilizzati ai fini dell'identificazione delle persone.

Nel corso del tempo, e particolarmente dopo i fatti dell'11 settembre 2001, si è assistito, in taluni casi, a un ampliamento degli scopi originari per i quali questi strumenti erano stati istituiti in nome di esigenze di securitization*.*

Scopo del paper *è quello di procedere alla descrizione delle tre principali banche dati interne a livello europeo, SIS, Eurodac e VIS, operanti nell'ambito dello spazio di libertà, sicurezza e giustizia. La ricostruzione delle banche dati, alla luce degli atti istitutivi, tenta inoltre di mettere in luce alcune criticità collegate, da un lato, alla tutela dei diritti delle persone e dall'altro ad alcune problematiche relative alla scarsa trasparenza dei processi decisionali che hanno condotto alla loro istituzione e/o modificazione.*

Lucia Musselli è professore associato di diritto amministrativo presso l'Università degli studi di Milano.

E-mail: lucia.musselli@unimi.it

1. Dalle frontiere "fisiche" alle frontiere "tecnologiche": aspetti introduttivi [*]

La libertà di circolazione e di stabilimento dei cittadini UE costituisce uno dei principi fondamentali dell'Unione Europea[1] e la creazione di un'area geopolitica (c.d. Area Schengen), nell'ambito della quale risultano eliminati i controlli alle frontiere interne, rappresenta la plastica manifestazione del livello di integrazione raggiunto.

Tale processo, come noto, prese le mosse nel 1985 quando cinque Stati, Germania, Francia, Belgio, Lussemburgo e Paesi Bassi decisero di abolire i controlli sulle persone alle frontiere[2].

L'abolizione dei controlli interni determinò, d'altro canto, come ben emerge dalla Convenzione applicativa dell'Accordo di Schengen, la necessità di definire un sistema di previsioni comuni volte a rafforzare i controlli alle "comuni frontiere esterne" dell'Unione, prevedendosi un set di regole dettagliate relative all'ingresso ed all'uscita dei cittadini di paesi terzi, accompagnate da misure di cooperazione in materia giudiziaria e di attività di polizia[3].

Oggi l'area Schengen è una realtà che interessa la maggioranza dei paesi dell'Unione europea[4], coinvolge anche alcuni paesi non UE[5] per un totale di circa 400 milioni di cittadini europei; essa si fonda sul divieto di controlli sistematici alle frontiere interne e sul rispetto, da parte dei paesi aderenti, di una serie di rigorose condizioni richieste dall'*acquis Schengen*, di cui oggi si prevede un più efficace strumento di valutazione e monitoraggio i cui esiti sono documentati in *reports* biennali elaborati dalla Commissione[6].

La rimozione fisica delle barriere determinò l'immediata necessità di prevedere un sistema informativo, denominato "Sistema di informazione Schengen" (SIS), in grado di garantire una

---

[*] Desidero ringraziare i professori Paola Bilancia e Filippo Scuto per aver letto una prima versione di questo *paper*. Un particolare ringraziamento va inoltre alla professoressa Alessandra Lang per i preziosi suggerimenti. Eventuali errori od omissioni sono, comunque, di esclusiva responsabilità dell'Autrice.

[1] Sulle numerose implicazioni di tale principio vd. M. CONDINANZI, A. LANG, B. NASCIMBENE (edts.), *Citizenship of the Union and Freedom of Movement of Persons*, Leiden-Boston, 2008.

[2] A questi paesi se ne aggiunsero poi altri, tra cui l'Italia, e nel 1990 quell'accordo diede vita alla Convenzione di Schengen (Convenzione di applicazione dell'Accordo di Schengen firmato il 19 giugno 1990), eseguita dal 1995. Nel 1999 essa perde la sua natura intergovernativa e viene integrata nell'ambito dell'Unione europea, attraverso il Trattato di Amsterdam. Per l'evoluzione normativa vd. B. NASCIMBENE, M. PASTORE (a cura di), *Da Schengen a Maastricht*, Milano, 1995.

[3] Sul punto vd. A. F. ATGER, *The abolition of International Border Checks in an Enlarged Schengen Area: Freedom of movement or a scattered web of security checks?*, CEPS Challenge Paper, No. 8, 2008 in www.ceps.eu, in part. 5 ss.

[4] Fatta eccezione, seppure per motivi diversi, per la Bulgaria, Cipro, l'Irlanda, la Romania e il Regno Unito.

[5] Quali Islanda, Norvegia, la Svizzera e il Lichtenstein.

[6] Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico-sociale e al Comitato delle regioni "Governance Schegen- Rafforzare lo spazio senza controlli alle frontiere esterne", 16.09.2011, COM(2011) 561 definitivo e, da ultimo, European Commission, *Report from the Commission to the European Parliament and the Council - Second biannual report on the functioning of the Schengen Area 1 May 2012-31 October 2012*, 23.11.2012, COM(2012) 686 final.

condivisione delle informazioni tra le autorità dei paesi aderenti circa persone ed oggetti segnalati.

La Convenzione di Schengen, nata per agevolare la libertà fondamentale della circolazione delle persone, contiene inoltre una prima forma embrionale di regolamentazione dell'immigrazione, seppure intesa in forme prevalentemente restrittive, volte a colpire l'immigrazione irregolare[7].

Con il passare del tempo questo scenario si amplia e si intreccia con quello relativo all'affermazione dello spazio di libertà, sicurezza e giustizia (SLSG) ed al progressivo sviluppo, in tale ambito, di una "autonoma" politica europea dell'immigrazione[8].

Il processo che parte dagli anni Novanta ed è rivolto all'affermazione di uno spazio europeo di libertà, sicurezza e giustizia, oggi fondato sull'art. 3 del TFUE[9], risulta basato su presupposti che sottendono un livello di integrazione politica assai avanzato. In particolare, com'è stato efficacemente ricordato, si assiste all'abbandono di un modello di cooperazione in ottica meramente "mercantile" a favore della delineazione di uno spazio "entro il quale le persone in quanto tali possono spostarsi liberamente – senza incontrare ostacoli determinati dalla sopravvenienza dei confini nazionali in condizioni di sicurezza, contando su di un regime armonizzato circa l'apprezzamento dei valori giuridici che presiedono a tale mobilità e circa le modalità di accesso alla giustizia"[10].

Il cammino di costruzione dello SLSG, d'altro canto, pone subito in evidenza aspetti problematici in materia di "*internal security risks of a transboundary nature*", in parti comuni a quelli relativi allo Spazio Schengen[11].

Tra questi, particolari rilievo assumono alcuni profili critici relativi all'immigrazione, che peraltro nel tempo – e particolarmente dopo il Trattato di Amsterdam – è diventata a pieno titolo materia

---

[7] Mediante la previsione di regole dettagliate sull'attraversamento delle frontiere esterne e sul controllo degli stranieri che intendevano attraversarle. In tal senso vd. l'accurata analisi di F. SCUTO, *I diritti fondamentali della persona quale limite al contrasto dell'immigrazione irregolare,* Milano, 2012, 75 ss.

[8] Sul punto, per una ricostruzione di tale evoluzione vd. A. LANG, *Giustizia ed affari interni,* in M.P. CHITI, G. GRECO (a cura di), *Trattato di diritto amministrativo europeo,* Torino, 2007, 1143 ss. e, da ultimo, vd. P. BILANCIA, *The dynamics of the EU Integration and the impact on the National Constitutional Law - The European Union after the Lisbon Treaties,* Milano, 2012, 119 ss.

[9] Ai sensi dell'art. 3 c. 2 del TUE, nella versione consolidate dopo Lisbona, si afferma che: "L'Unione offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, in cui sia assicurata la libera circolazione delle persone insieme a misure appropriate per quanto concerne i controlli alle frontiere esterne, l'asilo, l'immigrazione, la prevenzione della criminalità e la lotta contro quest'ultima". Sul punto vd. P. BILANCIA, *Lo spazio di libertà, sicurezza e giustizia tra realtà intergovernativa e prospettiva comunitaria,* in P. BILANCIA, F.G. PIZZETTI (a cura di), *Aspetti e problemi del costituzionalismo multilivello,* Milano, 2004, 345 ss.

[10] Così D. RINALDI, *L'assetto dello spazio di libertà, sicurezza e giustizia" dopo il Trattato di Lisbona: elementi di continuità e discontinuità,* in N. PARISI, V. PETRALIA (a cura di), *L'Unione europea dopo il Trattato di Lisbona,* Torino, 2011, 333. Per una recente analisi di tale processo, con particolare riferimento alla questione delle armonizzazione delle norme penali, vd. G. MARCHETTI, *I recenti passi avanti compiuti dall'Unione europea nella direzione di un'armonizzazione dei sistemi penali,* Novembre 2012, in www.csfederalismo.it.

