Centro di
Documentazione europea - UniCT

Università di Catania

I quaderni europei

Scienze giuridiche

DIRITTO ALLA *PRIVACY*
E TRATTAMENTO AUTOMATIZZATO DEI DATI
FRA DIRITTO CIVILE, DIRITTO PENALE
E DIRITTO INTERNAZIONALE ED EUROPEO

Francesco Priolo
Vincenzo Di Cataldo
Roberto Lattanzi
Valeria Scalia
Nicoletta Parisi
Giuseppe Versaci
Elisa Gulizzi
Giovanni Antonino Cannetti

Aprile 2014
n. 63

Università di Catania - *Online Working Paper* 2014/n. 63

URL: http://www.cde.unict.it/quadernieuropei/giuridiche/63_2014.pdf

Università degli Studi di Catania in collaborazione con il Centro di documentazione europea - *Online Working Paper*/ISSN 1973-7696
Periodico mensile registrato al Tribunale di Catania il 22 ottobre 2013 con il numero 15

Francesco Priolo, Professore ordinario di fisica della materia nell'Università degli Studi di Catania, Dipartimento di fisica e astronomia; Presidente della Scuola Superiore di Catania

Vincenzo di Cataldo, Professore ordinario di Diritto commerciale nell'Università degli Studi di Catania, Dipartimento di Giurisprudenza

Roberto Lattanzi, Dottore di ricerca in Diritto civile nell'Università S.C. Cattolica di Milano. Dirigente del servizio "Studi e documentazione" del Garante per la protezione dei dati personali

Valeria Scalia, Ricercatrice di diritto penale nell'Università degli Studi di Catania, Dipartimento di Giurisprudenza

Nicoletta Parisi, Professore ordinario di Diritto internazionale nell'Università degli Studi di Catania, Dipartimento di Giurisprudenza; Responsabile scientifico del Centro di documentazione europea dell'Università degli Studi di Catania

Giuseppe Versaci, allievo della Scuola Superiore di Catania, studente IV anno del Dipartimento di Giurisprudenza presso l'Università degli Studi di Catania

Elisa Gulizzi, allieva della Scuola Superiore di Catania, studente V anno del Dipartimento di Giurisprudenza presso l'Università degli Studi di Catania

Giovanni Antonio Cannetti, allievo della Scuola Superiore di Catania, studente IV anno del Dipartimento di Giurisprudenza presso l'Università degli Studi di Catania

Il periodico *online* "*I quaderni europei*" raccoglie per sezioni (scienze giuridiche, scienza della politica e relazioni internazionali, economia, scienze linguistico-letterarie, energia, serie speciale per singoli eventi) i contributi scientifici di iniziative sulle tematiche dell'integrazione europea dalle più diverse prospettive, avviate da studiosi dell'Ateneo catanese o da studiosi di altre Università italiane e straniere ospiti nello stesso Ateneo
I *papers* sono reperibili unicamente in formato elettronico e possono essere scaricati in formato pdf su: http://www.cde.unict.it/quadernieuropei

Edito dall'Università degli Studi di Catania in collaborazione con il Centro di documentazione europea d'Ateneo.
Via Umberto, 285 B - 95129 – CATANIA
tel. ++39.095.8737802 - 3
fax ++39.095.8737856
www.cde.unict.it

Diritto alla *privacy* e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo

Francesco Priolo – Vincenzo Di Cataldo – Roberto Lattanzi – Valeria Scalia – Nicoletta Parisi – Giuseppe Versaci – Elisa Gulizzi – Giovanni Antonino Cannetti

I. Abstract

Il contributo delinea il percorso storico-normativo del processo di affermazione del diritto alla protezione dei dati personali, che si affianca al "tradizionale" diritto alla tutela della vita privata sancito dalla Carta dei diritti fondamentali dell'Unione europea e dalla Convenzione europea dei diritti dell'uomo. In una prospettiva storico-evolutiva, l'Autore riflette sulle cause e le ragioni che determinarono agli inizi degli anni Sessanta, prima negli Stati Uniti e quindi in Europa, l'avvio del processo di concretizzazione e autonomizzazione del diritto alla tutela dei dati personali. Egli individua, altresì, le basi giuridiche e normative di una traiettoria multisfaccettata, che partendo dalle linee guida OCSE e dalla Convenzione di Strasburgo, arrivando infine al Trattato di Lisbona, è a tutt'oggi in pieno movimento e appare tutt'altro che esaurita.

The work drafts the historical – legislative route of the process which determined the establishment of the right to the protection of personal data. This right is placed side by side with the "traditional" right to private life ratified by the Charter of fundamental rights of the European Union and the European. Convention on Human. Rights. The Author reflects, from an historical - evolutionary perspective, on the causes and the reasons which caused at the beginning of sixties, first in the USA and then in Europe, the start of the process of concretization and autonomization of the right to the protection of personal data. Moreover He identifies the legal and normative basis of a multifaceted trajectory which starting from the OECD guidelines and the Strasbourg Convention and arriving to Lisbon Treaty, is still in movement and appears anything but concluded.

II. Abstract

Il presente lavoro si propone di analizzare gli sforzi compiuti dal legislatore europeo e da quello nazionale in ordine all'individuazione del corretto bilanciamento tra le esigenze di sicurezza e difesa sociale, derivanti dalla non trascurabile possibilità che la massiccia diffusione delle nuove tecnologie informatiche e telematiche dia luogo a nuovi comportamenti criminosi ovvero semplifichi la commissione di questi ultimi, e la necessità di tutelare la riservatezza dei dati immessi dagli utenti in rete, evitando al contempo di limitare incondizionatamente la possibilità di questi ultimi di realizzare la propria personalità nell'ambito dello spazio informatico e telematico, avendo particolare riguardo alla recente Direttiva 2013/40/UE, relativa agli attacchi ai sistemi d'informazione, ed al suo impatto sul quadro normativo italiano.

This article aims at analysing the efforts made by both the European legislator and the Italian one, in order to achieve a fair balance between the need of security - deriving from the concrete possibility that the massive use of the new digital technologies enhances new criminal behaviors or makes them easier to realize – and the necessary protection of data put on Internet by the users, trying at the same time to prevent an absolute limitation of the realization of their personality within the cyberspace. It examines, in particular, the recent Directive 2013/40/EU, concerning the attacks against the information systems, and its impact on the Italian criminal legislation.

III. Abstract

Nello spazio penale europeo si pone la difficile questione di coniugare libertà, sicurezza e giustizia. A tal fine i Trattati di Unione nella revisione di Lisbona hanno valorizzato il quadro di garanzie (istituzionali, sostanziali e processuali) nel rispetto delle quali deve essere organizzata la cooperazione fra tutte le autorità (nazionali ed europee) incaricate di presiedere all'applicazione della legge.
Il contributo si propone di valutare l'estensione di siffatto obbligo di cooperazione alla luce del principio di disponibilità delle informazioni, considerando le opportunità al proposito offerte dagli strumenti tecnologici. In particolare si intende valutare quali problemi possano determinarsi dall'utilizzo delle banche-dati informatizzate ai fini di conseguire la sicurezza interna agli Stati membri e all'Unione in relazione al rispetto dei diritti fondamentali e quali soluzioni giuridiche l'ordinamento dell'Unione sia in procinto di adottare, nell'ambito di una complessiva riforma del sistema di protezione dei dati personali avviata a partire dall'art. 16 TFUE.

Inside the European criminal area it is necessary to joint freedom, security and justice.
After the Lisbon revision, The European Union Treaties improved the legal framework guaranteeing the respect of human rights of persons involved in criminal proceedings. The topic is really relevant when mutual cooperation among police, jurisdictional, intelligence and custom authorities is at stake.
The paper intends to verify the latitude of the mentioned duty to cooperate stated in the European legal order, putting it in relation with the principle of international data availability and the modern technological devices. In particular, the study aims to identify which criticalities arise from the widespread use of data information systems, the principle of mutual cooperation among different authorities implied in the law application, and the respect of human rights to a fair trial, personal data protection, privacy, and so on.
The paper will verify these topics in the light of European case law and the proposed reform of data protection in the European legal order.

IV. Abstract

Il presente lavoro si propone di esaminare la sentenza della Corte di Cassazione n. 5525/2012 e, in particolar modo, le conclusioni, senza dubbio di una certa rilevanza, in tema di diritto all'oblio: diritto riconosciuto per la prima volta dalla stessa Corte nella sentenza n. 3679/1998. Nella sentenza oggetto di commento la Corte sancisce la massima secondo la quale il titolare dell'organo di informazione è tenuto a garantire la contestualizzazione e l'aggiornamento della notizie, a tutela del diritto del soggetto, cui i dati pertengono, alla propria identità personale o morale nella sua proiezione sociale. L'Autore compara le suddette conclusioni con quelle, parzialmente diverse, cui è giunto l'Avvocato generale Jääskinen in ordine a un rinvio pregiudiziale riguardante, da una parte, la qualificazione dei fornitori di servizi di motore di ricerca e, dall'altra, la possibilità di riconoscere un diritto all'oblio. Infine, si dà spazio ad alcuni spunti di riflessioni sul difficile rapporto tra memoria e oblio nella società dell'informazione.

The work aims at examining the judgment of the Court of Cassation n. 5525/2012 and, in particular, the relevant conclusions regarding the right to be forgotten: this right was recognized for the first time by the Court in the judgment n. 3679/1998. In the judgment under review, the Court establishes the principle according to which the media organization holder has to guarantee the contextualization and the update of the news in order to protect the right of the "data subject" and its personal and moral identity in social projection. The Author compares the above mentioned conclusions with the opinions, partially different, of the Advocate general Jääskinen about, on the one hand, the qualification of internet service providers and, on the other hand, the possibility to recognize a right to be forgotten. Finally, the Author suggests some reflections on the difficult relationship between memory and oblivion in the information society.

V. Abstract

La vicenda *Google vs Vividown* è considerata un *unicum* nel panorama internazionale ed ha suscitato, sin dalle prime fasi dell'*iter* processuale, clamore mediatico e riflessioni dottrinali. Il tentativo del giudice monocratico di attribuire il ruolo di guardiano del *web* all'*internet service provider*, si è rivelato carente di un sostegno tecnico-giuridico. Pertanto la sentenza d'Appello, di recente confermata dalla Suprema Corte di Cassazione, ha riformato parzialmente la pronuncia di primo grado, escludendo l'obbligo dell'ISP di rendere edotto l'utente circa l'esistenza della normativa sulla *privacy*. Si sono negati altresì la configurabilità del concorso omissivo nel reato di diffamazione e la sussistenza del dolo specifico richiesto dalla norma incriminatrice. La peculiarità del caso in esame, messa in risalto dal confronto con altri casi giurisprudenziali, è quella di aver posto il problema del ruolo da attribuire all'ISP, in una ricerca che non può trascurare il bilanciamento di valori primari.

The *Google vs Vividown* case is accounted as an *unicum* in the international legal scene and upfront it was at the core of media's attention as well as the doctrinal thought. The single presiding judge's attempt to ascribe the role of web warden to the internet service provider was legally unfounded. Therefore, the Appeal judgement, recently confirmed by the Supreme Court, has partially reformed the inferior court's sentence, ruling out the ISP's duty of noticing the uploader about the personal data protection legislation. Moreover it was stated the unmountability of both omissive complicity in defamation and malice. The distinguishing feature of this case, highlighted by comparison with other controversies, is the emerging need to address the problem of characterizing the ISP's role, trying not to overlook primary values.

VI. Abstract

Il presente elaborato intende offrire una panoramica sintetica della disciplina del trattamento dei *Personal Name Record* (PNR), intesi come dati personali informatizzati rilasciati dai consumatori ai fini dell'emissione di un titolo di viaggio aereo, oggetto di accordi bilaterali tra l'Unione europea e diversi altri Stati extraeuropei; in particolare, ci si è soffermati sull'evoluzione degli accordi USA-UE a partire dai tragici eventi dell' 11 settembre 2001 fino alla pronuncia della Corte di giustizia del 30 maggio 2006, relativa all'annullamento della decisione di *adeguacy finding* della Commissione europea sulla tutela offerta ai dati personali dalle autorità statunitensi e la decisione 2004/496/CE del Consiglio europeo. Vengono poi brevemente esposti gli ulteriori successivi sviluppi della disciplina ed analizzati sommariamente i tratti salienti degli accordi europei intercorrenti con Australia e Canada in una prospettiva comparativa.

The present study intends to offer a brief overview about the processing of personal name record (PNR) discipline, defined as a computerized personal data provided by consumers for the issuance of a ticket air travel, which has become the object of bilateral agreements between European Union and several other non-European countries; in particular, we focused on the evolution of the US-EU agreements since the tragic events of September 11th, 2001 until the judgment of the Court of Justice of 30 May 2006 concerning the annulment of the European Commission's Adequacy finding decision on the protection afforded to personal data by the U.S. authorities and the European Council's Decision 2004/496/EC. At the end, further subsequent developments are briefly exposed and the salient features of the European agreements entered into with Australia and Canada are analyzed, summarily, in a comparative perspective.

Keywords

I. Diritto alla protezione dei dati di carattere personale – processo di costituzionalizzazione - *OECD guidelines on the protection of privacy and transborder flows of personal data* – Convenzione europea di Strasburgo

n. 108/1981- *Recht auf informationelle Selbstbestimmung* - *Recht auf Datenschutz* - direttiva 95/46/CE - decisione quadro 2008/977/GAI - direttiva 2006/24/CE

Right to the protection of personal data - constituzionalization process - OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - Strasbourg Convention n. 108/81 - Recht auf informationelle - Selbstbestimmung - Recht auf Datenschutz – directive 95/46/EC - framework decision 2008/977/JHA – directive 2006/24/EC

II. Criminalità informatica - competenza penale dell'Unione europea - diritto alla riservatezza - protezione dei dati personali - direttiva 2013/40/UE - artt. 615 *ter* - 615 *quinquies* cp - art. 617 *quater* cp - artt. 635 *bis* - 635 *quinquies* cp

Computer crime - EU criminal competence - right to privacy - protection of personal data - directive 2013/40/EU - arts. 615 *ter*-615 *quinquies* - Italian criminal code - art. 617 *quarter* - Italian criminal code - arts. 635 *bis* - 635 *quinquies* - Italian criminal code

III. Cooperazione giudiziaria penale e di polizia - spazio europeo di libertà, sicurezza e giustizia - obbligo di mutua cooperazione fra le competenti autorità - principio della circolazione internazionale delle informazioni - banche-dati a fini investigativi - rispetto dei diritti della persona - giurisprudenza della Corte EDU e della CGUE - prospettive di riforma del sistema europeo di protezione dei dati personali

Criminal judicial and police cooperation - European area of freedom, security and justice - international availability of data information – investigation and data information system - EHRC and EU Courts' case law - EU reform of data protection

IV. diritto all'oblio - tutela della *privacy* - giurisprudenza italiana - conclusioni Avvocato generale C-131/12 - proposta regolamento europeo in materia di protezione dati personali

The right to be forgotten - privacy defense – Italian jurisprudence – opinion of advocate general in the case C-131/12 – proposal for an European regulation in the field of personal data protection

V. *Google vs Vividown* – Corte d'Appello – posizione di garanzia – responsabilità dell'*internet service provider* – Codice della *Privacy* – diffamazione – art. 167 Codice della *Privacy* – trattamento dei dati personali – obbligo di informativa – controllo preventivo – *providers*

Google vs Vividown – Appeals Court decision – duty of care – Data protection code – internet service provider's liability – defamation – art. 167 data protection code – processing of personal data - filtering content – notice concerning processing of personal data – providers

VI. *Personal name records* - 11 settembre - direttiva 95/46/CE - accordi internazionali - trasporto aereo

Personal name records - September 11 - directive 95/46/EC - international agreements - human aviation transport

PREFAZIONE

di Francesco Priolo

Nella mia veste di Presidente della Scuola Superiore di Catania, sono grato alla Prof.ssa Nicoletta Parisi per aver coinvolto gli allievi della Scuola, Giovanni Antonino Cannetti, Elisa Gulizzi e Giuseppe Versaci, nell'elaborazione del lavoro su "Diritto alla privacy e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo", tema di questo numero del periodico "I quaderni europei".

Un tema di grande interesse e attualità al quale la Scuola Superiore di Catania ha prestato particolare attenzione, inserendolo nell'ambito della programmazione didattica dell'anno accademico 2012/2013. E' stato, infatti, realizzato un corso specialistico rivolto agli allievi della Scuola, iscritti al Corso di Laurea Magistrale a ciclo unico in Giurisprudenza, che ha visto il coinvolgimento nell'attività di docenza della Prof.ssa Nicoletta Parisi e della Dott.ssa Valeria Scalia, nonché del Dott. Roberto Lattanzi, Dirigente presso il Garante per la protezione dei diritti personali.

E' una grande soddisfazione per la Scuola poter condividere con i docenti e gli allievi coinvolti i frutti di questo lavoro, maturato proprio tra i banchi di una sua aula.

Sono fiero di Elisa, Giovanni e Giuseppe che hanno saputo cogliere la sfida della Scuola: l'avvio precoce alla ricerca è, infatti, uno degli obiettivi su cui si fonda la *mission* della Scuola, unitamente alla formazione integrativa interdisciplinare e specialistica che viene offerta ai propri allievi.

Ringrazio ancora una volta la Prof.ssa Nicoletta Parisi che, in qualità di *tutor* della Scuola, segue con passione e dedizione gli allievi nel loro percorso formativo.

L'impegno della Scuola a sostegno di giovani meritevoli con l'obiettivo primario di far emergere il loro talento è premiante e questo lavoro lo testimonia!

INTRODUZIONE AI LAVORI

di Vincenzo di Cataldo

Come delegato del Dipartimento giuridico nel Consiglio scientifico della Scuola Superiore sono lieto di dare il mio saluto a tutti coloro che partecipano a questo incontro di studio, ed in particolare a coloro che hanno condotto la ricerca che è alla base di questo incontro.

Il tema del confronto tra diritto alla *privacy* e trattamenti automatizzati di dati si pone al crocevia tra diritto civile e diritto penale e trova indicazioni e condizionamenti forti nel diritto dell'Unione europea e nel diritto internazionale. Diritto dell'Unione europea e diritto internazionale, oggi, forniscono contributi normativi importanti a qualunque tema del diritto interno (civile o penale o amministrativo). Chi ha iniziato a studiare diritto in un'altra epoca può trovare difficile assuefarsi a questa idea; per coloro che si avviano oggi allo studio del diritto questo deve essere un dato di assoluta ovvietà. Ma questa ovvietà non sempre e non da tutti viene comunicata con la necessaria chiarezza ed insistenza. Ed è per questo che dobbiamo essere particolarmente grati alla Prof.ssa Nicoletta Parisi, che da anni, in questa Scuola, propone iniziative diverse (seminari, corsi interni, attività di ricerca coinvolgente gli Allievi), tutte ispirate rigorosamente a questa importante indicazione di fondo. E la Scuola è lieta di accogliere queste indicazioni, perché sono esattamente in linea con la sua *mission*, che è quella, ce lo ricorda di continuo il Presidente Priolo, della "contaminazione dei saperi".

Sono nato, ed ho studiato diritto, in un mondo che non era dotato di alcuna di quelle tecnologie che hanno costruito, praticamente dal nulla, il mondo oggi tentacolare dell'informatica. Era un mondo che non conosceva neppure, almeno a livello nazionale, regole positive di tutela della riservatezza. Il problema della *privacy* iniziava a porsi, ma rimaneva fermo ad apparizioni giurisprudenziali non frequentissime. Da un lato, non era ancora venuta a maturazione una precisa consapevolezza del valore che la riservatezza può avere per ciascuno di noi; dall'altro, gli strumenti capaci di attentare alla riservatezza del singolo erano ancora in una fase di sviluppo che potremmo dire embrionale. Si riducevano quasi solo alle macchine fotografiche dei paparazzi, rese immortali da Fellini ne "La dolce vita", ancora con il *flash* a lampada, ed ai primi registratori a nastro. Gli strumenti di tutela dei pochi che ne venivano colpiti spesso erano, più che processi e sentenze, i cazzotti e le risse, come quelli, famosi, tra Walter Chiari ed i fotografi che lo avevano sorpreso in compagnia della mitica Ava Gardner.

In realtà, allora, i problemi della riservatezza erano problemi di pochi. Dei pochi, pochissimi "divi" che, in un mondo ancora privo di divorzio, di aborto, di convivenze, potevano permettersi un comportamento deviante, e per questo erano invidiati e spiati da tutti gli altri, chiamati invece al rispetto di regole sempre meno sentite, e quindi sempre più opprimenti (chi non era un divo era chiamato a pagare, se faceva le stesse cose: la Dama bianca conobbe il carcere per avere avviato una relazione adulterina con Fausto Coppi). Ma, come ho detto, l'intrusione nella vita privata altrui era operazione tecnicamente difficile e complicata, quindi anche costosa, e perciò alla portata di pochissimi. Ce lo fa vedere, ed è oggi un vero pezzo di archeologia della tecnologia, quel bellissimo film di Francis Ford Coppola "La conversazione" ("The conversation"), girato nel 1974, con una interpretazione mostruosa di Gene Hackman.

Progressivamente è nata, è cresciuta e si è affinata anche da noi la sensibilità per la riservatezza.

Contemporaneamente, o quasi, sono nati, sono cresciuti e si sono sviluppati i computer, le banche dati, le chiavette USB, tutte quelle piccole micidiali cose che in gergo si chiamano "cimici". Lo sviluppo dell'informatica ha dilatato enormemente le possibilità di attentato alla riservatezza. Queste due storie, la storia del diritto alla riservatezza e la storia della *Information Technology*, dai primi computer a *internet*, si intrecciano fin dall'inizio, si sviluppano in tempi analoghi con interazioni costanti, in termini che sarebbe certamente interessante studiare in modo un po' più attento di quanto non sia stato fatto finora. Ma il risultato finale (almeno per oggi. Questa storia va avanti, continuerà, non sappiamo in

quali direzioni) è questo: i problemi della riservatezza, oggi, non sono più un problema di pochi, sono diventati un problema di tutti noi.

Il mondo dei computer ci offre enormi possibilità di miglioramento della qualità della nostra vita.

Raccolte di dati, interconnessioni tra archivi, forniscono supporti strepitosi al nostro benessere. A fronte di questi benefici, ci presentano anche, inevitabilmente, un conto di costi assai elevati, proprio, tra l'altro, sotto il profilo dell'attentato alla nostra vita privata, alla nostra riservatezza. È quindi diventato necessario intervenire a livello normativo per costruire barriere protettive. Ma l'evoluzione dell'informatica prosegue, ed offre di continuo nuove prospettive di rischio per la nostra riservatezza. Il che pone la necessità di continui aggiustamenti delle regole di protezione. La legislazione, in questo campo, è un cantiere aperto, un ininterrotto *work in progress*. Oggi abbiamo bisogno di regole di tutela diverse e più forti di quelle di ieri, perché più consistenti sono oggi gli attentati alla nostra riservatezza.

Domani avremo bisogno di nuove regole, ancora più forti, perché domani avremo strumenti informatici ancora più capaci di scrutare, classificare, controllare ciascuno di noi.

È per questo che la ricerca che viene oggi presentata non chiude un periodo di studio, ma se mai lo apre. Auguro agli Allievi che hanno preso parte a questo lavoro, ed a tutti coloro che li hanno aiutati, di conservare intatta la loro curiosità per questi temi. Saranno ancora attuali domani, ed anche dopodomani, ed essi potranno utilmente studiarne, con soddisfazione, nuovi accadimenti, nuovi sviluppi.

I. «DIRITTO ALLA PROTEZIONE DEI DATI DI CARATTERE PERSONALE»: APPUNTI DI VIAGGIO*

di Roberto Lattanzi

Sommario: 1. Da Nizza a Lisbona. - 2. Da Parigi e Strasburgo…- 3. *(Segue)* via Karlsruhe…- 4. *(Segue)* a Bruxelles. - 5. Schengen - L'Aja - Prüm. - 6. Dopo Lisbona.

1. Da Nizza a Lisbona

All'interno del capo II della Carta dei diritti fondamentali dell'Unione europea dedicato alle "Libertà" – oggetto nel suo complesso delle riflessioni di questa giornata di studio – il "tradizionale" diritto alla tutela della vita privata è seguito da un "nuovo" diritto fondamentale, il «diritto alla protezione dei dati di carattere personale»: questa la locuzione presente nell'articolo 8.

Con la Carta siglata a Nizza il 7 dicembre 2000, specie a seguito del Trattato di Lisbona che alla medesima ha riconosciuto pieno valore giuridico[1], ha così trovato formale compimento a livello europeo[2] non solo il processo di *costituzionalizzazione* del diritto alla protezione dei dati personali, nel solco di quanto già accaduto in alcune Costituzioni nazionali e con l'ispirazione di interventi autorevoli da parte di alcune Corti costituzionali[3], ma anche il percorso di sua *autonomizzazione* rispetto ad altre situazioni giuridiche soggettive[4], in particolare al diritto alla tutela della vita privata[5].

Considerazione, quest'ultima, che dovrebbe spingere l'interprete a non confondere più i tratti del nuovo "diritto" – grazie al quale, invero, si individuano, con formulazione ellittica, una serie di «tecniche di tutela che si offrono all'interessato ove esso intenda reagire ad un trattamento dei dati non conforme a legge»[6] – con altre situazioni giuridiche soggettive; ove si voglia più puntualmente far riferimento alla situazione giuridica soggettiva di cui si tratta, dovranno quindi essere utilizzate con

---

* Con l'aggiunta dei riferimenti bibliografici di primo riferimento e degli aggiornamenti essenziali, volti a rendere conto del complessivo processo di revisione della cornice normativa dell'Unione europea in materia di protezione dei dati personali (che interessa anzitutto la direttiva 95/46/CE), il testo riproduce la relazione svolta il 16 marzo 2009 nell'ambito del Convegno tenutosi nell'Università cattolica del Sacro Cuore di Milano, dal titolo "La libertà", organizzato dal Centro Europeo di Diritto del lavoro e Relazioni Industriali (CEDRI) con il coordinamento del Prof. Mario Napoli e a cura di questi pubblicato nel volume *La libertà,* Milano, 2013, p. 63 ss. Le considerazioni svolte, proprie dell'Autore, non sono riferibili all'Istituzione presso la quale opera.

1 L'art. 6, par. 1 del Trattato sull'Unione europea (in *GUUE*, C 83, 30 marzo 2010, p. 13) dispone infatti che «L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati». Si è così superato il dibattito sul valore (prevalentemente politico piuttosto che) giuridico della Carta, rispetto al quale v., tra i primi contributi, quello di S. RODOTÀ, *The Charter of Fundamental Rights*, in *ZSR*, 2001, p. 7.

2 E più precisamente, in base all'art. 16, par. 2 del Trattato sul funzionamento dell'Unione europea (TFUE), nelle materie che rientrano nel campo di applicazione del diritto dell'Unione europea (per le quali cfr., in particolare, gli artt. 2-4 TFUE).

3 Su tale aspetto si tornerà nel par. 3. Quanto alle previsioni inserite nelle carte fondamentali, basti considerare l'art. 35°, *Constituição da República Portuguesa*, del 2 aprile 1976 (più volte rimaneggiato), l'art. 18, comma 4, *Constitución española* del 27 dicembre 1978 e l'art. 10 della Costituzione olandese del 17 febbraio 1983, come pure, in tempi meno remoti, quelle contenute nei testi costituzionali dei "nuovi" *Länder* tedeschi (come, del resto, di molti paesi dell'est-Europa). Evidentemente influenzato dalla Carta di Nizza, l'art. 9A della Costituzione greca è stato introdotto nella revisione cui la medesima è stata sottoposta nel 2001.

4 In merito a tale profilo cfr. par. 2.

5 Con riferimento all'ordinamento italiano, v. già S. RODOTÀ, *Libertà personale. Vecchi e nuovi nemici*, in M. BOVERO (a cura di), *Quale libertà. Dizionario minimo contro i falsi liberali*, Roma – Bari, 2004, p. 33, p. 52; ID., *Il progetto della Carta europea e l'art. 42 Cost*., in M. COMPORTI (a cura di), *La proprietà nella Carta europea dei diritti fondamentali*. Atti del Convegno di studi organizzato presso l'Università degli Studi di Siena, 18-19 ottobre 2002, Milano, 2005, p. 155, p. 167; anche U. DE SIERVO, *La* privacy, in S.P. PANUNZIO (a cura di), *I diritti fondamentali e le Corti in Europa*, Napoli, 2005, p. 345, nell'*incipit* del saggio – che, in questo (prezioso ed esplicito) avvertimento, si differenzia dall'articolo pubblicato dall'Autore con il titolo *Tutela dei dati personali e riservatezza*, in *Diritti, nuove tecnologie, trasformazioni sociali. Scritti in onore di Paolo Barile*, Padova, 2003, p. 297 – chiarisce che la tutela dei dati personali è concetto «ormai largamente autonomo dalla riservatezza personale [e] qualcosa di radicalmente diverso da quello a cui ci si riferiva nel passato anche recente [parlando di *privacy*]»; incertezza, invece, manifestano sul punto ancora R. LEENES, B. J. KOOPS, P. DE HERT, *Conclusions and Recommendations*, all'esito dello studio comparatistico dagli stessi curato e pubblicato con il titolo *Constitutional Rights and New Technologies. A Comparative Study*, 2008, p. 265, p. 271.

6 A. DI MAJO, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in *Studi in onore di Pietro Rescigno*, II Diritto privato, 1, in *Persone, famiglia, successioni e proprietà*, Milano, 1998, p. 263, p. 271.

grande parsimonia (o, meglio, tutt'affatto) le locuzioni "vita privata" o riservatezza (familiari alla tradizione italiana) e, a maggior ragione (per quanto divenute di uso comune)[7], "privacy" o "diritto alla privacy", ancorché da queste si sia formato, per gemmazione, il diritto alla protezione dei dati[8]. Ciò per la ragione che quest'ultimo ha trovato ormai adeguata caratterizzazione in più corpi normativi, dapprima a livello internazionale e comunitario[9] e, quindi, «in zona ludibrio»[10], nazionale[11]; né il richiamo ad un maggiore rigore terminologico riposa sul solo tradizionale brocardo *entia non sunt multiplicanda sine necessitate*, ma sull'esigenza di "alleggerire" la clausola generale della *privacy*, espressione che, tanto più spazio è venuta guadagnando in estensione, tanto più è venuta mostrando incerti confini (con un accentuarsi del pericolo di un suo uso meno "controllato")[12].

Diritto, quello in esame, che, mediante l'introduzione di forme di tutela che si appuntano sui dati personali – tasselli del mosaico che va a comporre (e ricomporre) la "persona elettronica", quale risulta dal trattamento dei dati di volta in volta effettuato[13] –, intende invero proteggere la persona ("in carne e ossa", verrebbe da aggiungere) da usi impropri o illegittimi delle informazioni che ad essa si riferiscono o specifiche situazioni giuridiche soggettive alla stessa riconducibili, prime fra tutte la vita privata o l'identità personale (come si evince dall'art. 2, comma 1, d.lgs. n. 196/2003)[14], assicurando forme di partecipazione della stessa al processo decisionale basato sul trattamento dei dati personali che la riguardano[15] e – come di recente riconosciuto con formulazione felice dalla Corte di Cassazione – concorrendo «a delineare l'assetto di una società rispettosa dell'altro e della sua dignità in condizioni di eguaglianza»[16]. E diritto che, per un verso, ha una portata più ristretta rispetto al diritto alla tutela della

---

7 Nel contesto italiano un contributo in questa direzione è stato forse offerto dall'utilizzo colloquiale della dizione "Garante della privacy" attribuito al Garante per la protezione dei dati personali che, con più precisa, ma purtroppo lunga dizione, era stato originariamente denominato "Garante per la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" (art. 30, l. 31 dicembre 1996, n. 675).

8V. già, con riguardo al trattamento di dati personali riferiti alle condizioni di salute, la sentenza della Corte europea dei diritti dell'uomo, 25 febbraio 1997, *Z c. Finlandia*, App. 22009/93; 27 agosto 1997, *M.S. c. Svezia*, App. 20837/92.

9 V. infra parr. 2 e 3. Non deve trarre in inganno la più sobria individuazione dei caratteri del diritto alla protezione dei dati personali contenuta nell'art. 8 della Carta di Nizza (della quale è peraltro criticabile il peso che, diversamente da quanto emerge dall'esperienza, sembra essere attribuito al consenso individuale la cui valenza quale strumento effettivo di tutela dell'interessato è stata già da tempo rilevata: cfr. S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, p. 45) rispetto al più ricco armamentario del quale il diritto risulta dotato nella direttiva 95/46/CE, posto che l'art. 53 della Carta medesima prevede che «Nessuna disposizione della presente Carta deve essere interpretata come limitativa o lesiva dei diritti dell'uomo e delle libertà fondamentali riconosciuti, nel rispettivo ambito di applicazione, dal diritto dell'Unione, dal diritto internazionale, dalle convenzioni internazionali delle quali l'Unione o tutti gli Stati membri sono parti, in particolare dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, e dalle costituzioni degli Stati membri».

10 C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *EDP*, 1998, p. 653 e 654.

11 Dapprima con la l. 31 dicembre 1996, n. 675 (sulla quale v. G. BUTTARELLI, *Banche dati e tutela della riservatezza. La* privacy *nella società dell'informazione. Commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale*, Milano, 1997, *passim*) e, quindi, con il d.lgs. 30 giugno 2003, n. 196, con il quale si è riordinata la materia che nel volgere di pochi anni – anche in ragione del parziale esercizio della delega contenuta nella legge 31 dicembre 1996, n. 676 – era divenuta caotica, completando con lo stesso il recepimento delle direttive 95/46/CE e 2002/58/CE.

12 Come è noto, non sono mancate critiche autorevoli rispetto all'espressione "privacy" proprio in ragione dell'indeterminatezza che la connota: celebre quella con la quale si apre il saggio di R.A. POSNER, *The Right of Privacy*, 12, in *LQR*, 1978, p. 393: «[t]he concept of "privacy" is elusive and ill defined»; ID., *Privacy, Secrecy and Reputation*, 28, in *BuffLR,* 1979, p. 3); pure R. WACKS, *The Poverty of Privacy*, 96, in *LQR,* 1980, p. 73, p. 86 ss., ha (criticamente) rilevato l'attitudine del termine "privacy" a colonizzare altre (più tradizionali) situazioni giuridiche soggettive e, a trent'anni di distanza, ancora stima che «an acceptable definition of privacy remains elusive» (cfr. R. WACKS, *Privacy. A Very Short Introduction*, Oxford, 2010, p.40).

13 Ciò è reso evidente da F. HONDIUS, *A Decade of International Data Protection*, 30, in *NILR,* 1983, p. 103, p. 109, , per il quale «in the information age people should be protected by protecting the information relating to them»; nello stesso senso P. ANCEL, *La protection des données personnelles. Aspect de droit privé français*, in *RIDC*, 1987, p. 609, p. 611 ss., p. 624.

14 Circostanza che ha indotto autorevole dottrina a ricondurre il diritto alla protezione dei dati personali alla figura del "diritto su diritti": C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, cit., p. 656. Più in generale, sulla valenza strumentale del rispetto della stessa *privacy* ad altri (più alti) valori, primo fra tutti la dignità della persona (come in caso di utilizzo delle informazioni personali in chiave discriminatoria), v. il classico saggio di C. FRIED, *Privacy*, 77, in *YaleLJ*, 1968, p. 475, ove si mette in luce che «privacy in its dimension of control over information is an aspect of personal liberty» (p. 483).

15 Per il tramite della previa informativa e, in talune ipotesi, del consenso dell'interessato al trattamento dei dati che lo riguarda nonché mediante l'esercizio del diritto d'accesso ai medesimi.

16 Cass. (ord.), 4 gennaio 2011, n. 186, (sintetizzata), in *GI*, 2011, p. 256 e 257, ordinanza che – peraltro aderendo contenutisticamente a quanto già affermato dal Garante nel provvedimento generale relativo al trattamento dei dati personali nell'amministrazione dei condomini del 18 maggio 2006, punto 3.2, doc. *web* n. 1297626 (oltre che nei Provv.ti 12 dicembre 2001, doc. *web* n. 31007, 20 novembre

vita privata, specie ove si intenda quest'ultimo alla luce della giurisprudenza della Corte europea dei diritti dell'uomo[17], avendo come punto di riferimento immediato "soltanto" la protezione dei dati relativi a un soggetto individuato o individuabile[18]; ma, per altro verso, portata più ampia rispetto al tradizionale diritto alla riservatezza – la cui eco risuona ancora nella "tutela rinforzata" apprestata nei confronti dei c.d. dati sensibili (art. 8 direttiva 95/46/CE e artt. 22 ss. d.lgs. n. 196/2003)[19]– trovando applicazione rispetto al trattamento di qualunque dato personale, finanche pubblico[20], e non solo di quelli che interessano la sfera intima dell'individuo[21].

2. Da Parigi e Strasburgo …

Il processo di autonomizzazione sopra segnalato, sviluppatosi lungo un ampio arco temporale, ha avuto inizio non appena percepiti – a partire dalla metà degli anni sessanta del secolo scorso, anzitutto negli Stati Uniti d'America[22] e, quindi, in Europa[23] – i rischi connessi all'elaborazione elettronica delle informazioni personali, in particolare la multifunzionalità dei dati personali (con il conseguente possibile impiego degli stessi in contesti e per finalità diversi da quelli che ne avevano giustificato l'originaria raccolta)[24]. È stata questa, infatti, l'occasione (ma non l'unica causa efficiente) per elaborare principi e modalità di protezione della persona che di gran lunga sopravanzavano le tradizionali

---

2008, doc. *web* n. 1576139 e 8 luglio 2010, doc. *web* n. 1741950) – ha ritenuto illecita (e fonte di responsabilità) l'affissione nella bacheca dell'androne condominiale dell'informazione concernente le posizioni di debito del singolo partecipante al condominio.

17 Per un'aggiornata e sintetica analisi della portata applicative attribuita all'art. 8 della Convenzione cfr. F.G. JACOBS, R.C.A. WHITE, C. OVEY, *The European Convention on Human Rights*, V ed., Oxford, 2010, p. 357 ss.; R. J. SCHWEIZER, *Die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zum Persönlichkeits- und Datenschutz*, in *DuD*, 2009, p. 462; v. altresì, più diffusamente, gli scritti raccolti in F. SUDRE (a cura di), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruxelles, 2005.

18 Nozione, quella di "dato personale", assai lata, giunta a ricomprendere anche i campioni biologici [cfr. Corte europea dei diritti dell'uomo (Grande Camera), *S. e Marper c. Regno Unito*, 4 dicembre 2008 (Ricorsi no 30562/04 e 30566/04)], sulla quale v. GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI ARTICOLO 29 (Gruppo articolo 29), *Parere 4/2007 sul concetto di dati personali*, adottato il 20 giugno 2007, WP 136.