[11] Al riguardo vd. le riflessioni di J. MONAR, *Cooperation in the Justice and Home Affairs Domain: Characteristics, Constraints and Progress,* in *Journal of European Integration* 2006, 495 ss. Giustamente l'autore precisa come la questione dell'immigrazione illegale "*does not qualify as an internal security risk* per se", anche se presenta delle "*implications for internal security: think of the heavy involvement of organized crime in the facilitation of illegal immigration and trafficking in human beings, the crime rates amongst illegal immigrants with no access to the regular labour market and social security…*" (p. 496).

"comunitaria", oggetto, assieme a quella dell'asilo, di politiche comuni, le cui linee di azione sono ben illustrate nel Programma di Stoccolma[12].

Con particolare riguardo a tale aspetto occorre segnalare che se sicuramente l'aumento della pressione migratoria alle frontiere "esterne" dell'Unione europea, soprattutto a seguito della c.d. "Primavera araba", ha accentuato alcune problematiche collegate alla "sicurezza" tuttavia l'approccio europeo ha seguito un percorso evolutivo nell'ambito del quale, per raggiungere tale obiettivo, sono stati previsti strumenti di tipo diversi. Così, a fianco dell'utilizzo in misura sempre crescente di strumenti tecnologici atti a procedere all'*identificazione* dei soggetti non cittadini europei- e su questo si appunterà la nostra indagine- se ne sono affiancati altri volti a privilegiare la dimensione cooperativa tra gli Stati dell'Unione e gli Stati terzi[13]. Tra queste di particolare rilievo sono la previsione di forme di cooperazione intereuropea mediante la creazione dell'Agenzia Frontex e, a livello esterno, la promozione, in un'ottica di approccio globale alla problematica dell'immigrazione, del dialogo e della cooperazione con i paesi terzi[14].

Il processo di "autonomizzazione" dei settori della sicurezza e della gestione delle frontiere nell'area europea rispetto alle politiche comuni di immigrazione ed asilo subisce tuttavia una brusca battuta d'arresto dopo i fatti dell'11 settembre del 2001 e a seguito degli attentati di Madrid e Londra nel 2004 e 2005. Da questo momento le tematiche della gestione delle frontiere, del controllo dell'immigrazione e della lotta al terrorismo risulteranno fortemente collegate tra di loro. In particolare, nel dibattito pubblico, le *policy* relative all'immigrazione, all'integrazione dei migranti ed alla sicurezza vengono considerate come parti di uno stesso problema (da qualcuno polemicamente inteso nei termini di "*(in) security continuum*"), riassuntivamente espresso nella formula della *border security*[15].

In tale ottica risulta evidente che il raggiungimento dell'obiettivo di sicurezza transfrontaliera dipende in modo sempre significativo dall'utilizzo delle tecnologie, le quali non si identificano oggi tanto nella "forza bruta" delle navi, aerei od elicotteri che pattugliano le frontiere, quanto in strumenti tecnologici sempre più raffinati e complessi volti al riconoscimento delle persone sulla base della raccolta di dati "forniti" dal corpo umano, conservati e trattati in banche dati[16].

Tale fenomeno presenta aspetti di grande interesse, sia sotto il profilo organizzativo che con riferimento alle collegate esigenze di tutela dei diritti delle persone coinvolte.

---

[12] Sul punto vd. F. SCUTO, *I diritti fondamentali della persona*, cit. 71 ss.

[13] Per la descrizione delle varie tipologie di azioni europee nel settore dell'immigrazione vd. G. PINYOL JIMÉNEZ, *The Migration-Security Nexus in Short: Instruments and actions in the European Union,* in *Amsterdam L.F.*, 2012, 37 ss.

[14] Cfr. Consiglio dell'Unione europea, *Programma di Stoccolma - Un'Europa aperta e sicura al servizio e a tutela dei cittadini*, in GU C 115 del 4.05.2010, par. 6.1.1. Su Frontex vd. Da ultimo A. CANEPA, *The regulatory role of FRONTEX: risk analysis, border management and Exchange of data*, in L. AMMANNATI (ed.), *NETWORKS - In search of a Model for European and Global Regulation*, Torino, 2012, 127 ss.

[15] Così H. DIJSTELBLOEM, *Europe's New Technological Gatekeepers. Debating the Deployment of Technology in migration Policy,* in *Amsterdam L.F.* 11, 2008-2009, 12. Nello stesso senso vd. anche A. BALDACCINI, *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases,* in *Eur. J. Migration & L.*, 2008, 31 ss. Per un'analisi delle diverse questioni giuridiche che in tale contesto sorgono, con riferimento alla tutela dei soggetti vd. M. PEDRAZZI, I. VIARENGO, A. LANG (edts.), *Individual guarantees in the European judicial area in criminal matters*, Bruxelles, 2011.

[16] In tal senso H. DIJSTELBLOEM, *Europe's New Technological Gatekeepers,* cit. 11.

L'impiego di banche dati di larga scala, sovente organizzate mediante "*European Information Networks*", prediligendosi la forma elastica ed adattativa della "rete"[17], diviene quindi un elemento basilare dei sistemi di scambio di informazione a livello europeo nell'ambito dello spazio di libertà, sicurezza e giustizia e in tal senso la gestione strutturata delle informazioni assume almeno una duplice valenza: a carattere operativo, con riferimento al controllo alle frontiere esterne, alla gestione dell'immigrazione e delle politiche dei visti e di supporto al processo di *policy-making*[18].

A livello descrittivo i sistemi di scambio di informazioni utilizzati sono diversi e vengono classificati sulla base di differenti criteri ordinatori.

Una prima distinzione può essere fatta con riferimento alla tipologia di soggetti coinvolti, che possono essere gli Stati membri, le istituzioni europee, le parti private e paesi terzi (o organizzazioni internazionali)[19]. A seconda di quali siano i soggetti interessati troviamo differenti modellistiche organizzative.

Il primo modello, che è anche quello che ci interessa maggiormente, è rappresentato dallo scambio di informazioni tra paesi membri (o comunque aderenti al sistema) ed istituzioni europee che viene realizzato attraverso la previsione di un database centrale raccordato a punti nazionali come nel caso di SIS (*Schengen Information System*), Europol, Eurojust e VIS. Un secondo modello, invece, prevede uno scambio di informazioni tra Stati membri e privati; questo è il caso, ad esempio del sistema PNR (*Passenger Name Record*) che prevede l'impegno delle compagnie aeree a rendere disponibili, per finalità antiterroristiche, i dati dei passeggeri dei voli internazionali. Un terzo modello è rappresentato dal trasferimento di dati a paesi terzi, come nel caso della trasmissione dei dati PNR agli Stati Uniti. Da ultimo troviamo il modello di scambio di dati tra Stati membri sulla base di un accordo intergovernativo, come nel caso della Convenzione di Prüm, firmata nel 2005 da alcuni Stati europei[20].

Secondo un'altra ricostruzione invece i sistemi di scambio delle informazioni, intesi come *policy tools* e particolarmente come "*capacity instruments*" vengono distinti sulla base della loro rilevanza "interna" od "esterna" all'Unione[21].

A livello europeo il primo documento, che interviene, solo nel 2010, a ricostruire la panoramica dei sistemi di gestione dell'informazione nello spazio di libertà, sicurezza e giustizia è rappresentato dalla Comunicazione "Panorama generale della gestione delle informazioni nello spazio di libertà,

---

[17] Sul punto vd. L. AMMANNATI, *Governance e regolazione attraverso reti*, in L. AMMANNATI, P. BILANCIA (a cura di), *Governance multilivello regolazione e reti*, vol. II, Milano, 2008, 181 ss. e P. BILANCIA , *The area of freedom, security and justice*, cit. 120. Per l'utilizzo del modello della rete nell'ambito dei vari settori di *multilevel governance* vd., nello specifico, A. CANEPA, *Reti europee in cammino, regolazione dell'economia, informazione e tutela dei privati*, Napoli, 2010.

[18] Così J. MONAR, *Cooperation in the Justice*, cit. 500-501.

[19] Sul punto vd. M. TZANOU, *The EU as an emerging "Surveillance Society": The function creep case study and challenges to privacy and data protection*, in *Vienna Online J. on Int'l Const. L.*, 2010, 411-412.

[20] Sul punto vd. T. FREIXES, *Protección de datos y globalización. La Convención de Prüm*, in *Revista de derecho constitucional europeo*, 2007, 11 ss. e, nella dottrina italiana F. SCUTO, *I diritti fondamentali*, 143 ss.

[21] Sul punto cfr. T. BALZACQ, *The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies*, in *JCMS* 2008, 83 ss. Come strumenti "interni" vengono considerati Eurodac, SIS e VIS e come strumenti esterni gli Europol-USA Agreements e il PNR.

sicurezza e giustizia"[22]. Tale documento, pur nella molteplicità di schemi che propone, ben 25, distingue tra sistemi centralizzati quali SIS, VIS ed Eurodac e sistemi decentralizzati come quelli ai sensi della Convenzione di Prüm e della "*Swedish initiative*".

I sistemi di scambio di informazioni costituiscono dunque al momento uno dei principali strumenti utilizzati per garantire le varie *policy* sottese all'attuazione dello spazio di libertà, sicurezza e giustizia. Anche questi d'altro canto verranno toccati progressivamente da quel processo di *securitization*[23] che investe più in generale la materia dell'immigrazione dopo l'11 settembre.