19 Cfr. S. SIMITIS, "Sensitive Daten" – *Zur Geschichte und Wirkung einer Fiktion*, in *Festschrift für Mario M. Pedrazzini*, Bern, 1990, p. 469; sia consentito rinviare altresì, anche per ulteriori riferimenti, a R. LATTANZI, *Dati sensibili: una categoria problematica nell'orizzonte europeo*, in *EDP*, 1998, p. 713, p. 742, ove si mette in luce, tra le ragioni addotte per una tutela "rafforzata" di tali informazioni, il loro "tradizionale" prestarsi ad utilizzi di tipo discriminatorio (e in questo senso, in *obiter*, v. ora Cass. (ord.), 4 gennaio 2011, n. 186, cit.).

20 Così Corte europea dei diritti dell'uomo, 4 maggio 2000, *Rotaru c. Romania*, (Application no. 28341/95); v. pure Cass., 25 giugno 2004, n. 11864, in *FI*, I, 2004, p. 3380.

21 Cfr. pure Corte di giustizia, 20 maggio 2003, *Rechnungshof* (C-465/00)/*Österreichischer Rundfunk e al.*; *Christa Neukomm* (C-138/01), *Joseph Lauermann* (C-139/01)/*Österreichischer Rundfunk* (casi riuniti C-465/00, C-138/01 e C-139/01); Cass. (ord.), 4 gennaio 2011, n. 186, op. loc. cit.

22 Cfr., in particolare, A. R. MILLER, *Technology, Social Change, and the Constitution*, 33, in *GWLR,* 17, 1964; ID., *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67, in *MichLR,* 1968, p. 1089; A.F. WESTIN, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's*, 66, in *ColLR,* 1966, p.1003; ID., *Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part II: Balancing the Conflicting Demands of Privacy, Disclosure, and Surveillance*, 66, in *ColLR,* 1966, p. 1205; A.F. WESTIN, M.A. BAKER, *Databanks in a Free Society. Computers, Record-Keeping and Privacy*, New York, 1972; cfr. altresì P. BARAN, *Communications, Computers and People*, in *Proceedings of the Fall Joint Computer Conference*, 1965, p. 45; K.L. KARST, "The Files": *Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31, in *LCP*, 1966, p. 354). Ma si vedano altresì risultanze delle audizioni svoltesi presso la House of Representatives – Subcommittee of the Committee on Government operations, "The Computer and Invasion of Privacy", Hearings before a Subcomm. of the Comm. on Government Operations – House of Representatives, 89th Congress, July 26, 27, and 28, 1966, pubblicate in *The Computer and Invasion of Privacy. The Controversial U.S. Government Hearings on the Proposed National Data Center*, New York, 1967, *passim*.

23 R. KAMLAH, *Right of privacy: das allgemeine Persönlichkeitsrecht in amerikanischer Sicht unter Berücksichtigung neuer technologischer Entwicklungen*, Köln, 1969, *passim*; U. SEIDEL, *Datenbanken und Persönlichkeitsrecht. Unter besondere Berücksichtigung der amerikanischen Computer Privacy,* Köln, 1972, p. 56 ss. e p. 130 ss.; S. SIMITIS, *Datenschutz – Notwendigkeit und Voraussetzungen einer gesetzlichen Regelung*, in *DVR*, 1973, p. 138; G. BRAIBANT, *La protection des droits individuels au regard du développement de l'informatique*, in *RIDC*, 1971, p. 793. Per una ricognizione sul tema da parte della letteratura italiana v., tra i primi contributi, S. RODOTÀ, *Elaboratori elettronici, strutture amministrative e garanzie della collettività*, in *RTDP*, 1971, p. 1841; ID., *Elaboratori elettronici e controllo sociale*, Bologna, 1973, *passim*; R. PARDOLESI, *Riservatezza: problemi e prospettive*, in M. SPINELLI (a cura di), *Responsabilità civile*, vol. II, Bari, s.d. (ma 1974), p. 310, p. 316 ss. e p. 378 ss.; A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974, *passim*.

24 Cfr. S. SIMITIS, *Gesetzliche Regelungen für Personalinformationssysteme – Chancen und Grenzen*, *Informationsgesellschaft oder Überwachungsstaat. Strategien zur Wahrung der Freiheitsrechte im Computerzeitalter*, Wiesbaden, 1986, p. 43.

tecniche di tutela dei diritti della personalità (prevalentemente incentrate sul risarcimento del danno e l'inibitoria), inidonee ad offrire una tutela soddisfacente a fronte del mutato panorama (tecno-sociale)[25].

Principi e modalità di protezione originali – la cui attualità è in larga misura rimasta inalterata nel tempo[26] – destinati a consolidarsi, a livello internazionale, nelle *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* del 23 settembre 1980 e nella Convenzione n. 108 sulla tutela dell'individuo rispetto al trattamento dei dati a carattere personale adottata dal Comitato dei Ministri del Consiglio d'Europa il 28 gennaio 1981[27]. Testi sostanzialmente coevi e contenutisticamente prossimi, aventi però diverso valore giuridico: non vincolanti le *Guidelines* redatte a Parigi (in particolare grazie alle pressioni esercitate da gruppi d'interesse di marca nordamericana); vincolante, invece, per gli Stati membri del Consiglio d'Europa, la Convenzione di Strasburgo che, muovendo dalle rilevate carenze dell'art. 8 della Convenzione europea dei diritti umani e delle libertà fondamentali del 1950 (CEDU) nei confronti delle (allora) nuove tecnologie dell'informazione, viene ad integrarne l'armamentario giuridico «with regard to automatic processing of personal data» (art. 1, par. 1 Convenzione n. 108/1981)[28].

Già in questo diverso tratto – ma è solo un inciso, dato che la questione richiederebbe una più diffusa analisi – risiede il germe del diverso approccio di fondo che, nella materia della c.d. *informational privacy*, tuttora connota l'ordinamento statunitense rispetto a quelli europei (con riflessi sulla valutazione di adeguatezza del livello di protezione offerto dagli Stati Uniti d'America ai sensi dell'art. 25 direttiva 95/46/CE in relazione al flusso transfrontaliero di dati personali): impostato su interventi normativi di settore il primo (e, va aggiunto, con una spiccata propensione a favore della *self-regulation* nel settore privato, nonostante i limiti dalla stessa manifestati) ([29]); i secondi, invece, caratterizzati da discipline normative a vocazione generalista[30], integrate dall'operato di autorità di controllo che si vogliono indipendenti[31] e (in modo più marcato nel disegno della Convenzione di Strasburgo) da discipline settoriali[32].

---

25 Cfr. (tra i tanti) A. PROTO PISANI, *Le procedure cautelari d'urgenza in relazione ai dati raccolti con elaboratori elettronici*, in V. ZENO ZENCOVICH (a cura di), *Le banche dati in Italia*, Napoli, 1985, p. 155, p. 163.

26 Cfr. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *A comprehensive approach on personal data protection in the European Union*, Brussels, 4.11.2010, COM(2010) 609 final, che pur nella prospettiva di un aggiornamento della direttiva 95/46/CE (sul punto si tornerà nell'ultimo paragrafo), riconosce che «the core principles of the Directive are still valid and that its technologically neutral character should be preserved».

27 Convenzione essa stessa integrata dall'*Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) regarding supervisory authorities and transborder data flows*, nonché da una pluralità di Raccomandazioni settoriali, ed allo stato in corso di revisione: per una compilazione dei materiali del Consiglio d'Europa cfr. *http://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf*.

28 Il nucleo dei principi poi trasfusi nella Convenzione si rinviene già nell'*Annex* alla Resolution (73) 22 *on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector del Council of Europe* – (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies)e nell'*Annex* alla Resolution (74) 29 *on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector* (Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies).

29 Si tratta di constatazione ricorrente nell'esperienza statunitense: v., per tutti, J.R. REIDENBERG, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44, in *FCLJ*, 195, 1992, p. 208 ss; ID., *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60, in *FordhamLR*, 1992, p. 137, p. 148, che contrappone l' "ad hoc approach" americano all' "omnibus approach" europeo (p. 153); M.S. DORNEY, *Privacy and the Internet*, 19, in *HastCe&ELJ*, 1997, p. 635, p. 642 ss.. Tralasciando il settore delle telecomunicazioni, tra le principali discipline afferenti alla *informational privacy* (in più occasioni adottate sull'onda di scandali che hanno colpito l'opinione pubblica), sono essenzialmente riconducibili al *Freedom of Information Act*, al *Privacy Act*, al *Fair Credit Reporting Act* (FCRA) nonché al *Video Privacy Protection Act*.

30 Ma v. al par. 5 il *patchwork* di regole nei settori del trattamento di dati personali per finalità di polizia e giustizia.

31 Cfr. Corte di giustizia (Grande Sezione), sentenza 9 marzo 2010, causa C-518/07, *Repubblica Federale Tedesca c. Commissione europea,*), in *Raccolta*, 2010, p. I-01885.

32 Strategia questa che, con la (pur) significativa eccezione del settore delle telecomunicazioni e, quindi, delle comunicazioni elettroniche, purtroppo non è stata sufficientemente coltivata a livello comunitario (cfr. nota 55). Né (salvo rare eccezioni) l'autoregolazione (regolata) è stata in grado di produrre "regole" sufficientemente strutturate in grado, se non di sostituire, quanto meno di preparare il terreno per futuri interventi normativi: a questo proposito una nota positiva può ritrarsi dall'ordinamento italiano, nel quale hanno dato buona prova (trovando ampia applicazione nella prassi), in particolare, il *Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica* e, per quanto perfezionabile, il *Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti*.

3. *(Segue)* via Karlsruhe…

Anticipando gli esiti della Carta di Nizza, non solo l'enucleazione, ma il processo di *costituzionalizzazione* del diritto alla protezione dei dati personali (cui si è fatto cenno al par. 1) ha conosciuto un sicuro punto di svolta con l'enunciazione del *Recht auf informationelle Selbstbestimmung* ([33]) da parte del *Bundesverfassungsgericht* (che lo áncora ai par. 1 e 2 del *Grundgesetz*) – e, quindi, esplicitamente, del *Recht auf Datenschutz* ([34]) – quale concretizzazione della figura (dogmaticamente) sovraordinata dell'*allgemeines Persönlichkeitsrecht* ([35]): diritto che, nella prospettiva di questo insegnamento, filtrato al di là del sistema giuridico nel quale è stato formulato[36], consiste, in prima approssimazione, nella libertà accordata all'individuo – salva diversa *chiara* e *dettagliata* previsione normativa [37] – di decidere se e in che misura rendere disponibili informazioni sul proprio conto[38] nonché nel potere di controllarne la successiva circolazione[39] (per far valere, se del caso, ulteriori pretese individuali ed eventualmente attivare il controllo pubblico sui trattamenti effettuati), senza però, come di recente ribadito con forza dalla Corte di giustizia[40], che ciò si traduca in una sorta di signoria dello stesso sui dati personali a sé riferiti[41] sì da orientarne (arbitrariamente o capricciosamente) la circolazione[42].

---

[33] BVerfG, 15 dicembre 1983, in *BVerfGE*, 65, 1; v. anche in *NJW*, 1984, p. 419 con il commento di S. SIMITIS, *Die informationelle Selbstbestimmung – Grundbedingungen einer verfassungskonformen Informationsordnung*, in *NJW*, 1984, p. 398. In realtà la dottrina tedesca aveva già preconizzato l'elaborazione del diritto all'autodeterminazione informativa: cfr. lo sguardo retrospettivo di uno dei protagonisti del dibattito in materia offerto da W. STEINMÜLLER, *Das informationelle Selbstbestimmungsrecht: wie es entstand und was man daraus lernen kann*, in *RDV*, 2007, p. 158.

[34] Espressamente enunciato in BVerfG, 27 giugno 1991, in *NJW*, 1991, p. 2129, p. 2132.

[35] Processo analogo a quello che ha generato l'*informationelle Selbstbestimmungsrecht* è stato di recente reiterato dal *Bundesverfassungsgericht* con l'elaborazione di una figura allo stesso prossima, quella del *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*: cfr. BVerfG, 1 BvR 370/07 del 27 febbraio 2008, in particolare parr. 201 ss., in *http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html*.

[36] Si tratta di una decisione che ha avuto eco assai ampia: la *Supreme Court of Canada* ha descritto la *informational privacy* come «the right of the individual to determine for himself when, how and to what extent he will release personal information about himself» (*R. v. Duarte*, [1990] 1 S.C.R. 30, 46); sulle orme della giurisprudenza costituzionale tedesca v., nell'ordinamento spagnolo, la fondamentale sentenza del *Tribunal Constitucional*, 30 novembre 2000, n. 292, in *BOE* n. 4, 4 gennaio 2001 (e già in precedenza STC 254/93 del 20 luglio 1993, in *BOE*, n. 197, 18 agosto 1993).

[37] Oltre alla sentenza della Corte Costituzionale tedesca v. altresì Corte europea dei diritti dell'uomo, *Copland v. The United Kingdom*, 3 aprile 2007, 62617/00, punto 46: «the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures».

[38] In tal senso si esprimevano già O.M. RUEBHAUSEN, O.G. BRIM, *Privacy and Behavioral Research*, 65, in *ColLR*, 1965, p. 1184, p. 1189,: «[t]he essence of privacy is no more, and certainly no less, than the freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behaviour and opinion are to be shared with or withheld from others».

[39] Peculiarità che, per marcare la diversità rispetto al "tradizionale" diritto alla riservatezza è stata sintetizzata nello *slogan* "dal segreto al controllo" da S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, p. 102. Anche C Cost., 7 luglio 2005, n. 271, in *GCost*, 2005, p. 4, giunge ad affermare che la disciplina sulla protezione dei dati personali attribuisce all'interessato il «potere di controllare le informazioni che lo riguardano e le modalità con cui viene effettuato il loro trattamento».

[40] Cfr. Corte di giustizia, sentenza 9 novembre 2010, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke* e *Eifert*, punto 48 (con ulteriori riferimenti) e Corte di giustizia (III Sez.), sentenza 5 maggio 2011, C-543/09, avente ad oggetto una domanda di pronuncia pregiudiziale proposta dal *Bundesverwaltungsgericht*, par. 50 secondo la quale il «diritto alla protezione dei dati personali non appare […] come una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale».

[41] Chiarissimo a questo proposito il passo della sentenza secondo cui il diritto alla protezione dei dati «würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist» (BVerfG, 15 dicembre 1983, *BVerfGE* 65, 43). Nel senso che debba essere esclusa con riguardo alle discipline di protezione dei dati la prospettazione di una sorta di diritto reale dell'interessato sulle "proprie" informazioni – prospettiva acriticamente assunta (e senza cura alcuna del dato normativo) si svolge, invece, il saggio di G. CLERICO, *Informazione personale e* privacy. *Valutazione economica della scelta pubblica*, in ID., *Asimmetria informativa, incertezza e scelta pubblica*, Milano, 2002, p. 1 ss. – mi sono espresso in R. LATTANZI, *Dati sensibili*, cit., p. 717 ss. (cui sia consentito rinviare per una più ampia trattazione del profilo richiamato nel testo); ribadisce chiaramente il rifiuto di contaminazione con modelli proprietari di tutela (già argomentato in *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *RCDP*, 1998, p. 339) D. MESSINETTI, *Per un'ecologia della modernità: il destino dei concetti giuridici. L'apertura di* R. *Nicolò a situazioni complesse*, in *RCDP*, 2010, p. 23, p. 32: «si può dire che oggi la riservatezza è incommensurabilmente più esposta di ieri. Tuttavia il rimedio a questa maggiore esposizione non si trova certo riconducendo dati e vicende personali ad un problema appropriativo».

[42] Risalente, infatti, è la critica all'approccio quasi proprietario sulle informazioni personali che implicherebbe un illimitato potere di esclusione dell'accesso ad esse in assenza dell'autorizzazione dell'interessato medesimo: cfr. A. BALDASSARRE, Privacy *e Costituzione*, cit., p. 432, secondo il quale «[…] è stato giustamente detto che una disciplina che si fondasse unicamente sul consenso dell'interessato, onde permettere o meno la lecita intrusione nella propria vita privata, sarebbe una disciplina anacronistica, demagogica e fuorviante, poiché

La natura di diritto fondamentale (*Grundrecht*) attribuito all'*informationelles Selbstbestimmungsrecht* non lascia tuttavia spazio a concezioni grettamente individualistiche o a radicalizzazioni: vale infatti anche in questo ambito l'insegnamento di Luigi Mengoni secondo cui, «in quanto valori costituzionalmente riconosciuti e garantiti, i diritti fondamentali sono sempre intrinsecamente limitati, anche quelli enunciati nella Carta costituzionale senza richiamo, nemmeno generico, di limiti […]. Nel caso di collisione tra due diritti o tra un diritto individuale e un interesse collettivo costituzionalmente protetto occorre procedere a una valutazione ponderata (c.d. bilanciamento) per determinare, in rapporto alle circostanze concrete, la prevalenza dell'uno o dell'altro oppure la misura del contemperamento dell'uno con l'altro» [43]. Operazione (talvolta assai difficoltosa in termini di politica del diritto) rimessa, anzitutto, alla discrezionalità del legislatore: a quest'ultimo spetta la concreta articolazione tra varie opzioni di politica del diritto (e dunque la definizione dei termini del c.d. bilanciamento), salvo l'assoggettamento delle decisioni frutto del processo legislativo al vaglio di legittimità costituzionale; solo in seconda battuta, in via interpretativa, l'attività di bilanciamento compete al giudice[44] e, per quanto qui interessa, in materia di protezione dei dati personali, anche al Garante.

4. *(Segue)* a Bruxelles

Quanto finora descritto – unitamente alle esperienze nazionali nel frattempo maturate a partire dalla prima disciplina europea del 1970 nel *Land* dell'Assia – ha, da un lato, rappresentato il retroterra della direttiva 95/46/CE[45], matrice delle vigenti discipline di protezione dei dati personali nell'Unione europea – (pur con i dovuti adattamenti, in larga parte) indifferentemente applicabili a soggetti pubblici e privati – con la correlativa creazione di un ampio spazio geo-economico nel quale la materia è regolata secondo principi armonizzati e, dall'altro, ha favorito il (parziale) superamento della precedente situazione di (più o meno accentuata) frammentazione[46]. Esito divenuto improrogabile a livello comunitario atteso che, volendosi realizzare la libera circolazione di beni, servizi e persone, anche le

finirebbe per dimenticare sia i più complessi problemi sollevati dall'uso delle più moderne tecnologie, sia, soprattutto, i vari condizionamenti economici e sociali che normalmente incidono sulle manifestazioni di consenso dei singoli. Al contrario, il maggior onere relativo alla tutela della *privacy* non può non gravare sul legislatore, su cui ricade il dovere di stabilire una disciplina rigida e tassativa, laddove siano in questione interessi fondamentali dell'individuo». Non diversa posizione è sostenuta nella comparazione: cfr., tra i tanti, P. BLUME, *New Technologies and Human Rights*, cit., p. 3.

43 L. MENGONI, *Fondata sul lavoro: la Repubblica tra diritti inviolabili e doveri inderogabili di solidarietà*, in *Jus*, 1998, p. 45, p. 48. Sulla stessa linea, proprio in materia di protezione dei dati personali, la recente sentenza della Corte di giustizia (Grande Sezione), 9 novembre 2010, cause riunite C-92/09 e C-93/09, *Schecke e Eifert c. Land Hessen*, in part. punti 76 e 77 (con riguardo alla pubblicazione di dati personali in *internet* da parte di un soggetto pubblico per soddisfare esigenze di trasparenza); v. altresì, a seguito di una domanda di pronuncia pregiudiziale nelle cause riunite C-465/00, C-138/01 e C-139/01, la pronuncia della Corte di giustizia, 20 Maggio 2003, *Rechnungshof c. Österreichischer Rundfunk e a.* e tra *Neukomm e Lauermann c. Österreichischer Rundfunk*, punti 88-90. Ciò, peraltro, risulta chiaramente dall'art. 8, par. 2 CEDU.

44 Si tratta di un profilo già acutamente rilevato, proprio in relazione ai diritti della personalità, da A. BELVEDERE, *Riservatezza e strumenti d'informazione*, in N. IRTI (a cura di), *Dizionari di diritto privato*, vol. 1, Diritto civile, Milano, 1980, p. 727, p. 752 ss., del quale è opportuno riferire il passo: «[l]a tutela giuridica della riservatezza nasce quindi dalla valutazione comparativa di interessi, costituzionalmente garantiti e tendenzialmente contrastanti, il cui "peso specifico" andrà, però, valutato caso per caso. Questo difficile bilanciamento di interessi spetta in primo luogo al legislatore ordinario […], ma può essere compiuto anche dal giudice (e in genere dall'interprete) quando si tratti di interpretare le norme già esistenti, di regolarne l'estensione analogica, o di esprimere i principi generali applicabili, quando a questi debba farsi ricorso. Questo apprezzamento comparativo degli interessi in gioco, raggiungerà le punte della massima difficoltà quando a favore sia della circolazione che del "blocco" delle notizie militino ragioni di tutela della libertà del cittadino e della sua possibilità di partecipare alla vita politico-sociale del Paese […]. Più facile invece potrebbe essere la valutazione quando di fronte ad interessi di questo tipo ci fossero – a favore sia del riserbo […], sia della comunicazione […] – interessi di natura principalmente economica, tutelati sì dalla Costituzione (art. 41 e 42), ma subordinatamente alla difesa della libertà e dignità umane […]».

45 Direttiva 95/46/CE del Parlamento europeo e del Consiglio *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, in *GUCE*, L 281, 23 novembre 1995, p. 31.

46 Per una ricognizione dei contenuti delle principali normative europee alle soglie dell'emanazione della direttiva 95/46/CE cfr. C.O. DRESSEL, *Die gemeinschaftsrechtliche Harmonisierung des Europäischen Datenschutzrechts*, München, 1995, *passim*; sulle fasi che hanno condotto alla redazione della direttiva e sui diversi modelli che ne hanno influenzato il contenuto v. S. SIMITIS, *From the Market to the Polis: The EU Data Protection Directive on the Protection of Personal Data*, 80, in *Iowa*LR, 1995, p. 447, che correttamente in altro studio (S. SIMITIS, *Datenschutz und Europäische Gemeinschaft*, in *RDV*, 1990, p. 2, p. 3) evidenzia l'improprietà del ricorso ai termini "armonizzazione" o "ravvicinamento" delle legislazioni in materia di protezione dei dati (obiettivo proprio delle direttive) posto che, in taluni casi (come quello italiano o greco), la direttiva ha rappresentato l'ennesima spinta a colmare (più o meno ampie) lacune negli ordinamenti nazionali.

informazioni personali avrebbero dovuto circolare liberamente all'interno dei confini europei[47], ovviandosi così anche alla situazione di disparità concorrenziale nella quale venivano ad operare le imprese all'interno del mercato unico (quelle "obbligate" a conformarsi alle regole di protezione dei dati e quelle "autorizzate", dall'inerzia dei legislatori nazionali, a farne a meno).

Questi i fattori che hanno quindi condotto – attraverso un processo ostacolato da forti resistenze [48] – all'adozione della direttiva 95/46/CE, preordinata a rendere possibile, secondo il dettato del suo art. 1, la coesistenza di due valori[49]: da un lato, il raggiungimento di un livello di protezione dei diritti fondamentali della persona (come pure si legge nei considerando da 1 a 3 e 10), che il legislatore comunitario ha voluto di grado "elevato"; dall'altro, la realizzazione della libera circolazione dei dati personali (come esplicitato anche nei considerando 3 e 9) all'interno della Comunità europea, dando vita così a un «informationeller Großraum»[50] regolato da principi generali, già consolidatisi nelle normative di protezione dei dati personali all'epoca vigenti[51]. In particolare – e senza poter procedere, in questa sede, ad un esame di dettaglio – i principi "cardine" di liceità e correttezza del trattamento, al centro dei quali sta il principio di trasparenza (imperniato sul diritto dell'interessato ad essere informato circa le caratteristiche essenziali del trattamento) e di pubblicità (con la costituzione di registri dei trattamenti liberamente consultabili presso le autorità di controllo)[52], ai quali sono affiancati il principio di qualità dei dati[53], comprensivo dei principi di pertinenza e non eccedenza nell'uso delle informazioni (ulteriormente esplicitato, in taluni ordinamenti, dal principio di "minimizzazione" nella configurazione dei sistemi informativi)[54], il principio di finalità[55] e quello di sicurezza del trattamento[56]; si devono ricordare, infine, i "diritti" attribuiti all'interessato, primo fra tutti quello di accesso ai dati che lo riguardano[57], che prelude ad ulteriori facoltà attribuite all'interessato medesimo, quali – ricorrendone i

---

47 Cfr. S. SIMITIS, *Datenschutz und Europäische Gemeinschaft*, cit., p. 6.

48 Cfr. C. BENNETT, *Regulating Privacy*, cit., *passim*, con prevalente attenzione agli ordinamenti francese e tedesco.

49 Cfr. J. R. MAXEINER, *Freedom of Information and EU Data Protection Directive*, in *FCLJ,* 1995, vol. 48, p. 93.

50 Cfr. A. EINWAG, *Grenzüberschreitender Datenverkehr aus Sicht des Bundesbeauftragten für den Datenschutz*, in *RDV*, 1990, p. 1; non diversamente G. PEARCE, *Regulating Personal Data Transfers from the European Union to Third Countries*, 1999, in *www.abs.aston.ac.uk*, p. 4, parla di un «common data protection space enabling the unrestricted transfer of personal data across the UE».

51 S. SIMITIS, *From the Market to the Polis*, cit., p. 451, ha messo in luce, criticandola, la tendenza degli Stati membri (che ha contribuito a frenare il processo di adozione della direttiva) nel far filtrare nella disciplina comunitaria per quanto possibile i (propri) modelli nazionali piuttosto che forgiarne uno nuovo (con più ambiziose mete).

52 Cfr. ora, ad esempio, nell'ordinamento italiano, rispettivamente, gli artt. 13 ss. e 37, d.lgs. n. 196/2003.

53 Cfr. art. 11 d.lgs. n. 196/2003; v. altresì S. SIMITIS, *Datenschutz – eine notwendige Utopie*, in R.M. KIESOW, R. OGOREK, S. SIMITIS (a cura di), *Summa. Dieter Simon zum 70. Geburtstag*, Frankfurt a. M., 2005, p. 511, p. 526.

54 *Sparsamkeitsprinzip*, letteralmente "principio di economicità", inizialmente introdotto nell'ordinamento tedesco (ma già molto tempo addietro S. SIMITIS, *Computer, Sozialtechnologie und Jurisprudenz*, cit., p. 468, ebbe modo di affermare che «nur die Ökonomie der Daten garantiert die individuelle Freiheit») e, quindi, in quello italiano, con l'introduzione del precetto contenuto nell'art. 3 d.lgs. n. 196/2003, applicazione del più generale principio di necessità previsto all'art. 11, secondo cui «i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità»: principio, quello della "minimizzazione" dei dati personali, destinato ad assumere crescente rilevanza nella realtà attuale, specie in caso di interconnessione di diversi archivi [in merito, cfr. le conclusioni di S. SIMITIS, *Datenschutz – eine notwendige Utopie*, in R.M. KIESOW, R. OGOREK, S. SIMITIS (a cura di), *Summa. Dieter Simon zum 70. Geburtstag*, Frankfurt a. M., 2005, p. 511] e in corrispondenza dei c.d. trattamenti invisibili, rispetto ai quali, oltre ad una ridotta consapevolezza dei trattamenti effettuati da parte degli interessati, vi è anche una compressione del potere attribuito agli stessi di influenzare il trattamento (cfr. INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG DER ÖSTERREICHISCHEN AKADEMIE DER WISSENSCHAFTEN, *Datenvermeidung in der Praxis. Individuelle und gesellschaftliche Verantwortung. Endbericht*, Wien, 2002, p. 45 ss.).

55 Con ragione, insiste sulla sua centralità P. BLUME, *New Technologies and Human Rights: Data Protection, Privacy and the Information Society*, Paper no. 67, Institute of Legal Science, Section B, University of Copenhagen, 1998, 8: «[i]t should generally be made clear that the *finalité* principle must be conceived as a human rights principle which must be upheld and taken seriously by supervisory authorities, courts, etc. In this respect it must be maintained that the purpose of data processing should be stated precisely by controllers and also be formulate in a way that is comprehensible for the average individual. In particular it should be seen as unacceptable that a multitude of purposes are stated as the reason for the collection of data because this in reality means that the individual cannot grasp the situation». Merita aggiungere che la finalità del trattamento deve essere attuale, e non futura e ipotetica.

56 Così li sintetizza S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, (già in *RCDP*, 1984, p. 757 ss.) in ID., *Tecnologie e diritti*, Bologna, 1995, p. 41, p. 62 ss.

57 Si tratta di una delle prerogative fondamentali riconosciute all'interessato il quale «di regola non [sa] cosa sta succedendo e non lo [può] scoprire, perché un abuso di questo tipo viene normalmente nascosto alla fonte, anche se potrebbe avere conseguenze reali sulla vita delle persone»: così A. BELSEY, *Privacy, pubblicità e politica*, in A. BELSEY, R. CHADWICK, *Etica e giornalismo* (orig., *Ethical Issues in Journalism and the Media*, 1992, trad. it. di C. Montani), Torino, 1996, p. 109, p. 112. Uno strumento, non altrimenti ricavabile dall'ordinamento (come ebbi

presupposti – la richiesta di rettifica o cancellazione dei dati ovvero di opposizione ad un loro ulteriore trattamento o, ancora, quella volta a conoscere l'origine delle informazioni nonché le categorie di soggetti o i soggetti cui le stesse sono state comunicate[58].

5. Schengen - L'Aja - Prüm

Per quanto la direttiva 95/46/CE (e le rispettive discipline nazionali cui è stato affidato il suo recepimento)[59] abbia occupato (e tuttora occupi) larga parte della scena, essendo la sede dei principi di portata generale appena indicati, essa trova però applicazione alle sole materie (in passato denominate) di c.d. primo pilastro, restando invece estranea alle materie di c.d. secondo e terzo pilastro[60]. Ciò risulta a chiare lettere, peraltro, dall'art. 3, par. 2 direttiva 95/46/CE che espressamente esclude dal proprio ambito di applicazione, tra l'altro, i trattamenti «effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale»[61].

Per quanto in più di una circostanza sia risultato difficoltoso distinguere chiaramente i confini tra i vari "pilastri"[62], nel (preesistente) terzo pilastro, relativo alle materie di cooperazione di polizia e giudiziaria in materia penale, hanno continuato a trovare applicazione le discipline nazionali dettate, avendo principalmente a mente i principi della menzionata Convenzione di Strasburgo n. 108/1981[63], oltre ad una serie di altri strumenti i quali pure, sommatisi nel tempo in assenza di una disegno unitario

---

modo di rilevare in R. LATTANZI, *La tutela dei dati personali dopo la ratifica della Convenzione europea sulle banche-dati*, in *DII*, 1990, p. 220, p. 227) – oggi disciplinato agli. artt. 7 e 145 ss., d.lgs. n. 196/2003 – che si affianca (rimanendo tuttavia da essi distinto) ad altre ipotesi (ciascuna delle quali ha un proprio autonomo fondamento) di accesso (anziché a *dati*) a *documenti*: nell'ordinamento italiano, si pensi alle disposizioni contenute nell'art. 119, comma 4, d.lgs. 1° settembre 1993, n. 385 o, con riguardo alla materia delle assicurazioni, alla previsione già contenuta nell'art. 12-*ter*, l. 24 dicembre 1969, n. 990 e ora, parzialmente modificata (a detrimento dei consumatori), nell'art. 146, d.lgs. 7 settembre 2005, n. 209 (*Codice delle assicurazioni*); nel settore pubblico, si pensi alla disciplina contenuta negli artt. 22 ss., l. 7 agosto 1990, n. 241.

58 Profilo, quest'ultimo, assai delicato (e sul quale opportunamente, in sede di revisione della direttiva 95/46/CE, si dovrebbe intervenire), che ha determinato la pronuncia della Corte di giustizia, 7 maggio 2009, C-553/07, *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*, in particolare ai punti 57, 63 e 64.

59 Merita qui ricordare che, coerentemente con quanto riportato nel considerando 68 della direttiva 95/46/CE, solo nel settore delle telecomunicazioni e, quindi, delle comunicazioni elettroniche, si sono introdotte discipline armonizzate a livello europeo in materia di riservatezza e protezione dei dati personali, rispettivamente con le direttive 97/66/CE (poi abrogata) e 2002/58/CE.

60 Come è noto, a far data dall'entrata in vigore del trattato di Maastricht (1° novembre 1993) e sino al 1° dicembre 2009, con il trattato di Lisbona, la struttura istituzionale dell'Unione europea si è articolata su tre "pilastri".

61 V. altresì i considerando 13 e 16. Cfr. P. DE HERT, *Trends in European police and judicial cooperation with regard to data exchange*, in *Panopticon*, Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk, 2004, vol. 25, no 1, (26-56), 38, in *http://www.panopticon-net.org*.

62 Cfr. Corte di giustizia (Grande Sezione), 30 maggio 2006, cause riunite C-317/04 e C-318/04, *Parlamento europeo c. Consiglio dell'Unione europea*, con la quale si sono annullate la decisione del Consiglio 2004/496/CE del 17 maggio 2004 relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (*Passenger Name Record*, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti, e la decisione 2004/535/CE della Commissione 14 maggio 2004 relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti *United States' Bureau of Customs and Border Protection*; Corte di giustizia (Grande Sezione), 10 febbraio 2009, causa C-301/06, *Irlanda/Parlamento europeo, Consiglio dell'Unione europea,* con la quale si è, invece, respinto il ricorso per l'annullamento della direttiva 2006/24/CE del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.

63 Normative arricchite, in taluni ordinamenti, dalle regolamentazioni che hanno tenuto conto della Recommendation R (87) 15 *regulating the use of personal data in the police sector*, 17.9.1987 e della Recommendation R (92) 1 *on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system*. Talvolta normative lacunose: si pensi, rimanendo all'ordinamento italiano, alla (persistente) inerzia nell'adozione dell'allegato C al Codice in materia di protezione dei dati personali, contenente i trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia, da adottarsi con decreto del Ministro della giustizia ai sensi dell'art. 46 d.lgs. n. 196/2003 e con decreto del Ministro dell'interno ai sensi dell'art. 53 d.lgs. n. 196/2003. In materia cfr. il parere del Garante del 10 settembre 2009, in *http://www.garanteprivacy.it doc. web*, n. 1658464 che in passato ebbe a segnalare al Presidente del Consiglio dei ministri e al Ministro della difesa la necessità di un intervento, a livello legislativo e regolamentare, per integrare la normativa che regola attualmente le varie attività di raccolta e utilizzo dei dati da parte dell'Arma dei Carabinieri: cfr. Segnalazione 11 gennaio 2001, in *Bollettino* n. 16/gennaio 2001, p. 27 e doc. *web* n. 1074795.

a livello comunitario (prima ancora che di un quadro regolamentare unitario), hanno fatto riferimento alla Convenzione di Strasburgo quale *standard* minimo ([64]): ciò risulta chiaramente dalle regole che presiedono al funzionamento del Sistema d'informazioni Schengen (SIS e, in prospettiva, SIS II) – istituito a norma del titolo IV della convenzione del 1990 di applicazione dell'accordo di Schengen del 14 giugno 1985 relativo all'eliminazione graduale dei controlli alle frontiere comuni – [65] e del sistema di informazione visti (VIS)[66] o con le quali si sono regolati i flussi informativi necessari al perseguimento delle finalità istituzionali di Europol[67] ed Eurojust[68] o, ancora, inserite nella disciplina convenzionale del trattato di Prüm (sottoscritto il 27 maggio 2005)[69].

In tale ambito, solo tardivamente, e dopo una lunga trattativa, è stata adottata la Decisione quadro 2008/977/GAI[70], invero per controbilanciare l'introduzione a livello comunitario del (tuttora non chiaramente precisato) c.d. principio di disponibilità, secondo il quale le informazioni (anche personali) necessarie per contrastare la criminalità dovrebbero attraversare le frontiere interne dell'Unione europea senza ostacoli[71], e l'adozione della (criticata) direttiva 2006/24/CE in materia di conservazione dei c.d. dati di traffico[72]. Decisione quadro, peraltro, fortemente criticata, già solo in relazione al limitato ambito di applicazione che la connota[73] – confinato ai soli dati trattati all'esito della cooperazione tra autorità degli Stati membri e non esteso ai c.d. "trattamenti domestici" (quelli, cioè effettuati a livello nazionale), né (come risulta espressamente dal considerando 39) a tutti i trattamenti di

---

64 Cfr. P. DE HERT, V. PAPAKONSTANTINOU, C. RIEHLE, *Data protection in the third pillar: cautious pessimism*, in M. MIKE (a cura di), *Crime, rights and the EU: the future of police and judicial cooperation*, Justice, London, 2008, p. 121, p. 162.

65 Cfr. *Acquis* di Schengen di cui all'articolo 1, paragrafo 2, della decisione 1999/435/CE del Consiglio del 20 maggio 1999, in *GUCE* 22.9.2000, p. 1 e ivi cfr. il Capitolo 3 della Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 tra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni dedicato alla «Protezione dei dati personali e sicurezza dei dati nel quadro del sistema d'informazione Schengen», con particolare riferimento agli artt. 115 e 117 per i richiami ai principi della Convenzione di Strasburgo.

66 Cfr. (il testo consolidato del) Regolamento (CE) n. 767/2008 del Parlamento europeo 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 (Regolamento VIS).*

67 V. ora la Decisione del Consiglio del 6 aprile 2009 che istituisce l'Ufficio europeo di polizia (Europol) (2009/371/GAI), in *GUUE* L 121, 15 maggio 2009, p. 37, con particolare riferimento al capo II dedicato ai «Sistemi di trattamento delle informazioni» (e all'art. 27 per il rinvio ai principi della Convenzione di Strasburgo).

68 Cfr. la versione consolidata della decisione 2002/187/GAI del Consiglio, del 28 febbraio 2002, che istituisce Eurojust per rafforzare la lotta contro le forme gravi di criminalità, modificata dalla decisione 2003/659/GAI del Consiglio e dalla decisione 2009/426/JHA del Consiglio, del 16 dicembre 2008, relativa al rafforzamento di Eurojust, con particolare riferimento all'art. 14 per il richiamo dei principi della Convenzione di Strasburgo cui si sono ispirate le Disposizioni del regolamento interno dell'Eurojust relative al trattamento e alla protezione dei dati personali (Testo adottato all'unanimità dal collegio dell'Eurojust nella riunione del 21 ottobre 2004 e approvato dal Consiglio il 24 febbraio 2005), in *GUUE* C 68, 19 marzo 2005, p. 1

69 V. ora Decisione 2008/615/GAI del Consiglio del 23 giugno 2008 *sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera*, in *GUUE* L 210, 6 agosto 2008, p. 1, con particolare riferimento al capo 6 contenente «Disposizioni generali relative alla protezione dei dati» (e all'art. 25 il richiamo alla Convenzione di Strasburgo).