L'effetto più significativo che si determinerà sarà quello dell'ampliamento (o a seconda dei punti di vista della distorsione) delle finalità originariamente attribuite ad alcune banche dati, analizzato dalla dottrina nell'ambito della teoria della *function creep*[24].

Venendo al profilo dell'attività delle banche dati occorre ricordare come la gestione delle informazioni ed in particolare il trattamento di informazioni biometriche, se da un lato risponde a concrete esigenze di efficienza dei sistemi di controlli alle frontiere, pone dall'altro in evidenza numerosi aspetti critici con riferimento alla tutela della vita privata e della privacy delle persone (artt. 7 e 8 della Carta dei diritti fondamentali dell'UE), alla "necessarietà" delle misure approntate, soprattutto alla luce della giurisprudenza della CEDU in materia di "*purpose limitation principle*"[25] ed all'effettività dei rimedi disponibili per la tutela dei diritti.

La dottrina inoltre non appare del tutto concorde circa il complessivo giudizio sull'efficienza e l'efficacia delle metodiche applicate e circa l'attendibilità dei risultati raggiunti[26].

Scopo di questo *paper* è quello di fornire una prima ricostruzione, alla luce delle considerazioni preliminari sopra esposte, dei tre principali strumenti d'informazione interni approntati a livello europeo nello spazio di libertà, sicurezza e giustizia: SIS, Eurodac e VIS. Si cercherà tuttavia di riscostruire il dato normativo non in modo puramente descrittivo, ma alla luce dei contributi e

---

[22] Comunicazione della Commissione al Parlamento europeo ed al Consiglio, 20.07.2010 COM(2010) 385 def. Per un commento a tale documento, che peraltro non fornisce una chiara definizione di "information management", precisando solo che non rientrerebbero nella nozione gli scambi di informazione concernenti "non-personal data" cfr. D. BIGO, S. CARRERA, B. HAYES, N. HERNANZ, J. JEANDESBOZ, *Justice and Home Affairs Databases and a Smart Borders System at EU External Borders - An Evaluation of Current and Forthcoming proposals,* CEPS Paper in *Liberty and Security in Europe* No. 52, Dicembre 2012, in www.ceps.eu, 4 ss.

[23] Con tale termine nella dottrina, prevalentemente politologica (sul punto vd. ad es. G. PINYOL JIMÉNEZ, *The Migration-Security Nexus in Short,* cit 38) si intende un approccio teoretico che "*describes a process whereby urgent security issues or "threats" are identified or "constructed" in order to mobilize opinion and constitute legitimacy and authority for dealing with that "threat"*". Sul punto vd. anche F. SCUTO (*I diritti fondamentali della persona,* cit. 96) che ricorda come "A partire dal 2001, l'ago della bilancia in quel difficile equilibrio, tipico di ogni politica relativa all'immigrazione, tra tutela dei diritti e esigenza di sicurezza interna, ha iniziato a pendere decisamente a favore della seconda".

[24] Emblematico è, come vedremo, il caso del SIS che, da strumento creato originariamente per il controllo e la sicurezza delle frontiere assume, nel tempo, anche il carattere di strumento investigativo. Per tale aspetto vd. V. MITSILEGAS, *Immigration Control in an Era of Globalization: Deflecting Foreigners, Weakening Citizens, Strengthening the State,* in *Indian Journal of Global Legal Studies,* 2012, 17 ss. Per un'analisi di tali banche dati nell'ottica della "function creep" vd. M. TZANOU, *The EU as an emerging "Surveillance Society"* cit.

[25] Sul punto vd. G. GONZÁLEZ FUSTER, P. DE HERT, E. ELLYNE, S. GUTWIRTH, *Huber, Marper and Others: Throwing new light on the shadows of suspicion,* CEPS INEX Policy Brief, No. 11, 2010, in www.ceps.eu.

[26] Per una chiara analisi di tali aspetti vd. H. DIJSTELBLOEM, *Europe's New Technological Gatekeepers,* cit. 11 ss.

delle criticità rilevate in dottrina. Ad un successivo livello di indagine ci si dedicherà invece all'analisi della giurisprudenza europea intervenuta in materia.

2. Il Sistema d'informazione Schengen (SIS e SIS II)

Il Sistema d'informazione Schengen venne previsto fin dall'origine dalla Convenzione di Schengen e divenne operativo nel 1995 con la finalità di garantire la sicurezza pubblica all'interno dell'Area Schengen[27]. Come già ricordato la sua istituzione può essere considerata come una sorta di misura "compensatoria" rispetto al venir meno delle frontiere fisiche tra gli Stati membri.

Il SIS si articola in un network di SIS nazionali (N-SIS), situati presso ciascuno Stato membro e in un data-base a livello centrale (C-SIS), localizzato a Strasburgo con il compito di trasferire e standardizzare i dati[28].

Nella banca dati SIS vengono inserite una serie di informazioni concernenti persone o cose. In particolare, ai sensi della Convenzione di Schengen, gli Stati membri potevano segnalare cinque categorie di persone: 1) persone ricercate per l'arresto ai fini di estradizione (art. 95); 2) cittadini di paesi terzi ai fini della non ammissione (art. 96); 3) persone scomparse (art. 97); 4) testimoni e persone citate a comparire dinnanzi all'autorità giudiziaria (art. 98); 5) persone sottoposte a monitoraggio in quanto costituenti minaccia per la sicurezza (art.99).

Oltre alle informazioni su persone venivano inserite nella banca dati anche informazioni riferite a cose[29]. I dati inseriti nel sistema SIS erano il nome e cognome della persona, eventuali segni fisici particolari, data e luogo di nascita, sesso e nazionalità o se la persona fosse armata o ritenuta pericolosa. Così come era stato originariamente inteso il SIS ospitava prevalentemente informazioni di carattere alfanumerico. A tali dati potevano accedere, nei limiti delle proprie aree di competenza, le autorità di polizia, le autorità di controllo alle frontiere, le autorità doganali e le autorità giudiziarie nei procedimenti penali.

Le interrogazioni alla banca dati SIS funzionano secondo un sistema denominato "*hit/ no hit*"; si ottiene un "hit", cioè una segnalazioni positiva, quando le indicazioni relative ad una persona od oggetto corrispondono a quelle di una segnalazione esistente[30]. Ottenuto un "*hit*" positivo le autorità competenti possono rivolgersi, per ottenere informazioni supplementari, agli uffici della rete SIRENE (*Supplementary Information Request at the National Entry*) che costituisce uno strumento ausiliario del SIS per fornire tutta una serie di informazioni, quali le impronte digitali e le fotografie.

---

[27] In particolare il titolo IV della Convenzione di Schengen è dedicato al "Sistema di informazione Schengen". Ai sensi dell'art. 93 il suo scopo è quello "di preservare l'ordine pubblico e la sicurezza pubblica, compresa la sicurezza dello Stato e di assicurare l'applicazione, nel territorio delle Parti contraenti delle disposizioni sulla circolazione delle persone stabilite nella presente Convenzione".

[28] Cfr. J. MONAR, *Cooperation in the Justice and Home Affairs Domain*, cit. 501.

[29] Quali veicoli soggetti a monitoraggio straordinario per le loro caratteristiche si costituire una minaccia per la sicurezza pubblica o la sicurezza dello Stato, documenti ed armi da fuoco persi o rubati; banconote registrate.

[30] In caso di hit positivo il sistema forniva il comando "*apprehend this person*" o "*stop this vehicle*".

Lo stretto collegamento esistente tra i due sistemi, SIS e SIRENE, comporta che molto spesso nei paesi aderenti essi abbiano la medesima sede, normalmente presso gli uffici della direzione di polizia con competenza per la cooperazione internazionale[31].

Il SIS attualmente si applica a 27 Stati compresi paesi non UE quali Svizzera, Norvegia ed Islanda.

Nel corso degli anni si è assistito ad un'evoluzione della natura e delle funzioni del SIS fino ad arrivare a prevedere un sistema di seconda generazione, denominato SIS II, il quale ad oggi non risulta ancora operativo.

Le ragioni che hanno condotto a tali innovazioni sono molteplici: alcune di carattere tecnico ed altre di ragione politica, connesse, in particolare, agli eventi dell'11 settembre 2001.

Il sistema SIS si presentava come un database tecnicamente non complesso, nato per trattare prevalentemente informazioni analogiche; inoltre la sua struttura non ne permetteva un utilizzo con un numero eccessivo di Stati[32].

In secondo luogo dopo l'11 settembre 2001 la natura del SIS è destinata a cambiare e da strumento finalizzato essenzialmente al "*border control*" assume sempre più le sembianze di "*reporting and investigative system*"[33]. Tale processo di progressivo ampliamento di funzioni diverse rispetto a quelle originariamente attribuite è stato definito in dottrina come "*function creep*"[34].