70 Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, *sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale,* pubblicata in *GUUE* L 350, 30 dicembre 2008, p. 60 e destinata ad essere recepita entro il 27 novembre 2010.

71 Principio originariamente introdotto nel Programma dell'Aja, accantonato con la Decisione quadro 2006/960/GAI del Consiglio del 18 dicembre 2006 *relativa alla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge* (in *GUUE* L 386, 29 dicembre 2006, p. 89), ma nuovamente menzionato nel Programma di Stoccolma (punto 4.2.2., p. 18: «Il principio di disponibilità continuerà ad imprimere un notevole slancio a questi lavori»). V. in merito le considerazioni critiche svolte nel Parere del Garante europeo della protezione dei dati (GEPD) *sulla proposta di Decisione quadro del Consiglio sullo scambio di informazioni in virtù del principio di disponibilità* (COM (2005)490 def.), in *GUUE* C 116, 17 maggio 2006, p. 8, in particolare ai punti 27 ss.

72 Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 *riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, in *GUUE* L 105, 13 aprile 2006, p. 54. Direttiva, attualmente in corso di revisione, e sottoposta a (severe) critiche da parte del GRUPPO ARTICOLO 29, *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive*, adottato il 13 luglio 2010, WP 172; per ulteriori riferimenti, cfr. i materiali resi disponibili dalla Commissione europea, in *http://ec.europa.eu/home-affairs/policies/police/police_data_experts_en.htm*.

73 Per ulteriori critiche v. le considerazioni svolte dal Garante europeo della protezione dei dati in tre distinti pareri resi nel corso del processo di approvazione della Decisione quadro (Parere 19 dicembre 2005, in *GUUE* C 47, 25 febbraio 2006, p. 27; 29 novembre 2006, in *GUUE* C 91, 26 aprile 2007, p. 9; 27 aprile 2007, in *GUUE* C 139, 23 giugno 2007, p. 1), di recente ribadite nel parere del 5 ottobre 2010 sull'ordine di protezione europeo e sull'ordine europeo di indagine penale (in *GUUE* C 355, 29 dicembre 2010, p. 1, punti 51 ss.). Analoghi rilievi sono stati sollevati dal Gruppo di lavoro dell'articolo 29 per la protezione dei dati e dal Gruppo di lavoro «polizia e giustizia», *Il futuro della* privacy. *Contributo congiunto alla consultazione della Commissione europea sul quadro giuridico relativo al diritto fondamentale alla protezione dei dati personali*, WP 168, adottato il 1° dicembre 2009, pp. 4, 7 ss. e p. 24 ss.

dati personali effettuati nell'ambito della cooperazione giudiziaria in materia penale e di polizia regolati dagli specifici strumenti sopra menzionati, alla cui regolamentazione (comprensiva di meccanismi di controllo) la Decisione quadro è venuta quindi ad affiancarsi.

6. Dopo Lisbona

Se, come si è accennato, il diritto alla protezione dei dati personali – ormai consolidatosi nel panorama europeo[74] – ha trovato il proprio culmine nella Carta dei diritti fondamentali (e nei Trattati dell'Unione europea), deve tuttavia aggiungersi che la situazione, lungi dall'essere pervenuta ad un assestamento, è in pieno movimento.

Il consolidamento dello Spazio europeo di libertà, sicurezza e giustizia[75] e le modifiche introdotte con il trattato di Lisbona[76] hanno mutato la cornice istituzionale entro la quale il diritto alla protezione dei dati personali è oggi chiamato ad operare all'interno dell'Unione europea, estendendola ben al di là degli angusti confini (del mercato interno) entro i quali la direttiva 95/46/CE è stata costretta [77].Ciò risulta chiaramente dall'art. 16 TFUE, disposizione che (abbandonata la collocazione più "periferica" nella quale la materia della protezione dei dati era confinata con il previgente articolo 286 TCE) trova applicazione generale nelle materie di competenza dell'Unione ([78]).

Il venir meno del c.d. "terzo pilastro" e l'attribuzione della competenza in materia di cooperazione giudiziaria e di polizia all'Unione europea[79] rendono ormai superata la formulazione dell'art. 3, par. 2 della direttiva 95/46/CE, non più coerente, almeno in parte, con la prospettiva schiusa dal trattato di Lisbona. Alla luce di ciò, pur tenendo a mente la peculiarità degli ambiti appena richiamati[80], ma considerando altresì l'intenso utilizzo di dati personali, spesso di natura sensibile, che in essi si realizza – con trattamenti che vieppiù erodono il principio di finalità[81], anche in ragione della

---

74 Cfr. Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, *2010 Report on the Application of the EU Charter of Fundamental Rights*, Brussels, 30.3.2011, COM(2011) 160 final, p. 6.

75 Cfr., per primi riferimenti, D. RINOLDI, *Lo spazio di libertà, sicurezza e giustizia*, Napoli, 2010, *passim*; con particolare riferimento alle interrelazioni con le discipline di protezione dei dati personali, v. le critiche sollevate da F. DUMORTIER, C. GAYREL, Y. POULLET, J. JOURET, D. MOREAU, *La protection des données dans l'espace européen de liberté, de sécurité e de justice*, in *JDE*, 2010, p. 33 ss.

76 In particolare l'art. 87, par. 2, lett. *a*), TFUE, disposizione che, in materia di cooperazione di polizia, rimette al Parlamento europeo e al Consiglio (chiamati a deliberare secondo la procedura legislativa ordinaria) «la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio delle pertinenti informazioni», da svolgersi in conformità ai principi di protezione dei dati personali, pur tenendo conto delle necessarie peculiarità che tali trattamenti richiedono.

77 E non diversamente la direttiva 2002/58/CE, con le forzature che si sono poste in essere con la direttiva 2006/24/CE per la conservazione dei dati di traffico (cui si è fatto cenno in nota 59).

78 La menzionata disposizione prevede che «Parlamento europeo e Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, *nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione*, e le norme relative alla libera circolazione di tali dati», ribadendo che il «rispetto di tali norme è soggetto al controllo di autorità indipendenti» (mio il corsivo). Peraltro grande cautela traspare dalla 20ª Dichiarazione relativa all'art. 16 TFUE secondo cui «La conferenza dichiara che, ogniqualvolta le norme in materia di protezione dei dati personali da adottare in base all'articolo 16 possano avere implicazioni dirette per la sicurezza nazionale, si dovrà tenere debito conto delle caratteristiche specifiche della questione. Rammenta che la legislazione attualmente applicabile (vedasi in particolare la direttiva 95/46/CE) prevede deroghe specifiche al riguardo».

79 Ancorché, proprio in tale ambito, lo *status quo* sia destinato (nei fatti) a sopravvivere per i cinque anni successivi all'entrata in vigore del trattato di Lisbona (arg. *ex* art. 10 del Protocollo n. 36 sulle disposizioni transitorie allegato ai trattati dell'Unione europea).

80 Peraltro ribadita nella 21ª Dichiarazione relativa alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia secondo cui «La conferenza riconosce che potrebbero rivelarsi necessarie, in considerazione della specificità dei settori in questione, norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, in base all'articolo 16 del Trattato sul funzionamento dell'Unione europea».

81 Non solo considerato il crescente accesso ad archivi formati da soggetti private nello svolgimento della propria attività d'impresa da parte di *law enforcement agencies* (volendo usare l'ampia terminologia in uso nel contesto sovranazionale), ma anche per il "via libera" contenuto nell'art. 11, par. 1, lett. *d*), Decisione quadro 2008/977/GAI secondo cui «i dati personali trasmessi o resi disponibili dall'autorità competente di un altro Stato membro possono essere successivamente trattati» per «qualsiasi altra finalità, soltanto previa autorizzazione dello Stato membro che trasmette i dati o con il consenso della persona interessata espresso conformemente alla legislazione nazionale». Cfr. I. ANDOULSI, *Personal Data Protection and the First Implementation Semester of the Lisbon Treaty: Achievements and Prospects*, in *NJECrimL*, 2010, p. 362.

crescente "interoperabilità" degli archivi[82] – si rende più che opportuno un complessivo ripensamento sulla materia – peraltro chiaramente anticipato nella Comunicazione della Commissione europea intitolata *Un approccio globale alla protezione dei dati personali nell'Unione europea* [83] – per quanto non sia affatto scontato che, nell'ambito delle modifiche attese, si riuscirà a porre rimedio al *patchwork* di discipline cui si è fatto cenno nel paragrafo che precede[84]. *Patchwork* che sembra altresì caratterizzare la strategia europea in materia di antiterrorismo[85]: ricompresa anch'essa nel Programma di Stoccolma[86], trova ora svolgimento in più testi (non sempre coordinati) elaborati dalla Commissione [87], sì che una più ordinata regolazione delle forme di cooperazione che riguardano i flussi informativi all'interno dell'Unione europea – ma che pure coinvolgono Paesi terzi[88] –, previa valutazione del loro impatto sui diritti fondamentali e nel rispetto dei principi di protezione dei dati personali, deve essere attentamente considerata[89].

Nel "dopo Lisbona", il diritto alla protezione dei dati personali dovrebbe poi trovare adeguata articolazione – e con diversa procedura legislativa, questa volta radicata nell'art. 39 TUE[90] – anche nei settori della politica estera e della sicurezza comune.

Last but not least (è il caso di dire): il "dopo Lisbona" viene a coincidere con il processo di revisione della direttiva 95/46/CE[91] rispetto alla quale, pur ritenendosi validi i principi generali di

---

82 Cfr. S. PREUSS-LAUSSINOTTE, *L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité*, in *Cultures & Conflits*, Numéro 74, 2009, p. 81; P. DE HERT, S. GUTWIRTH, *Interoperability of police databases within the European Union: an accountable political choice?*, TILT Law & Technology Working Paper Series, n. 001/2006, April 2006, in *http://ssrn.com/abstract=971855*.

83 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, Bruxelles, 4.11.2010, COM(2010) 609 definitivo, punto 2.3.

84 Invero anche tra i *privacy advocates* si riscontrano posizioni diverse: a chi (operando all'interno del Garante europeo per la protezione dei dati) si pronuncia a favore di un *framework* normativo unitario [cfr. H. HIJMANS, A. SCIROCCO, *Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help?*, 46, in *CMLRev*, 1485, p. 1496 ss. (2009)] si oppone chi (dall'osservatorio di Eurojust) ritiene preferibile mantenere il sistema vigente, ormai collaudato [cfr. D. ALONSO BLAS, *Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom*, in *ERA Forum*, 2010, p. 233; EAD., *First Pillar and Third Pillar: Need for a common approach?*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing Data Protection*, Bruxelles, 2009, p. 225].

85 Strategia che, peraltro, si muove nel solco già segnato dal Consiglio dell'Unione europea del 30 novembre 2005 relativo alla strategia antiterrorismo dell'Unione europea, che si articola in quattro linee d'azione principali incentrate sulla "prevenzione" (della radicalizzazione del terrorismo e del reclutamento), sulla "protezione" (dei cittadini europei), sull'azione di investigazione e contrasto al terrorismo e sulla capacità di "risposta" ad eventuali attacchi terroristici (per minimizzarne le conseguenze).

86 Cfr. Consiglio europeo, *Programma di Stoccolma - Un'Europa aperta e sicura al servizio e a tutela dei cittadini*, in *GUUE* C 115, 4 maggio 2010, p. 1, *passim* e, in particolare, punto 4.5.; v. pure Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Creare uno spazio di libertà, sicurezza e giustizia per i cittadini europei. Piano d'azione per l'attuazione del programma di Stoccolma*, Bruxelles, 20.4.2010, COM(2010) 171 definitivo, p. 5 ss. e p. 41 ss.

87 Comunicazione della Commissione al Parlamento europeo e al Consiglio, *La politica antiterrorismo dell'UE: principali risultati e sfide future*, Bruxelles, 20.7.2010, COM(2010) 386 definitivo; Communication on *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, Brussels, 22.11.2010, COM(2010) 673 final; in materia cfr. altresì EU Counter-Terrorism Coordinator (CTC), *EU Action Plan on combating terrorism*, 15893/1/10, Brussels, 17 January 2011. Ma v. le numerose perplessità sollevate dal *Rapporteur* Rita Borsellino nel *Working document on the European Union's internal security strategy*, Committee on Civil Liberties, Justice and Home Affairs, 14.2.2011 e i rilievi sollevati nel Parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio, *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, in *GUUE* C 101, 1 aprile 2011, p. 6, in particolare (salvo gli aspetti di dettaglio, pur trattati nel parere) ai punti 20, 29 e 40.

88 Merita qui segnalare la *press release* dell'Unione europea intitolata *EU-US Negotiations on an agreement to protect personal information exchanged in the context of fighting crime and terrorism*, Brussels 29 marzo 2011, MEMO/11/203, con la quale è stata resa pubblica la formale apertura delle negoziazioni tra Unione europea e Stati Uniti d'America per il raggiungimento di un «agreement to protect personal information exchanged in the context of fighting crime and terrorism», iniziativa che fa seguito ai *Reports* presentati dall'*High Level Contact Group (HLCG) on information sharing and privacy and personal data protection*, Brussels, 23 November 2009 (in *http://register.consilium.europa.eu/pdf/en/09/st15/st15851.en09.pdf*).

89 Utile premessa è la ricognizione dei trattamenti in essere che, effettuata per la prima volta, si può rinvenire ora nella Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia*, Bruxelles, 20.7.2010, COM(2010)385 definitivo (ed ivi v. ampi riferimenti ai principi di protezione dei dati personali al punto 4).

90 «Conformemente all'articolo 16 del Trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo [i.e. in materia di politica estera e di sicurezza comune], e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti».

91 Processo attivatosi con la consultazione pubblica del luglio 2009 (in *http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm*), i cui esiti sono sintetizzati nel *Summary of replies to the public consultation about the future legal framework for protecting personal data*, Brussels, 4 November 2010

protezione dei dati personali, si sono tuttavia messi in luce sia la parziale armonizzazione conseguita – di tal che non sarebbe peregrino interrogarsi circa il ruolo effettivamente svolto dalla Commissione europea nel corso di questi anni nell'attivare i necessari procedimenti di infrazione per inosservanza o errata applicazione della direttiva[92] – sia gli effetti profondi sui trattamenti di dati personali determinati dallo sviluppo delle tecnologie della comunicazione, anzitutto *internet*[93], come pure dalla dimensione accentuatamente globalizzata dell'economia, sì che – in particolare sotto la pressione esercitata dalle multinazionali – la disciplina relativa al diritto nazionale applicabile[94] come quella relativa al flusso transfrontaliero dei dati personali potrebbero subire dei ritocchi[95]. Sono queste le punte dell'*iceberg* che, in assenza di una più larga convergenza su scala globale sui principi ispiratori della materia, i richiami (o le esortazioni) alla *privacy by design* e *by default* e ad un rinvigorimento delle autorità di controllo (nella dimensione nazionale e nelle forme di cooperazione reciproca) possono solo in parte contribuire ad evitare e che oggi minacciano il bene più prezioso che il diritto alla protezione dei dati personali, nel suo lungo (e mai agevole) cammino, ha inteso assicurare: quello dell'*effettività*, al di là del pur necessario riconoscimento nelle *black letters of law*, nella protezione dei diritti fondamentali suo tramite tutelati.

Nel Programma di Stoccolma si legge che «l'Unione deve garantire una strategia globale in materia di protezione dei dati all'interno dell'Unione e nell'ambito delle relazioni con i paesi terzi»[96].

Solo il tempo dirà se questo ambizioso obiettivo potrà essere conseguito o se "la montagna partorirà il (proverbiale) topolino".

Ciò che oggi si può affermare è che la traiettoria del diritto alla protezione dei dati personali – che nell'economia del presente intervento si è qui potuta solo per sommi capi tratteggiare – è tutt'altro che esaurita. Nel contesto europeo e transatlantico, il dibattito, ora alimentato dalle sole considerazioni generali (e talvolta generiche) contenute nella Comunicazione, è vivissimo[97], attualizzato dall'analisi di maggior dettaglio che è seguita alla presentazione delle proposte legislative da parte della stessa Commissione che andranno a comporre il nuovo quadro giuridico globale per la protezione dei dati personali nell'UE[98].

(*http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf*), e con ulteriori, più mirate, attività intraprese sia dalla Commissione europea, sia nell'ambito del Parlamento europeo. A questo processo ha preso parte anche il Gruppo articolo 29, *The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, adottato il 1° dicembre 2009, WP 168.

92 Troppo spesso, specie nel formulare critiche alla direttiva 95/46/CE rispetto alla parziale armonizzazione suo tramite conseguita, si dimentica (al di là del vizio "genetico", segnalato in nota 48) che le diverse "risposte" a livello nazionale derivano dall'applicazione del principio di liceità del trattamento, che esige una valutazione effettuata alla luce dell'ordinamento giuridico nazionale, non necessariamente armonizzato a livello europeo, sì che eventuali discrasie non possono non ripercuotersi, in seconda battuta, sui profili connessi (alla liceità del) trattamento dei dati personali. Per altro verso le critiche sono ingenerose (e, in fondo, poco lungimiranti) rispetto alla tecnica normativa, per norme e clausole generali, seguita dalla direttiva 95/46/CE, fattore che ne ha assicurato la longevità (nonostante i profondi mutamenti tecnologici). A quest'ultimo riguardo, vero è, semmai, che in alcuni contesti sarebbe stato necessario (e tuttora sarebbe più che auspicabile) introdurre discipline armonizzate di settore a livello europeo (come si è sopra segnalato in nota 30): un macro settore (tra i tanti) è certo quello del trattamento dei dati riferiti ai lavoratori, specie in relazione all'utilizzo delle tecnologie dell'informazione e della comunicazione (profilo peraltro sollevato in passato dall'Article 29 data protection working party, *Opinion 8/2001 on the processing of personal data in the employment context*, 13 September 2001, WP 48): sia consentito in merito rinviare a R. LATTANZI, *Dallo statuto dei lavoratori alla disciplina di protezione dei dati personali*, in *RIDL*, 2011, I, p. 147, p. 154 ss.

93 Limiti manifestatisi in Corte di giustizia, 6 novembre 2003, *Lindquist c. Svezia* (C-101/01). Ma *data protection*, *privacy*, *security* e *control* sono *buzzwords* che compaiono in ogni studio in materia: cfr. da ultimo OXFORD INTERNET INSTITUTE, *Towards a Future Internet. Interrelation between Technological, Social and Economic Trends*, Final Report for DG Information Society and Media, European Commission DG INFSO Project SMART 2008/0049, November 2010, *passim* (in *http://cordis.europa.eu/fp7/ict/fire/docs/tafi-final-report_en.pdf*).

94 Cfr. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 8/2010 on applicable law*, 16 December 2010, WP 179.

95 In particolare, quanto accaduto a livello nazionale in taluni Stati membri (tra cui l'Italia, dando seguito alla segnalazione del Garante al Parlamento e al Governo in materia di trasferimento di dati personali in paesi terzi e norme vincolanti d'impresa dell'8 novembre 2007, doc. *web* n. 1467485) – dando autonoma rilevanza alle c.d. *binding corporate rules* – potrebbe ripetersi anche a livello europeo.

96 Consiglio europeo, *Programma di Stoccolma*, cit. punto 2.5.

97 Come peraltro attestato dalla presentazione del *Commercial Privacy Bill of Rights Act of 2011*, recente proposta legislativa *bipartisan* presentata dagli (influenti) senatori Kerry e McCain contenente non pochi dei principi tradizionali di protezione dei dati personali, dalla quale traspare altresì il dibattito europeo in materia (come, ad esempio, il richiamo ai *minimization* e *accountability principles*).

98 Sono state presentate la Proposta di Regolamento del Parlamento europeo e del Consiglio *concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati),* COM(2012) 11 final, Bruxelles, 25.1.2012 nonché la Proposta di Direttiva del Parlamento europeo e del Consiglio *concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati*, COM/2012/010 final, Bruxelles, 25.1.2012. Non è possibile in questa sede soffermarsi nell'analisi

C'è da augurarsi che all'interno dell'ordinamento italiano la discussione (in questa rinnovata fase ascendente) non segni (ancora una volta) il passo[99].

delle Proposte. Deve però segnalarsi che le stesse hanno già formato oggetto di significativi rilievi critici (anche) da parte dell'Article 29 Data Protection Working Party, WP 191, *Opinion 01/2012 on the data protection reform proposals*, adopted on 23 March 2012, in *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf*; riserve sono state anche espresse nell'*Opinion of the European Data Protection Supervisor on the data protection reform package*, 7 marzo 2012, in *http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/OpinionsC*.

[99] Conviene qui tenere a mente il monito di S. RODOTÀ, *Diritti e libertà nella storia d'Italia. Conquiste e conflitti. 1861-2011*, Roma, 2011, p. 141 s.:«la cultura della *privacy* è fragile, le norme alle quali si affida sono sempre esposte a strumentalizzazioni e restrizioni, provenienti soprattutto da imperativi di sicurezza e pressioni di mercato. Le speranze in essa riposte rischiano d'essere deluse senza una convinta e continua attenzione istituzionale, indispensabile per mantenere e rafforzare la fiducia dei cittadini».

II. CRIMINALITÀ INFORMATICA *VS* DIRITTO ALLA RISERVATEZZA E PROTEZIONE DEI DATI PERSONALI. I LEGISLATORI (EUROPEO E NAZIONALE) ALLA RICERCA DEL GIUSTO PUNTO DI EQUILIBRIO NELL'EPOCA DELLA GLOBALIZZAZIONE DIGITALE

di Valeria Scalia

1. Considerazioni introduttive

La progressiva ed inarrestabile diffusione delle tecnologie informatiche e l'utilizzo crescente e massivo della rete *internet* in tutti i settori della vita professionale, sociale e privata delle persone, con il conseguente scambio di milioni di dati e informazioni relativi agli aspetti più disparati delle esistenze dei soggetti che si avvalgono di tali strumenti, hanno determinato una vera e propria rivoluzione copernicana che non poteva non ripercuotersi sui profili giuridici coinvolti sia a livello nazionale, ma probabilmente con una maggiore forza d'urto – considerata la peculiare e innata transnazionalità delle reti informatiche e telematiche – a livello europeo, richiedendo ai rispettivi legislatori di confrontarsi con problematiche del tutto nuove, caratterizzate inoltre dalla necessità di essere in possesso di una serie di puntuali conoscenze e competenze scientifiche, e in continua e rapidissima evoluzione.

In particolare, nella prospettiva del penalista, il compito sembra essere particolarmente arduo, in quanto si debba tener conto della circostanza che alla innegabile utilità e funzionalità sotto diversi profili di tali strumenti si accompagna inevitabilmente un ampliamento delle occasioni di commissione di reati, sia che si tratti di comportamenti lesivi già costituenti reato, rispetto ai quali le nuove tecnologie rappresentino soltanto una nuova modalità di realizzazione ovvero un diverso oggetto materiale della condotta, sia che si tratti, di contro, di ipotesi esclusivamente perpetrabili nell'ambito dello spazio informatico. In effetti, occorre da una parte non sottovalutare le esigenze di sicurezza e difesa sociale derivanti dalla non trascurabile possibilità che i nuovi mezzi messi a disposizione dalla rete rendano maggiormente semplice – ed in molti casi molto più pericolosa – la commissione di talune condotte illecite particolarmente allarmanti (si pensi, a titolo esemplificativo, alla criminalità organizzata o al terrorismo); tuttavia, bisogna anche valutare la necessità di tutelare la riservatezza dei dati immessi dagli utenti in rete e di evitare di limitare incondizionatamente la possibilità di questi ultimi di realizzare la propria personalità nell'ambito dello spazio informatico. Il bilanciamento di tali contrapposte esigenze da parte dei legislatori nazionale ed europeo ha rappresentato e continua a rappresentare indubbiamente un difficile banco di prova, sul quale incide pesantemente anche la necessità di doversi continuamente evolvere in seguito ai progressivi aggiornamenti delle nuove tecnologie.

Alla luce delle predette considerazioni, ci si propone di analizzare gli sforzi compiuti dal legislatore europeo in ordine all'individuazione di tale corretto bilanciamento, delineando gli strumenti adottati ed adottandi nell'ambito della tutela della riservatezza e della protezione dei dati personali e valutando la rispondenza a tali principi delle scelte di criminalizzazione operate recentemente dal legislatore con la direttiva 2013/40/UE, con specifico riguardo agli attacchi ai sistemi d'informazione. Si passerà poi a considerare la compatibilità del quadro normativo italiano rispetto alle istanze promananti dal legislatore sovrannazionale, tenendo conto dell'opera ermeneutica già svolta dalla giurisprudenza nazionale, vagliando eventuali interventi da porre in essere prima della scadenza del termine imposto dalla stessa direttiva (4 settembre 2015) nell'ottica di cogliere l'opportunità offerta dal

recepimento della normativa comunitaria per operare un eventuale riassetto maggiormente sistematico e razionale della materia in esame.

2. La tutela della riservatezza e la protezione dei dati personali nell'ambito dell'Area di libertà, sicurezza e giustizia dell'Unione europea

Muovendo dalle conclusioni delineate nel Programma di Stoccolma[100] e nel successivo Piano di azione[101] dello stesso, risulta chiaro come l'Unione europea abbia posto proprio come suo obiettivo primario una strategia globale in materia di protezione dei dati all'interno dell'Unione e nell'ambito delle relazioni con i Paesi terzi, nell'ottica di prevedere e regolare le circostanze in cui sia giustificato l'intervento dei pubblici poteri nell'esercizio di tali diritti ed applicare al contempo i principi relativi alla protezione dei dati nella sfera privata; e più in dettaglio, nello stabilire principi di base quali la limitazione delle finalità, la proporzionalità, la legittimità del trattamento, la durata limitata della conservazione, la sicurezza e riservatezza ed il rispetto dei diritti della persona, il controllo affidato ad organi nazionali di vigilanza indipendenti e l'accesso ad effettivi mezzi di ricorso giurisdizionale.

Nonostante la legislazione sovrannazionale esistente in materia non sia particolarmente rispondente a tali requisiti, in quanto essa non prevede limiti stringenti allo scambio di dati, così come previsto dalla decisione-quadro 2008/977/GAI, che tra l'altro ha ad oggetto esclusivamente il trattamento transfrontaliero dei dati e non si estende invece alle attività di trattamento effettuate dalla polizia e dalle autorità giudiziarie a livello nazionale, con la conseguente difficoltà per le forze di polizia e le altre autorità competenti di individuare esattamente il carattere puramente nazionale o transfrontaliero di un determinato trattamento o di prevedere il futuro scambio transfrontaliero di cui dati originariamente nazionali possano costituire oggetto[102], l'obiettivo enunciato nel Programma di Stoccolma può trovare, dopo l'entrata in vigore del Trattato di Lisbona, una rispondenza immediata nella Carta dei diritti fondamentali dell'Unione (d'ora in poi: Carta), in particolare negli articoli 7[103] e 8[104], ove trovano esplicita protezione rispettivamente il diritto al rispetto della vita privata e familiare (nonché del domicilio e delle comunicazioni) ed il diritto alla protezione dei dati di carattere personale, che sulla base della disposizione di cui all'art. 6 del TUE hanno ormai lo stesso valore giuridico dei Trattati, spiegando dunque la loro vincolatività giuridica non solo nei confronti dell'Unione (*rectius*: della normativa da essa adottata), ma anche rispetto agli Stati membri nell'attuazione del diritto dell'Unione (art. 51, par. 1, Carta).

Va sottolineato inoltre che un ulteriore riconoscimento, che potremmo definire costituzionale, dell'imprescindibilità del rispetto di tali diritti nell'ambito della costruzione europea si ritrova nell'art. 16 TFUE[105], che rappresenta la nuova base giuridica per l'adozione di tutti gli atti normativi dell'Unione aventi come obiettivo la tutela dei dati personali.

---

100 Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Uno spazio di liberta`, sicurezza e giustizia al servizio dei cittadini*, adottata a Bruxelles il 10 giugno 2009, COM(2009) 262 def.

101 *Programma legislativo e di lavoro della Commissione europea per il 2010 e Programma di 18 mesi del Consiglio dell'Unione europea presentato dalle Presidenze spagnola, belga e ungherese*, COM(2010)135 def.

102 Decisione quadro 2008/977/GAI del 27 novembre 2008 *sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale*, (*GUUE* L 350, 30 dicembre 2008, p. 60] che inoltre lascia un ampio margine di discrezionalità ai legislatori degli Stati membri nell'attuazione delle sue disposizioni e non prevede alcun meccanismo o gruppo consultivo analogo al Gruppo di lavoro articolo 29 volto a promuovere un'interpretazione comune delle sue disposizioni e non conferisce competenze esclusive alla Commissione per garantire un approccio attuativo comune.

103 Art. 7 - Rispetto della vita privata e della vita familiare - «Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni».

104 Art. 8 - Protezione dei dati di carattere personale - 1. «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano». 2. «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. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica». 3. «Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

105 Art. 16 - 1. «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano». 2. «Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte

Il particolare impegno delle istituzioni sovrannazionali nel raggiungimento di questo ambizioso obiettivo è testimoniato inoltre dall'adottando *pacchetto normativo*, composto dalla proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (Regolamento generale sulla protezione dei dati)[106] e dalla proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati[107] - di recente approvati in prima lettura dal Parlamento europeo[108] -, che andranno a sostituire rispettivamente la direttiva 95/46/CE – definita dalla stessa Relazione alla proposta di regolamento come «pietra angolare nell'impianto della vigente normativa dell'UE in materia di protezione dei dati personali» - e la decisione quadro 2008/977/GAI – strumento generale applicabile per proteggere i dati personali nei settori della cooperazione giudiziaria e di polizia in materia penale. Tale nuovo assetto normativo si propone di rispondere all'esigenza – già evidenziata in ambito europeo in diversi importanti documenti di *soft law*[109] - di instaurare un quadro giuridico più solido e coerente in materia che, accanto ad efficaci misure di attuazione, garantisca alle persone fisiche il controllo dei loro dati personali, rafforzando contestualmente la certezza giuridica e operativa per i soggetti economici e le autorità pubbliche[110].

Accanto a tale rassicurante prospettiva *de iure condendo* del quadro normativo sovrannazionale, un approccio altrettanto serio e razionale alla materia del rispetto del diritto alla riservatezza e alla protezione dei dati personali è stato assunto dalla CGUE, che ha da ultimo dichiarato l'invalidità della direttiva 2006/24/CE in materia di conservazione dei dati personali[111] per contrasto con gli articoli 7 e 8 della Carta[112]. Si tratta di una pronuncia particolarmente interessante, in quanto essa ricostruisce i passaggi logico-argomentativi che la conducono alla dichiarazione d'invalidità tenendo in precipua considerazione i diritti fondamentali tutelati dalla Carta, che rappresentano il parametro sulla base del quale essa valuta la legittimità della normativa comunitaria soggetta al suo vaglio. Il ragionamento intessuto dalla Corte muove dalla considerazione che la direttiva 2006/24/CE incide in maniera penetrante e generalizzata sul diritto di tutti i cittadini dell'Unione al rispetto ed alla protezione dei propri dati personali, senza alcuna limitazione dell'obbligo di conservazione da essa imposto con riguardo ai dati di soggetti per i quali esistano fondate ragioni per ritenere che possano porre in essere in un prossimo futuro condotte criminose[113]. Inoltre, nonostante l'atto normativo abbia come obiettivo secondario – accanto a quello dell'armonizzazione delle legislazioni degli Stati membri, indicato come

---

degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti».
Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del Trattato sull'Unione europea.

106 COM(2012) 11 definitivo.

107 COM(2012) 10 definitivo.

108 Si vedano i testi approvati in prima lettura dal Parlamento europeo il 12 marzo 2014, rispettivamente P7_TA-PROV(2014) 212 e P7_TA-PROV(2014) 219.

109 Si vedano in questo senso la Comunicazione della Commissione su *Un approccio globale alla protezione dei dati personali nell'Unione europea* COM(2010) 609 definitivo, in cui si dichiara espressamente che «Obiettivo della presente comunicazione è definire l'approccio della Commissione per modernizzare il quadro giuridico dell'UE che disciplina la protezione dei dati personali in tutti i settori di attività dell'Unione, tenendo conto in particolare delle sfide generate dalla globalizzazione e dalle nuove tecnologie in modo da continuare a garantire un elevato livello di protezione delle persone fisiche con riguardo al trattamento dei dati personali in quei settori. L'Unione europea continuerà così a svolgere un ruolo trainante nel promuovere norme elevate di protezione dei dati nel mondo intero» e la Comunicazione della Commissione su *Europa 2020. Una strategia per una crescita intelligente, sostenibile ed inclusiva* COM(2010) 2020, che mira in particolare a rafforzare la diffusione e l'efficienza delle reti informatiche, nell'ottica di migliorare il loro utilizzo in campo imprenditoriale e professionale e rimanda all'attuazione dell'Agenda digitale europea COM(2010) 245 def.

110 D. BIGO, S. CARRERA, G. GONZÁLES FUSTER, E. GUILD, P. DE HERT, J. JEANDESBOZ, V. PAPAKONSTANTINOU, *Towards a New Legal Framework for Data Protection and Privacy*, *Challenges, Principles and the Role of the European Parliament*, European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, in *http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/453216/IPOL-LIBE_ET(2011)453216_EN.pdf*.

111 Direttiva del Parlamento europeo e del Consiglio, del 15 marzo 2006, *riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, in *GUUE* L 105, 13 aprile 2006, p. 54

112 CGUE, Grande Sezione, 8 aprile 2014, *Digital Rights Ireland Ltd.* e *Seitlinger ed altri*, cause riunite C-293/12 e C-594/12.

113 CGUE, Grande Sezione, 8 aprile 2014, *Digital Rights Ireland Ltd.* e *Seitlinger ed altri*, cit., punto 57.

primario – quello della lotta contro i crimini gravi e della salvaguardia della sicurezza dei cittadini europei, esso non richiede alcuna relazione tra i dati per i quali sussiste l'obbligo di conservazione e l'esistenza di una minaccia alla sicurezza pubblica, in particolare non prevedendo puntuali limitazioni di tale obbligo con riguardo ai dati relativi a un periodo di tempo circoscritto o ad una delimitata zona geografica o ancora a una ristretta cerchia di soggetti, in qualche modo probabilmente coinvolti in attività criminose di una certa gravità, ovvero con riguardo a specifici soggetti che potrebbero per altre ragioni contribuire alla prevenzione, all'investigazione o al perseguimento di gravi crimini[114]. Secondo la Corte, la direttiva non prevede criteri certi attraverso i quali delineare i limiti di accesso ai dati conservati da parte della autorità competenti o regolare il loro successivo utilizzo per gli scopi di prevenzione, investigazione e perseguimento dei reati[115], che, proprio nell'ottica di bilanciare l'incisività dell'interferenza nel godimento dei diritti tutelati dalla Carta determinata dall'obbligo di conservazione imposto dalla direttiva, dovrebbero essere caratterizzati da una particolare gravità. Di contro, le disposizioni della direttiva operano un generico riferimento alla criminalità grave, così come definita dalle legislazioni degli Stati membri.

La previsione dell'art. 6 della predetta direttiva, inoltre, impone che i dati elencati nell'art. 5 della stessa siano conservati per un periodo che non può essere inferiore a sei mesi e non deve superare i due anni, senza operare tuttavia alcuna distinzione tra i dati elencati nella predetta disposizione, né richiedere che la determinazione del periodo di conservazione debba essere basata su criteri oggettivi che assicurino la stretta necessità dell'obbligo imposto. La mancanza nel corpo della direttiva, dunque, di indicazioni precise volte a restringere l'ambito di operatività delle penetranti interferenze nel godimento dei diritti protetti dagli artt. 7 e 8 della Carta a quanto strettamente necessario in ordine alla realizzazione dell'obiettivo di interesse generale perseguito, ossia la prevenzione, l'investigazione ed il perseguimento della criminalità, rende l'intero contenuto della direttiva contrastante con il principio di proporzionalità, delineato nell'ambito delle c.d. clausole orizzontali della Carta, ed in particolare nell'art. 52, par. 1, secondo cui «Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.»[116]. Tali conclusioni risultano ulteriormente avallate, nell'ottica della Corte, dalla circostanza per la quale la stessa direttiva non prevede sufficienti garanzie idonee ad assicurare la sicurezza e la protezione dei dati conservati dal rischio di abusi o di accessi non autorizzati, in quanto non contiene regole precise e puntuali volte a tutelare l'integrità e la riservatezza dei dati raccolti, nonostante la massività della raccolta, la *sensibilità* di taluni dati e il forte rischio derivante pertanto da accessi illegali a questi ultimi. Essa inoltre non garantisce la distruzione definitiva dei dati raccolti una volta trascorso il periodo di conservazione indicato dall'art. 6 e non richiede che i dati siano custoditi in banche dati presenti all'interno dell'Unione europea, con la conseguenza di escludere qualsiasi forma di controllo su di essi da parte di un'autorità indipendente all'interno del territorio europeo, così come stabilito in un'ottica garantistica dall'art. 8, par. 3, della Carta[117].

La sentenza della CGUE contiene affermazioni particolarmente importanti sia con riguardo alla materia della protezione dei dati personali dei cittadini europei – che come abbiamo avuto modo di constatare rappresenta una priorità nell'agenda europea degli ultimi anni -, richiedendo al legislatore sovrannazionale di corredare le norme che hanno un'incidenza penetrante sul diritto alla riservatezza e sulla protezione delle informazioni e dei dati personali di garanzie adeguate e puntuali, in ordine alla

114 CGUE, Grande Sezione, 8 aprile 2014, *Digital Rights Ireland Ltd.* e *Seitlinger ed altri*, cit., punti 58-59.

115 Non viene previsto inoltre dal testo della direttiva alcun obbligo per le autorità nazionali competenti all'accesso ai dati conservati di richiedere una previa autorizzazione all'autorità giudiziaria ovvero ad altra autorità amministrativa indipendente, debitamente motivata da fondate ragioni relative alla prevenzione, investigazione e perseguimento dei reati, cfr. CGUE, Grande Sezione, 8 aprile 2014, *Digital Rights Ireland Ltd.* e *Seitlinger ed altri*, cit., punto 62.