La necessità di rafforzare i sistemi di scambio di informazioni fra Stati e di garantire un ampio accesso ad Europol venne prospettata nel drammatico Consiglio europeo che seguì i fatti dell'11 settembre[35].

Con le due decisioni del Consiglio del 2004 e del 2005[36] si sono introdotte nuove funzione per il SIS nella lotta al terrorismo e si consente ad Europol la possibilità di accesso ai dati contenuti nel sistema SIS ai sensi degli artt. 95, 99 e 100 della Convenzione.

---

[31] Così D. BROEDERS, *The New Digital Borders of Europe- EU Databases and the Surveillance of Irregular Migrants*, in *Int. Sociology*, 2007, 80. In Italia ad esempio la Divisione N.SIS, a carattere interforze, è inserita nell'ambito dell'ufficio Coordinamento e Pianificazione Forze di polizie (d.interm. 555/43 del 1994) che, per il tramite del servizio II, cura i rapporti con l'UE (fonte: www.interno.gov.it.mininterno).

[32] Si riteneva infatti che non potesse funzionare con più di 18 Stati.

[33] Sul punto vd. T. BALZACQ, *The Policy Tools of securitization*, 84 ss.; D. BROEDERS, *The New digital borders*, cit. 81 e A. BALDACCINI, *Counter-terrorism and the EU Strategy for Border Security*, cit. 39.

[34] Secondo D. BIGO, S. CARRERA, B. HAYES, N. HERNANZ, J. JEANDESBOZ (*Justice and Home Affairs Databases* cit., 46) "The notion of function creep can be seen as a virtual line between a lawful and justified data processing system and a sorveillance tool- crossing that line entails going away from the original purpose of the system".

[35] European Council "*Conclusions and Plan of Action of the Extraordinary European Council meeting*" SN 140/01, 21.09.2001, ove si afferma: "*The European Council calls upon the Justice and Home Affairs Council to undertake identification of presumed terrorists in Europe and of organisations supporting them in order to draw up a common list of terrorist organisations. In this connection improved cooperation and exchange of information between all intelligence services of the Union will be required. Joint investigation teams will be set up to that end. 3. Member States will share with Europol, systematically and without delay, all useful data regarding terrorism. A specialist anti-terrorist team will be set up within Europol as soon as possible and will cooperate closely with its US counterparts.*"

[36] Regolamento del Consiglio n. 871/2004 del 29.04.2004 "relativo all'introduzione di alcune nuove funzioni del sistema d'informazione Schengen, compresa la lotta contro il terrorismo" e decisione del Consiglio 2005/211/GAI del 24.02.2005 "relativo all'introduzione di alcune nuove funzioni del Sistema d'informazione Schengen, anche nel quadro della lotta contro il terrorismo".

La questione dell'ampliamento soggettivo dell'accesso ai data-base nello SLSG non assume peraltro un valore puramente descrittivo, bensì sostanziale e collegato all'imporsi di un modello di sicurezza interna "*based on pro-active and intelligence-led policing*"[37].

Nel corso del 2006 e del 2007, pur in assenza di un convincente dibattito pubblico sul punto e senza che si fossero adottati significativi documenti pubblici di valutazione del funzionamento del sistema[38], si arriva all'approvazione del nuovo regolamento e della decisione sull'istituzione del sistema SIS II[39].

La struttura fondamentale del sistema SIS, articolata su un sistema centrale e su sistemi locali non viene ad essere sconvolta, anche se viene precisato che le spese per i sistemi nazionali (NI-SIS II) sono a carico degli Stati membri. Nell'immediato futuro inoltre, nell'ottica di un'interoperabilità tra banche dati, si prevede la condivisione della medesima infrastruttura tecnologica con il sistema VIS[40].

Nella nuova regolamentazione il SIS aumenta le sue funzioni in modo tale da accentuarne la natura di strumento investigativo[41], così come ampliato appare l'ambito oggettivo delle informazioni presenti nei database che includono i dati biometrici quali impronte digitali e fotografie[42].

Lo scopo generale del sistema SIS II viene ora definito in senso più ampio: "assicurare un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione europea, incluso il mantenimento della sicurezza pubblica e dell'ordine pubblico e la salvaguardia della sicurezza nel territorio degli Stati membri e applicare le disposizioni della parte terza, titolo IV, del trattato CE relativo alla circolazione delle persone in detto territorio avvalendosi delle informazioni trasmesse tramite tale sistema" (art. 1, c.2 dec. 533).

Le categorie di segnalazioni che vengono ad essere inserite nel sistema SIS II sono qualificate in modo parzialmente differente rispetto al passato. Esse sono quelle relative a: 1) persone ricercate per l'arresto a fini di consegna o di estradizione (cap. V); 2) persone scomparse (cap. VI); 3)

---

[37] Per a ricostruzione di tale tendenza vd D. BIGO, S. CARRERA, B. HAYES, N. HERNANZ, J. JEANDESBOZ, *Justice and Home Affairs Databases*, in part. pp. 19-20.

[38] In tal senso vd. la ricostruzione di J. PARKIN (*The Schengen Information System and the EU Rule of Law, Inex* Policy Brief No. 13, Giugno 2011, in www.ceps.eu, 3 ss.) che sottolinea come sull'onda della situazione "emergenziale" si rinunciò in ambito europeo ad impostare un dibattito pubblico e trasparente circa le modifiche del sistema SIS maggiormente attento alle implicazioni relative alla tutela dei diritti umani.

[39] Reg. CE n. 1987/2006 del Parlamento europeo e del Consiglio del 20.12. 2006 "sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II)" e la decisione 2007/533/GAI del Consiglio del 12.06 2007 "sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II)".

[40] Per una lettura, non puramente tecnica dell'interoperatività dei due sistemi, vd. M. BESTERS, F.W.A. BROM, *"Greedy" Information Technology: The Digitalization of the European Migration Policy*, in *Eur. J. Migration & Law*, 2010, 462 ss.

[41] Sul punto vd. ad es. la previsione contenuta all'art. 36 par. 2 della Dec. 533 ove si prevede la possibilità di effettuare una segnalazione "ai fini della repressione dei reati e per prevenire minacce alla sicurezza pubblica". Sul punto V. F. CHRISTOU, *Legislative Development: the Council decision of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II),* in *Columbia Journal of European Law*, 2008, 3.

[42] Ancorchè sottoposte alle previsioni di cui all'art. 22 della dec. 533 con riferimento alla necessità del rispetto di certi standard qualitativi.

persone ricercate per presenziare ad un procedimento giudiziario (cap. VII); 4) persone o oggetti ai fini di un controllo discreto o di un controllo specifico (cap. VIII); 5) oggetti ai fini di sequestro o di prova in un procedimento penale (cap. IX).

I dati contenuti nelle segnalazioni verranno trattati nel rispetto di particolare cautele come si desume dal capo XII della dec. n. 533 e dal capo VI del Reg. 1987. In tal senso appare opportuno ricordare come l'effettività del ricorso ai mezzi di tutela previsti (il diritto ad essere informati sui dati contenuti nel database ed il diritto di proporre impugnazione contro una decisione che si ritiene lesiva) risulta una questione altamente problematica[43].

Oltre ai ricordati aspetti di criticità emersi con relazione alla scarsa trasparenza del processo decisionale[44] altri aspetti problematici sono stati segnalati in dottrina con particolare riguardo all'utilizzo di dati biometrici come unico strumento per procedere all'identificazione dei soggetti ed ai suoi possibili esiti erronei[45]. La soluzione di compromesso istituzionale[46] che fu adottata prevede che l'utilizzo dei dati biometrici per identificare cittadini di paesi terzi avvenga dopo che la Commissione presenti una "relazione sulla disponibilità e sullo stato di preparazione della tecnologia necessaria in merito alla quale il Parlamento europeo è consultato"[47].

Oltre alla tutela dei diritti fondamentali delle persone coinvolte alcuni problemi applicativi sono destinati a riproporsi nel nuovo contesto SIS II, con riferimento alle diverse prassi applicative nazionali di registrazione delle persone nel sistema[48].

3. Eurodac

La banca dati Eurodac (acronimo per "*European Dactyloscopie*") venne istituita con il Reg. n. 2725/2000[49] ed è operativa dal 2003 con lo scopo di facilitare l'identificazione dello Stato

---

[43] A tal fine è particolarmente illuminante il c.d. caso Moon. Il signor Moon era il leader coreano della "*Unionist Church*", a lui ed alla moglie venne negata la possibilità di ingresso in Germania per ragioni di pubblica sicurezza. Solo dopo dodici anni dalla presentazione del primo ricorso i giudici tedeschi riconobbero la inesattezza dei dati contenuti nel database SIS. Su tale caso vd. E. BROUWER, *The other side of Moon- The Schengen Information System and Human rights: a task for National Courts*, CEPS Working Document, No. 288, April 2008, in www.ceps.eu, p. 16.

[44] Seconda la dottrina tale aspetto sarebbe in qualche modo collegato all'origine "intergovernativa" del sistema SIS; sul punto vd. M. BESTERS, F.W.A. BROM, "*Greedy" Information Technology*, cit. 464.

[45] Sul punto vd. ad es. A. BALDACCINI, *Counter-terrorism and the EU Strategy for Border Security*, cit. 38 che richiama anche il parere critico del 2006 reso dall'*European Data Protection Supervisor* sul disegno di riforma del SIS II.

[46] Al riguardo infatti vi erano state alcune tensioni con il Parlamento europeo favorevole ad un approccio più flessibile

[47] Così art. 22 lett.c) Reg. n. 1987/2006. Non ci risulta che tale relazione sia al momento disponibile.

[48] Sul punto vd. A. BALDACCINI, *Counter-terrorism and the EU Strategy for Border*, cit. 38-39 che ricorda come "*Some member States, notoriously German and Italy, interpret the criteria for listing unwanted third-country nationals rather widely, with the result that they account for the vast majority of data entered into the System*".

[49] Reg. (CE) n. 2725/2000 del Consiglio dell'11.12.2000 che istituisce l' "Eurodac" per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino. Tale regolamento venne completato dal Reg. (CE) n. 407/2002 del Consiglio del 28 febbraio 2002 che definisce talune modalità di applicazione del regolamento (Ce) n. 2752/2000 che istituisce l' "Eurodac" per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino.

competente per l'esame di una richiesta d'asilo ai sensi del sistema di Dublino[50] e di ridurre la pratica del ricorso al c.d. *asylum shopping*[51].

Attualmente il ruolo di Eurodac appare fortemente connesso con la politica delle espulsioni la cui attuazione è spesso impedita dalla difficoltà di effettuare il riconoscimento della persona da espellere[52].

A differenza della banca dati SIS, o di altre banche dati ove il rilevamento delle impronte digitali è limitato a categorie di persone sospettate di qualche reato, la banca dati Eurodac, per come era stata originariamente concepita, prevede la rilevazione su basi routinaria delle impronte digitali di intere categorie di persone sulla base del fatto oggettivo che abbiano presentato richiesta di asilo in paese aderente alla Convenzione di Dublino[53].

Più in generale Eurodac contiene, oltre alle impronte di individui di età maggiore dei 14 anni richiedenti asilo in uno Stato (categoria 1), altre due categorie di impronte in cui si evidenzia invece un collegamento con l'attività soggettiva posta in essere. Queste sono rappresentate, rispettivamente, dalle impronte di persone fermate in relazione all'attraversamento irregolare di una frontiera esterna (categoria 2)[54] e di quelle di persone illegalmente presenti in uno Stato membro (categoria 3)[55].

Il sistema Eurodac, similmente a quello SIS, si qualifica come un "*hit/no hit system*"; esso contiene, oltre ai dati relativi alle impronte digitali, alcune categorie di informazioni quali lo Stato membro d'origine, il luogo ed il giorno in cui è stata presentata domanda d'asilo, il sesso, la data di rilevamento delle impronte digitali, la data di trasmissione dei dati all'unità centrale, la data di inserimento dei dati nella banca dati centrale[56]. Le autorità abilitate all'accesso, che sono di norma quelle competenti per l'asilo e l'immigrazione, le guardie di frontiera e le autorità di polizia[57], inseriscono le impronte digitali delle persone fermate nella banca dati centrale tramite i punti d'accesso nazionali ed ottengono un riscontro con quelle contenute nel database centrale. Se l'operazione è stata correttamente impostata e non si sono verificati problemi di carattere

---

[50] Sul punto vd. E.R. BROUWER, *Eurodac: Its Limitations and Temptations,* in *Eur. Journ. of Migration and Law*, 2002, 231 che sottolinea come lo scopo di Eurodac sia strettamente definito dall'atto istitutivo.

[51] Cfr. art. 1 Reg. Con l'espressione di *asylum shopping* si fa riferimento alla presentazione successiva di più richieste di asilo in Stati diversi. Sul punto vd. D. BROEDERS, *The New Digital Borders of Europe,* cit. 82.

[52] Se infatti i migranti irregolari che non possono essere riconosciuti sono "*constitutionally rather invulnerabile to expulsion*) (Van der Leun), un "*hit*" nel sistema Eurodac può fornire un *link* con un dossier di richiesta di asilo presentata in un altro paese che può contenere elementi identificativi della persona; sul punto cfr. D. BROEDERS, *The New Digital Borders*, cit. 84. Sul diritto d'asilo in Italia vd. D.U. GALETTA, *Il diritto d'asilo in Italia e nel'Unione europea oggi: fra impegno a sviluppare una politica comune europea, tendenza all'"esternalizzazione" e politiche nazionali di gestione della c.d. "emergenza immigrazione",* in *Riv. It. Dir. Pubbl., Com.,* 2010, 1449 ss.

[53] Per tale osservazione vd. E. R. BROUWER, *Eurodac: Its Limitation,* cit. 231.

[54] I dati di questi soggetti sono registrati nella banca dati centrale all'unico scopo di confrontarli con i dati relativi ai richiedenti asilo trasmessi successivamente alla stessa unità centrale (art. 9 c.1).

[55] I dati di queste persone invece vengono trasmesse alla banca dati centrale esclusivamente al fine del confronto con i dati sulle impronte digitali dei richiedenti asilo trasmessi da altri Stati membri e già registrati nella banca dati centrale (art. 11 c. 3),

[56] Art. 5 Reg. 2725/2000. Non sono contenuti invece dati come il nome e l'indirizzo.

[57] Sul punto si precisa che gli Stati membri debbono comunicare alla Commissione l'elenco delle Autorità che hanno accesso al sistema (art. 15 c.2).

tecnico dovuti, ad esempio, alla cattiva qualità delle impronte rilevate l'operazione si conclude con una "*successful transaction*".

Al riguardo, come si ricava dagli ultimi dati disponibili, riferiti al 2011, l'unità centrale ha ricevuto un totale di 412,303 *successful transactions* con un aumento di più del 30% rispetto all'anno precedente, con particolare riguardo alla categorie dei richiedenti asilo[58].

Già da queste prime note si possono rilevare quali siano i potenziali rischi di violazione dei diritti fondamentali delle persone e dunque, del tutto opportunamente nel c. 1 dell'art. 4 del Reg. Eurodac, si prevede che la procedura nazionale di rilevamento delle impronte -che conserva una certa autonomia procedurale- debba tuttavia rispettare i principi previsti nella Convenzione europea dei diritti dell'uomo e della Convenzione ONU sui diritti dei fanciulli.

Data la particolarità dei dati biometrici contenuti in Eurodac il regolamento istitutivo prevede la necessità di sviluppare particolari metodiche di sicurezza[59], così come di misure volte a tutelare la privacy delle persone.

Il reg. 2725 prevede al riguardo varie previsioni che gravano sullo Stato che procede alla rilevazione delle impronte, sia sotto il profilo della procedura di rilevazione[60] che sotto il versante informativo. Tra queste ultime di particolare rilievo risulta il diritto ad essere informato circa il nominativo del responsabile del trattamento, le finalità per cui i dati saranno trattati e i destinatari dei dati (art.18 c.1). Inoltre vengono garantiti ai soggetti il diritto d'accesso ai dati registrati (art. 18 c.2) e la possibilità di chiederne la modifica o la cancellazione (art. 18 c.3) così come, ove ne ricorrano i presupposti, la possibilità di ottenere un risarcimento dei danni (art. 17).

In aggiunta a ciò importanti previsioni si ritrovano circa la durata di conservazione dei dati.

In particolare le impronte digitali dei richiedenti asilo sono conservate per 10 anni ed esse debbono essere cancellate nel momento in cui lo straniero abbia ottenuto un permesso di soggiorno, o lasci il paese o acquisti la cittadinanza (artt. 6, 7). Mentre i dati di coloro che sono stati fermati mentre attraversavano le frontiere debbono essere conservati per due anni[61].

La supervisione sul sistema viene svolta a livello centrale dall'*European Data protection Supervisor* (EDPS) e, a livello nazionale, dai Garanti nazionali competenti in materia di privacy.

Attualmente, come si desume dalla nona relazione della Commissione[62], prevista ai sensi dell'art. 24 del reg., il sistema Eurodac è al centro di un importante processo di revisione. Da un lato, infatti, la rete infrastrutturale, chiamata ad operare in un ambito di Stati molto maggiore, si è rilevata obsoleta ed è stata potenziata mediante lo sviluppo del sistema EURODAC Plus, e

---

[58] Cfr. *Report from the Commission to the European Parliament and the Council for the activities of the EURODAC system,* Bruxelles 21.09.2012, COM(2012) 533 def., p. 7 cui si rimanda anche per un'analisi dettagliata delle categorie di *Hits*. In particolare hanno contribuito all'innalzamento della percentuale paesi, quali Malta e l'Italia particolarmente interessati dal fenomeno migratorio.

[59] Sotto un profilo tecnologico si registra l'impiego della rete s-TESTA (*secured Trans-European Services for Telematics between administrations*).