116 Sul principio di proporzione nella giurisprudenza della Corte di giustizia, cfr. A.M. MAUGERI, *Il principio di proporzione nelle scelte punitive del legislatore europeo: l'alternativa delle sanzioni amministrative comunitarie*, in G. GRASSO, L. PICOTTI, R. SICURELLA (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, p. 67 ss., in particolare pp. 90-98.

117 CGUE, Grande Sezione, 8 aprile 2014, *Digital Rights Ireland Ltd.* e *Seitlinger ed altri*, cit., punti 63-69.

loro integrità e sicurezza, in modo tale da limitare le interferenze nel godimento di tali diritti allo stretto indispensabile per il raggiungimento di ulteriori finalità di interesse generale; sia, più in generale, con riguardo al controllo giurisdizionale operato dalla stessa Corte sulla normativa europea in base al parametro dei diritti fondamentali. Sembra infatti di poter cogliere nel ragionamento sviluppato dalla Corte un approccio maturo e razionale - già ampiamente, e probabilmente in maniera più puntuale ed argomentata, delineato nelle Conclusioni dell'Avvocato generale Cruz Villalón ed in parte mutuato dai numerosi arresti giurisprudenziali, principalmente in materia di art. 8 CEDU[118], della Corte di Strasburgo, richiamati sia nelle Conclusioni dell'Avvocato generale, sia nelle motivazioni della Corte – al ruolo di *controllore* del rispetto dei diritti fondamentali da parte del legislatore europeo, dimostrato dall'attenta riflessione riservata all'analisi delle singole disposizioni della direttiva ed alla loro rispondenza ai principi di stretta necessità e proporzionalità rispetto agli obiettivi perseguiti, attraverso un minuzioso esame delle lacune presenti nel testo della direttiva alla luce del precipuo interesse alla protezione dei diritti fondamentali. La Corte dunque sottopone a dura e severa critica il bilanciamento tra interessi contrapposti (prevenzione, investigazione e perseguimento dei reati, da una parte, e riservatezza e protezione dei dati personali, dall'altra) operato dal legislatore europeo, ammonendolo anche con riguardo alla scelta deresponsabilizzante di delegare alle legislazioni nazionali il compito di fissare le limitazioni alle interferenze nel godimento dei diritti fondamentali derivanti dall'attuazione delle disposizioni sovrannazionali, così evidentemente ritenendo secondaria – se non del tutto marginale - la necessaria armonizzazione anche di tali imprescindibili profili, accanto a quelli concernenti l'imposizione degli obblighi di conservazione idonei a realizzare la finalità di sicurezza perseguita[119].

Di particolare interesse risulta inoltre la puntuale analisi condotta dalla Corte sulle disposizioni della direttiva, in quanto essa non si limita ad enunciarne le lacune, ma indica altresì quali accorgimenti avrebbero reso le disposizioni del testo normativo compatibili con il rispetto dei diritti fondamentali (anche alla luce delle indicazioni provenienti dalla giurisprudenza di Strasburgo), così fornendo al legislatore europeo una serie di preziosi suggerimenti per la futura redazione di una nuova legislazione in materia, maggiormente rispondente alla tutela dei diritti dei cittadini europei.

Con la predetta pronuncia la CGUE sembra confermare la positiva tendenza, già delineata nelle sentenze *Fransson*[120] e *Melloni*[121], a valorizzare il suo ruolo di controllo sulla normativa europea e su quella nazionale - nei limiti, ancora a dire il vero non precisamente delineati, tracciati dall'art. 51, par. 1, della Carta – alla luce dei diritti fondamentali e dei principi di necessità e proporzionalità, operando un proficuo richiamo delle linee ermeneutiche già indicate nella giurisprudenza della Corte EDU, in tal modo mostrando – in maniera progressivamente più evidente – l'intento di rilanciare il proprio ruolo di *garante costituzionale* attraverso il sindacato sul rispetto dei diritti fondamentali, in una prospettiva tuttavia di continuo e proficuo dialogo con le altre Corti deputate al medesimo ruolo, ossia la Corte EDU e le Corti costituzionali nazionali.

Un ultimo cenno merita la risposta in senso positivo dell'Avvocato generale alla questione relativa agli obblighi, gravanti sui giudici nazionali, di esaminare e valutare la compatibilità dei provvedimenti nazionali di trasposizione di una direttiva con le garanzie previste dalla Carta, sulla quale la Corte non si è di contro pronunciata. Probabilmente la laconica risposta dell'Avvocato generale è dovuta, da una parte, all'inutilità di maggiori indicazioni in merito, considerata la necessità valutata dal giudice

---

118 Per una puntuale disamina della giurisprudenza della Corte EDU in materia di protezione dei dati personali *ex* art. 8 CEDU in rapporto alle esigenze di prevenzione, investigazione e perseguimento della criminalità, e delle conseguenze da trarne per il legislatore europeo, cfr. R. SICURELLA, V. SCALIA, *Data mining and Profiling in the Area of Freedom, Security and Justice. State of Play and New Challenges in the Balance between Security and Fundamental Rights Protection*, in *NJECrimL*, 2013, 4, p. 432 ss. Si veda anche, con riguardo al bilanciamento tra investigazioni ad alto contenuto tecnologico e diritti fondamentali della persona, R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* Online Durchsuchung. *La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona*, in *RTDPE*, 2009, 3, p. 695 ss.

119 Ci sia consentito il rinvio a V. SCALIA, *Controllo giurisdizionale su necessità e proporzione delle scelte di criminalizzazione del legislatore europeo: uno sguardo sulle possibilità di dialogo tra le Corti europee*, in G. GRASSO, G. ILLUMINATI, R. SICURELLA, S. ALLEGREZZA, *Le sfide dell'attuazione di una Procura europea: definizione di regole comuni e loro impatto sugli ordinamenti interni*, Milano, 2013, p. 342 ss.

120 CGUE, 26 febbraio 2013, *Aklagaren c. Hans Akerberg Fransson,* causa C-617/10.

121 CGUE, Grande Sezione, 26 febbraio 2013, *Melloni,* causa C-399/11.

nazionale di far ricorso in via pregiudiziale alla Corte, dall'altra, alla superfluità di un nuovo esame di una questione già risolta positivamente dalla Corte nella recente sentenza *Fransson*, richiamata anche dallo stesso Avvocato generale.

Meno chiari sembrano gli effetti immediati che la dichiarazione di invalidità della direttiva spiegherà, in attesa che il legislatore europeo raccolga i suggerimenti forniti della Corte e formuli nuove disposizioni in materia, ma non è possibile procedere ad un'analisi di essi in questa sede.

3. Il contrasto della criminalità informatica nel contesto europeo

Il rilievo attribuito nell'ambito dell'attuale costruzione europea al diritto alla riservatezza e alla protezione dei dati personali e le prospettive *de iure condendo* testimoniano la particolare rilevanza e meritevolezza che essi assumono agli occhi del legislatore europeo, in quanto possibili beni giuridici oggetto di una specifica tutela penale. Va rilevato altresì che l'entrata in vigore del Trattato di Lisbona ha impresso una forte accelerazione al processo di creazione di *norme minime* di matrice europea relative alla definizione dei reati e delle relative sanzioni, introducendo per talune forme di criminalità, tra le quali figura anche la criminalità informatica, - definite particolarmente gravi, che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni - una sorta di presunzione di necessità di tale intervento sovrannazionale (art. 83, par. 1, TFUE).

L'esigenza, tuttavia, di prevedere strumenti normativi a livello europeo volti ad armonizzare – talvolta anche attraverso l'introduzione di apposite fattispecie incriminatrici ad opera dei legislatori nazionali – le legislazioni penali degli Stati membri in materia di criminalità informatica era stata già avvertita ben prima dell'entrata in vigore del Trattato di Lisbona, che rappresenta - potremmo dire – il punto di approdo di un lungo cammino iniziato negli ultimi anni '80 nell'ambito del Consiglio d'Europa con la Raccomandazione n. 9 (89) 9[122] ed il Rapporto finale del Comitato europeo sui problemi concernenti la criminalità informatica, che evidenziava già i rischi derivanti dalla diffusione delle nuove tecnologie e prevedeva una lista minima di reati informatici (*computer-related offences*) da introdurre negli Stati membri, proprio sul presupposto del carattere transnazionale di tali condotte e della conseguente opportunità di armonizzare le legislazioni penali nazionali intorno a *standard* minimi di tutela.

Sempre nell'ambito del Consiglio d'Europa, più di recente, è intervenuta la Convenzione *Cybercrime*, approvata a Budapest il 23 novembre 2001 e promossa per rafforzare e adeguare gli strumenti di diritto penale sostanziale e processuale, nonché la cooperazione giudiziaria e di polizia, diretti a contrastare non solo la criminalità informatica nelle sue nuove dimensioni e caratteristiche globali, ma anche quella *comune* che utilizzi come mezzo la rete, in quanto essa si applica non soltanto ai reati da essa stessa definiti – denominati da una parte della dottrina *cibernetici in senso proprio* -, ma anche a

[122] Council of Europe, European Committee on Crime Problems, *Computer-related Crime. Recommendation n. 9 (89) 9 on computer-related crime and final report of the European Committee on Crime Problems*, Strasbourg 1990, in particolare per la lista minima di reati si veda p. 33 ss. Lo studio condotto aveva un approccio in parte criminologico, preoccupandosi di descrivere preliminarmente il fenomeno dei reati informatici, ed in parte dogmatico, constatando la mancanza di una definizione generale di criminalità - volutamente non colmata nell'ottica di lasciare agli Stati la massima libertà di introdurre le fattispecie elencate nella lista minima, al di là di una definizione condivisa di criminalità informatica – e delineando le singole fattispecie in modo da evidenziarne l'oggetto della tutela, le modalità di realizzazione e le eventuali perplessità esistenti con riguardo ad ipotesi già esistenti in taluni Stati ovvero a potenziali sovrapposizioni tra le fattispecie previste. In Italia, il predetto documento è stato in parte attuato attraverso la legge 23 dicembre 1993, n. 547, che ha profondamente innovato l'impianto del nostro codice penale, prevedendo una sorta di *microsistema* di fattispecie tendenti al contrasto della criminalità informatica «in una molteplicità di manifestazioni considerate ormai "classiche" (quali le frodi, le falsificazioni, i danneggiamenti, gli accessi abusivi, le intercettazioni), ha cercato di operare seguendo un disegno più sistematico, integrando e modificando il codice penale e – più limitatamente quello di procedura penale, con norme inserite nei diversi titoli seguendo criteri che le rendessero il più possibile *assimilabili* al tessuto preesistente», cfr. L. PICOTTI, Internet *e il diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *DInt,* 2, 2005, p. 190; e più in dettaglio, con riguardo alle singole fattispecie introdotte, cfr. ID., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di* Internet, Padova, 2004, pp. 30-42.

tutti i reati comunque commessi mediante un sistema informatico, nonché a qualsiasi altro di cui si debbano o possano raccogliere prove in forma elettronica – definiti *cibernetici in senso improprio*[123].

Nell'ambito della prima categoria la stessa Convenzione fa rientrare quattro titoli, dedicati rispettivamente ai reati contro la riservatezza, l'integrità e la disponibilità dei dati e sistemi informatici (artt. 2-6) – tra i quali sono previsti l'accesso illegale, l'intercettazione illegale, l'attentato all'integrità dei dati e dei sistemi e l'abuso di dispositivi; ai reati informatici classici (artt. 7-9) – che ricomprendono la falsità informatica e la frode informatica; ai reati relativi al contenuto comunicativo (art. 9) – concernenti le ipotesi di diffusione di pornografia minorile; ed infine ai reati relativi alle violazioni del diritto d'autore (art. 10).

Nell'ambito dell'Unione europea, già nelle Conclusioni del Consiglio europeo di Tampere del 1999 si faceva riferimento all'esigenza di un ravvicinamento delle legislazioni degli Stati membri in materia di criminalità informatica, per una più efficace strategia di contrasto di tale pericolosa forma di criminalità, successivamente nell'ambito del III pilastro della costruzione europea, veniva adottata la decisione quadro 2005/222/GAI del Consiglio del 24 febbraio 2005 relativa agli attacchi ai sistemi di informazione[124], con l'obiettivo di migliorare la cooperazione tra le autorità giudiziarie e le altre autorità competenti degli Stati membri, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione della legge, mediante il ravvicinamento delle legislazioni penali degli Stati membri nel settore degli attacchi contro i sistemi di informazione, sulla base della constatazione che una risposta efficace alle minacce provenienti da tali attacchi richiede un approccio globale rispetto alla sicurezza delle reti e dell'informazione, in quanto le rilevanti lacune e le notevoli differenze nelle normative degli Stati membri in questo settore possono ostacolare la lotta contro la criminalità organizzata ed il terrorismo e complicare un'efficace cooperazione giudiziaria e di polizia. Il carattere transnazionale e senza frontiere dei moderni sistemi di informazione, inoltre, fa sì che gli attacchi contro tali sistemi siano spesso di natura transnazionale, e rende evidente la necessità di adottare urgentemente azioni per il ravvicinamento delle legislazioni penali in questo settore. Sulla base di tali considerazioni, viene ritenuto particolarmente importante delineare definizioni comuni, in particolare quelle inerenti ai sistemi di informazione[125] e ai dati informatici[126] e giungere ad un approccio comune nei confronti degli elementi costitutivi dei reati mediante la definizione dei reati di accesso illecito ad un sistema di informazione, di interferenza illecita per quanto riguarda i sistemi e di interferenza illecita per quanto riguarda i dati. L'art. 2 configura dunque l'ipotesi dell'accesso illecito a sistemi di informazione, consistente nei casi gravi di accesso intenzionale, senza diritto[127], ad un sistema di informazione o ad una parte dello stesso. È prevista altresì la possibilità per gli Stati di rendere punibili tali condotte solo quando siano poste in essere violando una misura di sicurezza.

Vengono altresì configurati come comportamenti da sottoporre a sanzione penale, almeno nei casi gravi, quelle condotte di interferenza illecita concernenti sistemi o dati, consistenti rispettivamente nell'atto intenzionale, commesso senza diritto, di ostacolare gravemente o interrompere il funzionamento di un sistema di informazione mediante l'immissione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione, la soppressione di dati informatici o rendendoli inaccessibili (art. 3) e nell'atto intenzionale, commesso senza diritto di cancellare, danneggiare, deteriorare, alterare, sopprimere o rendere inaccessibili dati informatici in un sistema di informazione (art. 4). In queste due ultime ipotesi è richiesto che sia prevista una pena detentiva della

---

123 Cfr. per tali definizioni L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, cit., p. 58 ss.; ID., Internet *e il diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, cit., p. 197.

124 Pubblicata in *GUUE* L 69, 16 marzo 2005, p. 67, sulla quale v. S. PORTESI, *Attacks against information systems: an analysis of aspects related to illegal access*, in *CibD,* 2004, vol. 5, n. 4, p. 411 ss.

125 Ai sensi dell'art. 1, lett. a), della Decisione quadro «per "sistema di informazione" s'intende qualsiasi apparecchiatura o gruppo di apparecchi interconnessi o collegati, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma, nonché i dati informatici immagazzinati, trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione».

126 Ai sensi dell'art. 1, lett. b), della Decisione quadro «per "dati informatici" s'intende qualsiasi rappresentazione di fatti, informazioni o concetti in una forma che può essere trattata da un sistema di informazione, compreso un programma atto a far svolgere una funzione ad un sistema di informazione».

127 Ai sensi dell'art. 1, lett. d), della Decisione quadro «l'espressione "senza diritto" significa l'accesso o l'interferenza non autorizzati da parte di chi ha il diritto di proprietà o altro diritto sul sistema o una sua parte, ovvero non consentiti ai sensi della legislazione nazionale.».

durata massima compresa almeno tra uno e tre anni. È inoltre prevista l'applicazione di circostanze aggravanti (pene detentive della durata massima compresa almeno tra due e cinque anni) nell'ipotesi in cui le condotte delineate siano tenute nell'ambito di un'organizzazione criminale, ovvero qualora i comportamenti abbiano provocato gravi danni o abbiano colpito interessi essenziali, in tal caso tuttavia viene lasciato agli Stati membri un ampio margine di discrezionalità («uno Stato membro può adottare»), diversamente dalla prima ipotesi, nella quale la previsione sembra essere obbligatoria da parte degli Stati («ciascuno Stato membro adotta»). La decisione quadro richiede inoltre la punibilità per il tentativo e la partecipazione nei reati indicati (art. 5) e l'estensione della responsabilità anche alle persone giuridiche, con la previsione di apposite sanzioni (artt. 8 e 9).

I limiti derivanti dalla previsione delle predette disposizioni di ravvicinamento in uno strumento di III pilastro risultano peraltro superati dall'estensione del c.d. metodo comunitario, dovuto al dissolvimento della originaria costruzione in pilastri dell'Unione, determinato dall'entrata in vigore del Trattato di Lisbona che ha inoltre introdotto una specifica base giuridica, ossia l'art. 83 TFUE, che attribuisce all'Unione la competenza ad adottare norme minime relative alla definizione dei reati e delle relative sanzioni con riguardo a forme di criminalità grave, aventi una dimensione transnazionale derivante dal carattere o dalle implicazioni dei reati commessi o da una particolare necessità di combatterli su basi comuni (par. 1)[128], tra le quali viene ricompresa esplicitamente la criminalità informatica; ovvero «Allorché il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri in materia penale si rivela indispensabile per garantire l'attuazione efficace di una politica dell'Unione in un settore che è stato oggetto di misure di armonizzazione, norme minime relative alla definizione dei reati e delle sanzioni nel settore in questione possono essere stabilite tramite direttive.» (par. 2)[129]. La portata innovativa di tale previsione non viene ridotta dalla circostanza per la quale l'esercizio di siffatta competenza da parte dell'Unione sia pur sempre *filtrato* dal necessario - anche se vincolato dalle scelte operate in sede europea - intervento attuativo dei legislatori nazionali, configurando pertanto una competenza pur sempre *indiretta* dell'organismo sovrannazionale[130], in quanto essa consente all'Unione di operare legittimamente delle vere e proprie scelte di criminalizzazione, in presenza dei requisiti richiesti dai parr. 1 e 2 dell'art. 83 TFUE, considerandone pur sempre di volta in volta la necessità e la proporzionalità in un'ottica di razionale e ponderata valutazione politico-criminale, in particolare con riguardo all'esercizio delle competenze delineate nel par. 2, ove «l'assenza di ogni riferimento circa l'appartenenza dei settori interessati alle "sfere di criminalità particolarmente grave che presentano carattere transnazionale" (laddove l'esigenza di efficacia delle politiche europee può logicamente rendere necessario un intervento di armonizzazione anche con riguardo a violazioni non costituenti criminalità grave)» per ciò stesso richiede una «maggiore

---

128 Nello stesso paragrafo 1 dell'art. 83 vengono elencate le forme di criminalità per le quali sussiste tale competenza: terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata. Si tratta di un'elencazione che va considerata al momento tassativa, tuttavia si è tenuto conto della circostanza che l'evolversi delle forme di criminalità potrebbe richiedere un'estensione di tale lista, pertanto è previsto che il Consiglio può adottare una decisione che individua altre sfere di criminalità che rispondono ai criteri indicati, deliberando all'unanimità previa approvazione del Parlamento europeo.