[60] Tale procedura deve essere ispirata alla stretta osservanza del principio di legalità ed al rispetto di particolari obblighi di sicurezza nella trasmissione dei dati (artt. 13, 14).

[61] Cfr. art. 10 c. 1.

[62] *Report from the Commission to the European Parliament and the Council for the activities of the EURODAC system*, cit.

dall'altro si registrano proposte di modifica del regolamento 2725, con particolare riferimento all'ampliamento delle categorie dei soggetti abilitati all'accesso per finalità di prevenzione e lotta al terrorismo ed alla criminalità organizzata[63].

A differenza di quanto avvenuto con riferimento al sistema SIS, tali proposte, anch'esse intese come tipica espressione di *function creep* [64], non sono state ancora approvate. La questione appare particolarmente problematica sotto il profilo della tutela dei diritti, andando ad incidere su soggetti particolarmente vulnerabili, quali i richiedenti asilo[65].

4. Visa Information System (VIS)

L'istituzione del sistema d'informazione visti (VIS) risulta una diretta conseguenza degli eventi dell'11 settembre[66]. Esso venne istituito per lo scambio dei dati sui visti rilasciati dai paesi membri a cittadini di paesi (al momento sono più di 130) per i quali viene richiesto il visto[67].

A differenza degli altri data-base analizzati, quale ad esempio SIS, che nei suoi successivi "aggiornamenti" è stato al centro di fenomeni di modifica legislativa dello scopo originario, mediante un aumento significativo delle sue funzioni in nome della *securitization*, la banca dati VIS si presenta come un tipico "*securitizing tool*" a carattere "*multipurpose*"[68].

La disciplina base del VIS che si trova al momento in una fase di prima operatività[69] si ritrova oggi nel Regolamento VIS[70] e nelle sue successive modificazioni ove all'art. 2 gli si attribuisce un

---

[63] In particolare nel 2009 fu avanzata una proposta "*for a Council decision on requesting comparison with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes*", COM(2009) 324 final su cui vd. criticamente M. TZANOU, *The EU as an emerging "Surveillance Society* 424. Più di recente vd. la proposta della Commissione del 30 maggio 2012 "*concerning a recast for a Regulation of the European Parliament and of the Council on the establishment of EURODAC for the comparison of fingerprints for the effective application of Regulation (EU) N (…). And to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) no 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice*" COM(2012) 254 final su cui vd. il giudizio critico espresso dalla *European Data Protection Supervisor* nella sua *Opinion (Recast version)* del 5 settembre 2012, in part. Par. 3.

[64] Sul punto vd. M. BESTERS, F.W.A. BROM, *"Greedy" Information Technology*, cit. 465 e M. TZANOU, *EU as an emerging "Surveilance Society"*, 422 ss.

[65] Sul punto vd. M. TZANOU, *EU as an emerging "Surveilance Society"*, cit. 425.

[66] In tal senso vd. A BALDACCINI, *Counter-terrorism and EU strategy*, cit. che richiama quando deciso nel Consiglio straordinario "Giustizia ed affari interni" del 20 settembre 2001 (DOC 12019/01) e nel successivo Consiglio di Siviglia del giugno 2002. Il sistema venne poi formalmente istituito con la decisione 2004/512/CE del Consiglio del 06.06.2004.

[67] Secondo T. BALZACQ (*The Policy Tools of Securitization*, cit. 88-89) "*the fact that a person needs a visa to enter the EU means that he or she is regarded as a potential threat to the Union*".

[68] Secondo altra dottrina (M. TZANOU, *The Eu as an emerging "Surveillance society"* cit. 416) invece VIS costituirebbe un esempio di *function-creep* perché sarebbe stato creato unicamente in attuazione delle politiche comuni d'asilo non qualificandosi in origine come "*a law enforcement tool*". Nonostante sia indubbio che il sistema sia stato modificato nel corso del tempo si ritiene, in questa sede, anche alla luce della stessa occasione di istituzione, che fin dall'origine ad esso fossero state attribuite funzioni di *counter-terrorism*.

[69] Cfr. Decisione di esecuzione della Commissione del 21.09.2011 che stabilisce la data di inizio delle attività del sistema di informazione visti (VIS) in una prima regione; Decisione di esecuzione della Commissione del 27.04.2012 che stabilisce la data di inizio delle attività del sistema di informazione visti (VIS) in una seconda regione e Decisione di esecuzione della Commissione del 21 settembre 2012 che stabilisce la data di inizio delle attività del sistema di informazione visti (VIS) in una terza regione.

margine d'azione molto ampio. Esso infatti ha lo scopo di "migliorare l'attuazione della politica comune in materia di visti, la cooperazione consolare e la consultazione tra autorità centrali competenti per i visti, agevolando lo scambio di dati tra Stati membri in ordine alle domande di visto e alle relative decisioni".

Le finalità di tale attività sono molteplici e vanno da quella amministrativa di agevolare la procedura relativa alla domanda di visto, a quella di evitare frodi o elusioni dei criteri fissati per la domanda, all'agevolazione dei controlli alle frontiere esterne, alla prevenzione delle minacce di sicurezza interna degli Stati membri (art. 2). Particolare interessante appare la previsione relativa alla identificazione o, più correttamente alla ri-identificazione, delle persone entrate legalmente in uno Stato membro con un visto temporaneo, successivamente scaduto[71].

Sotto un profilo organizzativo il sistema VIS è simile al SIS II, esso si compone di un "Central Visa information system" che ha sede nello stesso luogo fisico ove trova collocazione il Sistema centrale SIS II e cioè a Strasburgo con cui si interfacciano le sezioni nazionali ("The National Interfaces") presso ciascun Stato aderente.

Il sistema VIS condividerà, come si è ricordato, la stessa infrastruttura tecnologica con SIS II e non è un caso dunque se la sede fisica del sistema centrale risulta la medesima.

Possono accedere ai dati, che possono essere anche biometrici, le autorità competenti in materia di politiche dei visti. A seguito dell'adozione della decisione 2008/633/GAI anche le autorità di polizia nazionali appositamente identificate dallo Stato possono accedere ai dati contenuti in VIS, purchè esistano fondati motivi per ritenere che la consultazione del VIS contribuisca in maniera sostanziale alla prevenzione, all'individuazione o all'investigazione di reati di terrorismo o di altri gravi reati, così come l'accesso è consentito all'Europol, seppure non in modo indiscriminato[72]. In dottrina tale apertura alle autorità di polizia ed in particolare ad Europol è stata contestata[73] venendo ritenuta estranea agli scopi originali di istituzione del data-base, ma costituendo una sproporzionata intrusione nella privacy dei viaggiatori in modo non conforme al "*purpose limitation principle*"[74].

5. Qualche prima conclusione

Da quanto sopra esposto risulta confermato il fatto che l'eliminazione delle barriere fisiche tra gli Stati ha determinato la creazione di un imponente apparato di barriere tecnologiche, basate su

---

[70] Reg. n. 767/2008 del Parlamento e del Consiglio del 9 luglio 2008 concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata.

[71] Sul punto vd. D. BROEDERS, *The New Digital Borders of Europe,* cit. 85.

[72] Essa può infatti accedere "entro i limiti delle sue competenze e laddove ciò sia necessario per l'adempimento delle sue funzioni" (art. 3. c.1 Reg. VIS). Sul punto, per l'esame delle condizioni di accesso di tali soggetti alla luce della decisione del Consiglio su VIS vd. M. TZANOU, *EU as an emerging "Sorveillance Society",* cit. 418 ss.

[73] A. BALDACCINI, *Counter-Terrorism and the EU Strategy for Border Security,* cit. p. 41 ove si ribadisce che "*VIS is an information system developed in view of implementation of the European visa policy. It si not a law enforcement tool*", p. 41.

[74] Per un'analisi sotto tale profilo vd. M. TZANOU, *EU as an emerging "Sorveillance Society",* cit. 420-421. Secondo tale principio risulta necessario che vi sia uno stretto nesso tra lo scopo della raccolta dei dati e l'uso che ne viene fatto.

"*large Europe-wide database*". La necessità dell'utilizzo dell'IT risulta del resto un tratto tipico di ogni moderna amministrazione ove l'informazione automatizzata assume un crescente rilievo anche in funzione di assicurare un'attività amministrativa più efficiente[75].

La specificità delle politiche dell'immigrazione e dei visti, connesse alla necessità di procedere all' "identificazione" dei soggetti, laddove essi siano privi di documenti identificativi o non collaborino, fa sì che tali banche dati spesso contengano informazioni a carattere biometrico "fornite" dal corpo umano[76]. In alcuni casi questo dato si estremizza, come ad esempio nella banca dati Eurodac, contenente informazioni biometriche "*on a politically sensitive group of persones, namely asylum seekers and refugees*"[77]. Inoltre il *decision-making* di tipo automatizzato, che sta alla base del funzionamento di tali data-base si esplica prevalentemente in attività di *profiling* o *predictive data-mining*[78] che presentano il forte rischio di determinare conseguenze discriminatorie, ed al riguardo viene richiamata in dottrina la nuova categoria della "discriminazione statistica"[79].

La particolarità del processo di integrazione europea rende poi necessario un collegamento dei database nazionali con quello centrale, mediante sistemi infrastrutturali di larga scala.

L'implementazione di tali *European information networks* richiede la messa in campo di onerose e complesse misure di sicurezza, che da un lato necessitano di importanti investimenti e dall'altro mostrano comunque qualche elemento di debolezza come si ricava dal fatto che, ad oggi, il sistema SIS II non sia ancora operativo mentre il sistema VIS risulta ancora in una fase di prima operatività.

Un ulteriore aspetto di criticità si evidenzia a livello di applicazioni nazionali, ove si ravvisano difformità applicative tra Stati che determinano un quadro di notevole frammentazione[80].

La dottrina soprattutto politologica, osservando il fenomeno di tali moltiplicazione di banche dati di larga scala ha evocato lo spettro della "*surveillance society*" [81] . Così espressioni come "*cyber*

---

[75] Sul punto, per la lettura del fenomeno sotto il profilo dell'attività regolatoria, vd. L. AMMANNATI, *Regulation Information and New Information Technology - Do "wiki-based instruments" play an influent role in regulatory procedures at the global level?* in www.astrid-online.it

[76] Con tutti i problemi che da questo derivano laddove, si pensi al caso dei minori, ove si preveda di definire l'età mediante scansione ossea; sul punto per la problematicità di tali metodiche, suscettibile di incidere anche sul diritto della salute, cfr. H. DIJSTELBLOEM, *Europe's New Technological Gatekeepers"*, cit. 13.

[77] In tal senso si esprime E.R. BROUWER, *Eurodac: Its Limitation*, 246.

[78] D. BIGO, S. CARRERA, B. HAYES, N. HERNANZ, J. JEANDESBOZ, *Justice and Home Affairs Databases,* cit. "*Profiling is used to "select" a group of people as a potential risk or a threat and may lead to discriminatory ethnic profiling, which is by nature difficult to reconcile with the obbligation for national and EU law enforcement authorities and agencies not to discriminate on grounds of a sensitive nature such as national or ethnic origin*" (p.39).

[79] Tale sarebbe da intendersi una "*decision to exclude or deny opportunity to an individual on the basis of the attributes of the group to which he or she is assumed to belong…as a result, what would otherwise be treated as illegal racial discrimination is routinely justified as a legitimate and inherently rational act*" (O.H. GANDY, *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage,* Ashgate, 2009, pp. 69-72 richiamato in D. BIGO, S. CARRERA, B. HAYES, N. HERNANZ, J. JEANDESBOZ, *Justice and Home Affairs Databases,* cit. 51-52).

[80] Si pensi ad esempio ai ritardi di comunicazioni da parte dei sistemi nazionali dei dati all'unità centrale nell'ambito del sistema Eurodac. Sul punto vd. J. MONAR, *Cooperation in the Justice,* cit. 507 che afferma come "*the central analysis capacity remains dependent on an uneven supply from the national system and is partially weakened by institutional proliferation and fragmentation*".

Fortresse"[82], "*panopticon Europe*"[83] ed altre simili trovano frequentemente impiego, soprattutto a livello descrittivo, per richiamare i rischi collegati allo sviluppo tecnologico.

Secondo un'altra teoria, prospettata di recente, la tecnologia applicata alla gestione dell'immigrazione non risulterebbe mai neutrale rispetto agli obiettivi politici, ma sarebbe caratterizzata da una "*capability to (re)-shape its predefined goal*" ed in tal senso si è parlato di "*greedy information tecnology*"[84].

Al di là di tali pur suggestive letture, di maggiore interesse sotto un profilo giuridico appare la lettura del fenomeno alla luce della teoria della *function creep*, termine con il quale si intende "*a gradual widening of the use of a system or database beyond the purpose for which it was originally intended*"[85]. Questo trova d'altro canto un parallelo, in termini più generali, in quel processo di ibridazioni delle *policies* che risulta connaturato al processo di *securitization* indotto dai fatti dell'11 settembre.

Quello che non si può ancora determinare con certezza è se tale tendenza all'utilizzo di banche dati di larga scala a carattere "*multipurpose*", talora tecnicamente interoperabili sia da leggersi come un fenomeno di tipo emergenziale, occasionato dalle vicende drammatiche dell'11 settembre e delle successive stragi di Londra o Madrid o se questi fatti abbiano determinato un irreversibile "giro di boa della storia"[86] tale da plasmare in modo irreversibile le politiche in materia di immigrazione.

Su questo ovviamente oggi non ci possiamo esprimere in modo definitivo, anche in ragione del fatto che l'operatività di tali banche dati è ancora agli inizi. Quella che però appare una sensazione condivisa, supportata anche da un autorevole recente studio[87], è che il fenomeno dell'impiego di

---

[81]Sul punto vd. M. TZANOU, *The EU as an emerging "Surveillance Society"*, cit. 409 ss. ed ivi ampia bibliografia.

[82] E. GUILD, S. CARRERA, A. EGGENSCHWILER, *Informing the Borders Debate*, CEPS Special Reports, 2009, in www.ceps.eu.

[83] Cfr. G. ENGBERSEN, *The Unanticipated Conseguences of Panopticon Europe. Residence Strategies of Illegal Immigrants*, in V. GUIRAUDON, C. JOPPKE (eds), *Controlling a New Migration World*, London, 2001, 242.

[84] Sul punto vd. Il già citato saggio di M. BESTERS, F. W.A. BROM, *Greedy Information Tecnology*, cit. 455 ss. Secondo tale autori la "*greediness*" "*indicates the distorting potential of information technology regarding the means-end logic*". Un esempio emblematico si ritroverebbe nella nozione di interoperatività che lungi dal rivestire un significato meramente tecnico, implica una precisa opzione politica circa il futuro assetto delle banche dati nello spazio di libertà, sicurezza e giustizia. Su tale punto vd. anche B. HAYES, *NeoConOpticon. The EU Security-Industrial Complex*, 70 ss. in www.statewatch.org.

[85] *Opinion of European Data protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU)* (Recast version), 5 September 2012, p. 10, in http://www.edps.europa.eu cit. pag. 7.

[86] Per tale espressione vd. C. Magris *(Il giro di boa della storia*, in *Corriere della sera*, 11 settembre 2011*)* che così scrive*:* "Dopo l'11 Settembre il mondo traballa ancor più di prima e traballa pure la logica che lo ha regolato; si alterano equilibri politici, si confondono i rapporti di forza, vacillano le gerarchie – giuste o inique – che dominano la nostra esistenza, diventano più incerti o scompaiono i progetti del futuro, del futuro di tutti noi. In questo senso l'11 Settembre è un giro di boa della storia, dopo il quale sappiamo ancor meno di prima cosa ci attende. Chi, morto o sopravvissuto, ha patito direttamente, sulla sua pelle, quell'11 Settembre è stato anche la cavia di un orribile esperimento di un nuovo ordine ossia disordine del mondo".

[87] Sul punto vd. D. BIGO, S. CARRERA, B. HAYES, N. HERNANZ, J. JEANDESBOZ, *Justice and Home Affairs Databases* cit. ove si afferma che "*there is non reversibility in the growing reliance on data and information exchange schemes for the conduct of the European Union's Justice and Home Affairs (JHA) policies*"(p.4).

banche dati su larga scala per finalità *anche* di controllo antiterroristico costituisca, al momento, un tratto ineludibile delle politiche europee in materia.

L'accettazione di tale presupposto implica la ricerca di un difficile bilanciamento tra le esigenze della sicurezza e quelle della protezione dei diritti delle persone, sia sotto il profilo della tutela della privacy e della vita privata, che con riferimento al divieto di discriminazioni[88].

Del tutto condivisibile appare poi la critica, espressa da più parti circa le carenze informative e l'assenza di controllo pubblico sulle *technicalities* impiegate nella gestione delle frontiere e dell'immigrazioni[89]. Da un lato, infatti, sono mancati per lungo tempo documenti pubblici relativamente ai sistemi di scambio di informazione e da questo punto di vista è significativo il fatto che solo nel 2010 sia stato pubblicata la Comunicazione della Commissione sulla gestione delle informazioni che si pone esplicitamente "*as a contribution to an informed policy dialogue with all stakeholders*"[90]. Dall'altro lato quasi assente risulterebbe il controllo democratico sull'implementazione delle tecnologie nel settore dell'immigrazione per il semplice motivo che esse si applicano di *default* a soggetti "non" cittadini, come tali esclusi dai processi di partecipazione democratica[91].

Di conseguenza l'ambito della gestione delle informazioni nel settore, non potendo contare sui tradizionali strumenti di *feed-back* o *learning by mistakes* usualmente impiegati nell'ambito dell'implementazione di politiche pubbliche nei settori a forte automatizzazione (quale ad esempio quello fiscale), sembra divenire una sorta di laboratorio ove testare, forse senza eccessive preoccupazioni circa la tutela dei soggetti coinvolti, strumenti potenzialmente molto invasivi nella sfera personale[92].

Tutto questo determina sovente una situazione non solo di "*doubtful technical legitimacy*", ma anche di "*questionable political legitimacy*"[93].

In conclusione, se il processo di affermazione di data-base sempre più complessi e potenti si inserisce in un *trend* crescente nel panorama delle gestioni delle informazioni nello spazio di libertà, sicurezza e giustizia con particolare interesse vanno osservate alcune prime previsioni di strumenti di controllo "esterno" sugli stessi che si aggiungono a quelli già esistenti. In tale ottica può essere letta la recente istituzione dell'Agenzia europea per la gestione operativa dei sistemi IT su larga scala[94].

---

[88] Sul punto vd. C. RIJKEN, *Re-balancing Security and Justice: Protection of Fundamental Rights in Police and Judicial Cooperation in Criminal matters,* in *CMLR,* 2010, 1455 ss.

[89] H. DIJSTELBLOEM, *Europe's New Tecnologicla Gatekeepers,* 2009 ss.

[90] Sul punto D. BIGO, S. CARRERA, B. HAYES, N. HERNANZ, J. JEANDESBOZ, *Justice and Home Affairs Databases,* cit. 10 ss.

[91] Così H. DIJSTELBLOEM, *Europe's New Technological Gatekeepers,* cit. (17).

[92] La ricostruzione è quella seguita da H. DIJSTEBOLEM, *Europe's New Technological Gatekeepers,* cit. 15 ss.

[93] Così H. DIJSTELBLOEM, *Europe's New Technological Gatekeepers,* 17.

[94] Tale Agenzia è istituita dal Reg. UE n. 1077/2011 del Parlamento europeo e del Consiglio del 25 ottobre 2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia.

Tale Autorità, oltre a vigilare sulla gestione operativa, a carattere prevalentemente tecnico[95], delle banche dati SISII, Eurodac e VIS, ha l'espresso compito di "garantire un elevato livello di protezione dei dati, conformemente alle norme applicabili". Inoltre, per colmare quelle carenze informative riscontrate con riferimento agli sviluppi tecnologici delle banche dati (non sempre ritenuti "politicamente neutri"[96]), essa ha il compito di "riferire periodicamente al Parlamento europeo, al Consiglio, alla Commissione e, per le questioni relative alla protezione dei dati, al Garante europeo di protezione dei dati" gli sviluppi della ricerca per la gestione operativa del SISII, del VIS, Di Eurodac e di altri sistemi IT di larga scala (art. 8 c.2).

[95] Ai sensi dell'art. 2 gli obiettivi dell'Agenzia sono quelli di garantire un esercizio efficace, sicuro e continuo dei sistemi di larga scala, di garantirne una gestione efficiente e "finanziariamente responsabile", di garantire un servizio di qualità adeguatamente elevata, una continuità ed un livello adeguato di sicurezza.

[96] Seguendo la teoria della "*greediness*" richiamata in precedenza.

Bibliografia di riferimento

L. AMMANNATI, "Regulation Information and New Information Technology - Do "wiki-based instruments" play an influent role in regulatory procedures at the global level?" in www.astrid-online.it.

A. F. ATGER, *The abolition of International Border Checks in an Enlarged Schengen Area: Freedom of movement or a scattered web of security checks?,* CEPS Challenge Paper, No. 8, 2008 in www.ceps.eu.

A. BALDACCINI, "Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases", in *Eur. J. Migration & L.*, 2008, 31 ss.

T. BALZACQ, "The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies", in *JCMS* 46/2008, 75 ss.

M. BESTERS, F.W.A. BROM, ""Greedy" Information Technology: The Digitalization of the European Migration Policy", in *Eur. J. Migration & Law,* 12/2010, 455 ss.

D. BIGO, S. CARRERA, B. HAYES, N. HERNANZ, J. JEANDESBOZ, *Justice and Home Affairs Databases and a Smart Borders System at EU External Borders - An evaluation of Current and Forthcoming proposals,* CEPS Paper in *Liberty and Security in Europe* No. 52, Dicembre 2012, in www.ceps.eu.

P. BILANCIA, "Lo spazio di libertà, sicurezza e giustizia tra realtà intergovernativa e prospettiva comunitaria", in P. BILANCIA, F.G. PIZZETTI (a cura di), *Aspetti e problemi del costituzionalismo multilivello,* Milano, 2004, 345 ss.

P. BILANCIA, *The dynamics of the EU Integration and the impact on the National Constitutional Law - The European Union after the Lisbon Treaties,* Milano, 2012.

D. BROEDERS, "The New Digital Borders of Europe- EU Databases and the Surveillance of Irregular Migrants", in *Int. Sociology,* 2007, 71 ss.

E.R. BROUWER, "Eurodac: Its Limitations and Temptations", in *Eur. J. Migration & Law*, 2002, 231 ss.

A. CANEPA, "The regulatory role of FRONTEX: risk analysis, border management and Exchange of data", in L. AMMANNATI (ed.), *NETWORKS - In search of a Model for European and Global Regulation,* Torino, 2012, 127 ss.

M. CONDINANZI, A. LANG, B. NASCIMBENE (edts.), *Citizenship of the Union and Freedom of Movement of Persons,* Leiden-Boston, 2008;

V. F. CHRISTOU, "Legislative Development: the Council decision of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)", in *Columbia Journal of European Law,* 2008, 3 ss.

H. DIJSTELBLOEM, "Europe's New Technological Gatekeepers. Debating the Deployment of Technology in Migration Policy", in *Amsterdam L.F.* 11/2008-2009, 11 ss.

T. FREIXES, "Protección de datos y globalización. La Convención de Prüm", in *Revista de derecho constitucional europeo,* 2007, 11 ss.

D.U. GALETTA, "Il diritto d'asilo in Italia e nel'Unione europea oggi: fra impegno a sviluppare una politica comune europea, tendenza all'"esternalizzazione" e politiche nazionali di gestione della c.d. "emergenza immigrazione"", in *Riv. It. Dir. Pubbl., Com.,* 2010, 1449 ss.

G. GONZÁLEZ FUSTER, P. DE HERT, E. ELLYNE, S. GUTWIRTH, *Huber, Marper and Others: Throwing new light on the shadows of suspicion,* CEPS INEX Policy Brief, No. 11/2010, in www.ceps.eu.

G. GONZÁLEZ FUSTER, P. DE HERT, S. GUTWIRTH, *Privacy and Data Protection in the EU Security Continuum*, CEPS INEX Policy Brief, No. 12/2011, in www.ceps.eu.

A. LANG, "Giustizia ed affari interni", in M.P. CHITI, G. GRECO (a cura di), *Trattato di diritto amministrativo europeo,* Torino, 2007, 1143 ss.

G. MARCHETTI, *I recenti passi avanti compiuti dall'Unione europea nella direzione di un'armonizzazione dei sistemi penali,* CSF Research Paper, Novembre 2012, in www.csfederalismo.it.

V. MITSILEGAS, "Immigration Control in an Era of Globalization: Deflecting Foreigners, Weakening Citizens, Strengthening the State", in *Indian Journal of Global Legal Studies,* 19/2012, 3 ss.

J. MONAR, "Cooperation in the Justice and Home Affairs Domain: Characteristics, Constraints and Progress", in *Journal of European Integration* 5/2006, 495 ss.

B. NASCIMBENE, M. PASTORE (a cura di), *Da Schengen a Maastricht,* Milano, 1995.

B. NASCIMBENE, "Recent trends in European Migration and Asylum Policies" in G. VENTURINI, S.BARIATTI (a cura di), *Diritti individuali e giustizia internazionale,* Milano, 2009, 597 ss.

J. PARKIN, *The Schengen Information System and the EU Rule of Law,* CEPS INEX Policy Brief No. 13, Giugno 2011, in www.ceps.eu.

G. PINYOL JIMÉNEZ, "The Migration-Security Nexus in Short: Instruments and actions in the European Union", in *Amsterdam L.F.,* 2012, 36 ss.

M. PEDRAZZI, I. VIARENGO, A. LANG (edts.), *Individual guarantees in the European judicial area in criminal matters,* Bruxelles, 2011.

D. RINALDI, "L'assetto dello spazio di libertà, sicurezza e giustizia" dopo il Trattato di Lisbona: elementi di continuità e discontinuità", in N. PARISI, V. PETRALIA (a cura di), *L'Unione europea dopo il Trattato di Lisbona,* Torino, 2011, 333 ss.

F. SCUTO, *I diritti fondamentali della persona quale limite al contrasto dell'immigrazione irregolare,* Milano, 2012.

M. TZANOU, "The EU as an emerging "Surveillance Society": The function creep case study and challenges to privacy and data protection" in *Vienna Online J. on Int'l Const. L.,* 2010, 407 ss.

CENTRO STUDI SUL FEDERALISMO

Via Real Collegio 30
10024 Moncalieri (TO)
Tel. +39 011 670 5024
Fax. +39 011 670 5081
www.csfederalismo.it
info@csfederalismo.it