129 Sulle differenze tra le disposizioni dei primi due paragrafi dell'art. 83 TFUE e sulle questioni problematiche da essi e dal meccanismo del c.d. freno di emergenza scaturenti, cfr. G. GRASSO, *La* "competenza penale" *dell'Unione europea nel quadro del Trattato di Lisbona*, in G. GRASSO, L. PICOTTI, R. SICURELLA (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, p. 694 ss.; R. SICURELLA, "Prove tecniche" *per una metodologia dell'esercizio delle nuove competenze concorrenti dell'Unione europea in materia penale*, ivi, p. 37 ss.; L. PICOTTI, *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona*, ivi, p. 216 ss. Per una valutazione sulla legittimità dell'adozione di norme penali minime *ex* art. 83 TFUE in materia ambientale, cfr. G.M. VAGLIASINDI, *Obblighi di penalizzazione di fonte europea e principi di politica criminale: le indicazioni promananti dalla materia ambientale*, *ivi*, p. 140 ss.

130 Per tale definizione della natura della competenza attribuita all'Unione dall'art. 83 TFUE, cfr. G. GRASSO, *La* "competenza penale" *dell'Unione europea nel quadro del Trattato di Lisbona*, cit., pp. 694-696. Per una definizione diversa, giustificata tuttavia dalle medesime ragioni di fondo, cfr. R. SICURELLA, "Prove tecniche" *per una metodologia dell'esercizio delle nuove competenze concorrenti dell'Unione europea in materia penale*, cit.., p. 6, che fa riferimento ad una «"competenza integrata" nazionale e dell'Unione quanto alla predisposizione della tutela penale e la definizione dei contenuti di quest'ultima»; ID., *Questioni di metodo nella definizione di una teoria delle competenze penali dell'Unione*, in *Studi in onore di Mario Romano*, IV, Napoli, 2011, p. 2575. Definisce di contro le competenze di cui all'art. 83, par. 1, come *dirette*, L. PICOTTI, *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona*, cit., pp. 217-218, «in quanto inerenti direttamente le materie elencate, senza necessità di individuare ulteriori atti o fonti cui riferirsi per determinarne la sussistenza in concreto».

rigidità quanto alla valutazione di sussidiarietà di un legittimo intervento dell'Unione […], espresso dall'impiego del termine "indispensabilità"»[131].

Per quanto specificamente concerne la materia della criminalità informatica, come accennato, l'art. 83, par. 1, ricomprende tra le forme di criminalità particolarmente grave dal carattere transnazionale anche quest'ultima, attribuendo pertanto al legislatore europeo una competenza penale per la quale viene in sostanza richiesta una valutazione meno stringente in termini di indispensabilità/necessità dell'intervento sovrannazionale, proprio per la *presunzione* della sussistenza di un tale requisito, ricavabile dalle caratteristiche specifiche dei tipi di criminalità descritti dalla disposizione.

La estrema genericità della terminologia usata dall'art. 83 TFUE con riguardo alla descrizione delle forme di criminalità per le quali il legislatore europeo può esercitare la competenza penale attribuitagli rende particolarmente disagevole delimitare i confini delle singole ipotesi elencate, nonché delle linee di demarcazione tra queste ultime. Pertanto, occorre preliminarmente riflettere su cosa debba intendersi per criminalità informatica, ai sensi dell'art. 83, par. 1, TFUE, in ordine all'esatta individuazione degli specifici settori nell'ambito dei quali può intervenire l'esercizio delle competenze del legislatore europeo. Prendendo le mosse dalla constatazione dell'assenza allo stato attuale di una definizione generale di tale forma di criminalità nell'ambito degli strumenti europei ed internazionali, che pur contengono disposizioni che esplicitamente sono indirizzate al contrasto di siffatto tipo di criminalità[132], ed accogliendo la distinzione proposta da una parte della dottrina tra *reati cibernetici in senso stretto* - ossia quelli che presentano «fra i requisiti del "fatto" *tipico*, uno *specifico* "elemento tecnico" che richiami la "rete", quale modalità o "luogo" di commissione od anche solo di possibile destinazione della condotta o dei suoi effetti» (ad esempio, accesso abusivo a sistemi o dati informatici, frodi informatiche, falsità informatiche, danneggiamenti informatici, intercettazioni informatiche) -, *reati cibernetici in senso ampio* - ossia quelli che presentano «elementi costitutivi formulati in modo tale da risultare applicabili, in via interpretativa, a questa specifica modalità o sede di commissione» (come, ad esempio, la diffamazione a mezzo *internet*, l'istigazione al razzismo, ed in generale tutte le condotte che determinano la comunicazione o la diffusione di un pensiero o di un contenuto illecito o dannoso nella rete) – e *reati cibernetici in senso improprio* - ossia le ipotesi in cui «nessun elemento *tipico* del fatto di reato […] viene rappresentato od integrato da un requisito *tecnico* di natura informatica o cibernetica, la cui rilevanza è circoscritta alle fasi "atipiche" della preparazione, dell'organizzazione, del postfatto, ecc.» (come nei casi di criminalità organizzata, terrorismo, corruzione, traffico di stupefacenti, armi, organi, rifiuti)[133], sembra di poter facilmente ricomprendere nella predetta nozione i reati cibernetici in senso stretto che risultano tra l'altro essere già in larga parte previsti da taluni strumenti europei, come la Convenzione *Cybercrime*, la decisione quadro 2005/222/GAI ed oggi, come vedremo, la direttiva 2013/40/UE. Altrettanto facilmente pare potersi escludere che rientrino nella nozione indicata dal par. 1 dell'art. 83 TFUE i reati cibernetici in senso improprio, nei quali l'elemento informatico si pone all'esterno del fatto tipico. Qualche perplessità maggiore potrebbe invece sorgere con riguardo alla categoria dei reati cibernetici in senso ampio, in cui la presenza dell'elemento tecnico-informatico è solo eventuale e funge frequentemente da mero *amplificatore* della dannosità (aumentandone la diffusività) di condotte comunque ritenute meritevoli di sanzione, a prescindere dalla sussistenza di tale elemento[134].

---

131 Cfr. R. SICURELLA, "Prove tecniche" *per una metodologia dell'esercizio delle nuove competenze concorrenti dell'Unione europea in materia penale*, cit., p. 39, e più diffusamente p. 49 ss.

132 In quanto tali strumenti considerano frequentemente solo specifiche modalità di manifestazione di tali forme di criminalità, come i reati di accesso illecito e di interferenze illecite su dati e sistemi; la diffusione, produzione, possesso di materiale pedopornografico; la realizzazione di attacchi terroristici con distruzione di infrastrutture e sistemi informatici. O altrimenti rinviano per tale definizione alle legislazioni nazionali, presumendo una sorta di omogeneità delle fattispecie ivi rientranti, cfr. L. PICOTTI, *La nozione di* "criminalità informatica" *e la sua rilevanza per le competenze penali europee*, in *RTDPE*, 4, 2011, p. 857.

133 Cfr. L. PICOTTI, *La nozione di* "criminalità informatica"*e la sua rilevanza per le competenze penali europee*, cit., p. 845 ss.

134 Ricomprende tale categoria di reati nella nozione di criminalità informatica di cui all'art. 83, par. 1, TFUE L. PICOTTI, *La nozione di* "criminalità informatica" *e la sua rilevanza per le competenze penali europee*, cit., p. 861, il quale ritiene di «includere nell'oggetto dei poteri di intervento "armonizzatore" anche le *nuove* manifestazioni criminose che via via emergono nel *Cyberspace* per la corrispondente necessità di introdurre *nuovi e specifici* strumenti di contrasto, sia di natura sostanziale che di natura processuale», in modo tale da evitare che gli

D'altro canto, bisogna rilevare come l'esclusione di tale categoria dalla nozione di criminalità informatica non necessariamente comporterebbe l'impossibilità per il legislatore europeo di esercitare le proprie competenze in materia penale con riguardo alle condotte ivi ricomprese, che potrebbero frequentemente rientrare nelle altre forme di criminalità elencate nello stesso par. 1 dell'art. 83 TFUE, ovvero essere oggetto di un intervento di ravvicinamento, sussistendo i requisiti richiesti dal par. 2 della stessa disposizione. Una tale interpretazione ristretta sarebbe anche maggiormente in linea con il dato letterale della disposizione di cui all'art. 83, par. 1, che si riferisce specificamente alla criminalità informatica (*computer crime* nella versione inglese) e non generalmente al *cybercrime*, come invece accade per la Convenzione del Consiglio d'Europa del 2001, e sembra riprendere invece la Raccomandazione dello stesso Consiglio d'Europa n. 9 (89) 9, concernente proprio il *computer-related crime*, ove si richiede agli Stati di sottoporre a sanzioni penali una serie di condotte corrispondenti tendenzialmente a quelle rientranti nella predetta categoria dei reati cibernetici in senso stretto.

3.1 La direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione

Il legislatore europeo non ha tardato ad esercitare la competenza in materia penale attribuitagli dal predetto art. 83, par. 1, TFUE attraverso la predisposizione di una direttiva volta a ravvicinare il diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione, stabilendo norme minime per la definizione dei reati e delle sanzioni rilevanti[135], a facilitare la prevenzione di tali reati ed a migliorare la cooperazione tra autorità giudiziarie e altre autorità competenti (art. 1).

Le valutazioni concernenti la sussistenza dei requisiti richiesti dall'art. 83, par. 1, TFUE per l'esercizio delle competenze penali da parte dell'Unione, ovvero la particolare gravità ed il carattere transnazionale delle forme di criminalità in relazione alle quali va delineato l'intervento armonizzatore a livello sovrannazionale, vengono svolte nell'ambito dei considerando preliminari della direttiva. In particolare, nel considerando n. 3 viene messa in evidenza la pericolosità di attacchi ai sistemi d'informazione che fanno parte dell'infrastruttura critica[136] degli Stati membri, che rappresenta una minaccia per la creazione di una società dell'informazione più sicura e di uno spazio di libertà, sicurezza e giustizia; nei considerando nn. 5 e 6 si sottolinea la particolare dannosità di attacchi condotti su larga scala e con metodi sempre più sofisticati (come ad esempio le c.d. *botnet*), che possono comportare le perturbazioni dei servizi di sistema di rilevante interesse pubblico o la creazione di costi finanziari esorbitanti o la perdita di dati personali o di informazioni sensibili, o ancora l'interruzione dei sistemi di informazione e delle comunicazioni sia attraverso la perdita o l'alterazione di informazioni riservate commercialmente importanti o di altri dati, anche se la determinazione della nozione di "danno grave" viene delegata ai legislatori nazionali.

La selezione delle condotte più gravi da sottoporre a sanzione penale viene poi operata attraverso una previsione restrittiva con riguardo al criterio d'imputazione soggettiva, in quanto ricadono nell'ambito di operatività della direttiva i soli comportamenti connotati dal dolo (considerando n. 17), e con l'esclusione dei casi di minore gravità, la cui nozione viene tuttavia demandata ancora una volta ai legislatori nazionali, venendo indicate solo alcune ipotesi esemplificative, ovvero – con una menzione piuttosto generica - qualora il danno causato dal reato e/o il rischio per gli interessi pubblici o privati, ad esempio per l'integrità di un sistema di informazione o per dati informatici, o per l'integrità, i diritti o altri interessi di una persona, sia insignificante o di natura tale da non rendere necessario imporre una sanzione penale entro i limiti di legge o stabilire una responsabilità penale.

---

ordinamenti penali nazionali «siano costretti ad applicare norme ed istituti concepiti per fattispecie e necessità di tutela, nonché esigenze investigative e probatorie, diverse e superate, seppur talora riconducibili ad un'analoga *ratio*».

135 Direttiva 2013/40/UE del Parlamento europeo e del Consiglio del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio, pubblicata in *GUUE* L 218, 14 agosto 2013, p. 8.

136 Il considerando 4 precisa cosa debba intendersi per infrastruttura critica di uno Stato, riferendosi ad «un elemento, un sistema o parte di questo […] che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico o sociale delle persone, come gli impianti energetici, le reti di trasporto o le reti governative, e il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni».

Infine, il carattere transnazionale delle condotte oggetto degli obblighi di penalizzazione imposti dalla direttiva viene evidenziato nel considerando 27, sul rilievo del carattere transnazionale e senza frontiere dei moderni sistemi di informazione, che fa sì che gli attacchi contro tali sistemi abbiano una dimensione transfrontaliera, che rende evidente la necessità del ravvicinamento del diritto penale in questo settore.

Per quanto specificamente attiene alle condotte, gli obblighi di penalizzazione concernono in primo luogo le ipotesi di accesso intenzionale e senza diritto – ossia non autorizzato da parte del proprietario o da un altro titolare di diritti sul sistema o su una sua parte, ovvero non consentito a norma del diritto nazionale - a un sistema di informazione o a una parte dello stesso, qualora sia commesso *in violazione di una misura di sicurezza*, prevedendo come soglia minima del massimo edittale una pena detentiva non inferiore a due anni (art. 3 – Accesso illecito a sistemi di informazione).

Vengono poi previste le condotte di interferenza illecita relativamente ai sistemi e ai dati (artt. 4 e 5), che puniscono gli atti – compiuti intenzionalmente e senza diritto – rispettivamente «di ostacolare gravemente o interrompere il funzionamento di un *sistema di informazione* mediante l'immissione di dati informatici, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di tali dati o rendendo tali dati inaccessibili» e «di cancellare, danneggiare, deteriorare, alterare, sopprimere *dati informatici* in un sistema di informazione, o di rendere tali dati inaccessibili» (corsivo aggiunto). In questi casi viene prevista come soglia minima del massimo edittale della pena base, una pena detentiva non inferiore a due anni, che viene aumentata a tre anni, se un numero significativo di sistemi di informazione è stato colpito avvalendosi di programmi, *password*, codici di accesso utilizzati per commettere una delle altre ipotesi previste dalla direttiva[137].

L'art. 6 della direttiva richiede invece che gli Stati configurino come reato l'interferenza illecita, consistente nel comportamento di chi intercetta intenzionalmente e senza diritto, tramite strumenti tecnici, trasmissioni non pubbliche di dati informatici verso, da o all'interno di un sistema di informazione, incluse le emissioni elettromagnetiche da un sistema di informazione che trasmette tali dati informatici, prevedendo come soglia minima del massimo edittale una pena detentiva non inferiore a due anni. Infine, lo stesso trattamento sanzionatorio viene stabilito per le condotte di fabbricazione, vendita, approvvigionamento per l'uso, importazione, distribuzione o messa a disposizione in altro modo intenzionali di un programma per computer, destinato o modificato principalmente al fine di commettere uno dei reati indicati dalla direttiva stessa ovvero di una *password* di un computer, di un codice d'accesso, o di dati simili che permettono di accedere in tutto o in parte a un sistema di informazione, qualora siano compiute senza diritto e con l'intenzione di utilizzarli al fine di commettere uno dei reati descritti dalla direttiva.

Il legislatore richiede altresì che risultino punibili le condotte di istigazione, favoreggiamento e più in generale di partecipazione concorsuale nei reati indicati ed il tentativo di questi ultimi, sottolineando anche la necessità di prevedere la responsabilità delle persone giuridiche per questi ultimi.

La direttiva in esame sembra porsi tendenzialmente nell'alveo del rispetto sia del principio di sussidiarietà, avendo essa stessa evidenziato l'indispensabilità di un intervento sovrannazionale con riguardo a forme di criminalità, quali sono gli attacchi informatici, caratterizzate dalla transnazionalità degli strumenti usati e delle implicazioni da esse derivanti; sia dei principi - inerenti a considerazioni di politica criminale proprie delle scelte di criminalizzazione - di necessità e proporzionalità di un intervento punitivo posto a tutela di un bene giuridico, quale l'integrità, il buon funzionamento e la sicurezza dei sistemi di informazione strettamente connesso tra l'altro alla tutela della riservatezza e alla protezione dei dati personali custoditi all'interno dei sistemi d'informazione, limitato alle sole condotte dolose connotate, come evidenziato, da una certa gravità. Rimane, ciononostante, qualche perplessità con riguardo a talune ipotesi che prevedono probabilmente un'eccessiva anticipazione della tutela penale – così come si rileverà anche per le corrispondenti fattispecie incriminatrici già presenti

[137] Sempre con riguardo alle due ipotesi di interferenza (artt. 4 e 5) sono inoltre configurate specifiche circostanze aggravanti, che portano la pena detentiva ad una soglia minima del massimo edittale non inferiore a cinque anni, qualora siano commesse nell'ambito di un'organizzazione criminale o ai danni di sistemi di informazione di un'infrastruttura critica dello Stato; causino gravi danni.

nell'ordinamento italiano (art. 615 *quater* cp) -, ed in particolare la condotta di fabbricazione o di approvvigionamento per l'uso di codici di accesso o *password*, al fine di commettere uno dei delitti previsti dalla direttiva, che mira a punire in sostanza il pericolo del pericolo e nel quale l'intero disvalore del fatto si concentra nella sua direzione finalistica alla commissione di altri delitti del tipo di quelli delineati dalla direttiva[138].

In quanto all'obiettivo di armonizzazione delle legislazioni penali degli Stati perseguito dalla direttiva, la mancanza di nozioni comuni a livello sovrannazionale relative ai concetti di "casi di minore gravità", di "danno grave", nonché di norme della parte generale del diritto penale, concernenti il tentativo, la partecipazione, il regime delle circostanze, la determinazione ed esecuzione della pena, può di fatto frustrare tale obiettivo soprattutto con riguardo ai regimi sanzionatori concretamente applicabili nei diversi Stati membri[139].

4. La compatibilità del quadro normativo italiano con la direttiva 2013/40/UE

Analizzata dunque la normativa sovrannazionale ed accertata la tendenziale rispondenza delle scelte di penalizzazione operate in sede europea ai principi generali di necessità e proporzionalità dell'intervento punitivo, rimane a questo punto da verificare se il quadro normativo italiano in materia di attacchi ai sistemi di informazione, stratificatosi nel tempo in seguito ai diversi interventi di riforma che l'hanno riguardato, risponda pienamente alle richieste di penalizzazione promananti dal legislatore europeo o se al contrario necessiti di una nuova modifica per soddisfare le esigenze di tutela delineate in ambito sovrannazionale.

A tal fine, va preliminarmente rilevato che il legislatore italiano, provvedendo alla ratifica della Convenzione *Cybercrime*, ha adottato la legge 18 marzo 2008, n. 48[140], con la quale: a) è stata riformulata la fattispecie di cui all'art. 615 *quinquies* cp (*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*), per renderla maggiormente compatibile all'ipotesi di abuso di codici prevista dall'art. 6 della stessa Convenzione; b) è stata modificata la fattispecie di danneggiamento di informazioni, dati e programmi informatici di cui all'art. 635 *bis* cp e sono state introdotte tre nuove ipotesi di danneggiamento, rispettivamente all'art. 635 *ter* cp, che disciplina il delitto di danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità, al successivo art. 635 *quater* cp, che punisce il danneggiamento di sistemi informatici o telematici, ed infine all'art. 635 *quinquies* cp, che delinea l'ipotesi del danneggiamento a carico di sistemi informatici e telematici di pubblica utilità; c) sono state infine abrogate le disposizioni di cui ai commi secondo e terzo dell'art. 420 cp, che punivano le fattispecie di attentato ad impianti di pubblica utilità relativo a sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o ad essi pertinenti e l'ipotesi aggravata dall'effettiva distruzione, danneggiamento o interruzione anche parziale del funzionamento dell'impianto o del sistema.

---

138 Cfr. G. MARINUCCI, E. DOLCINI (a cura di), *Art. 615* quater, in *Codice penale*, Milano, 2011, pp. 5994-5995.

139 Sulla necessità di un'armonizzazione con riguardo ad alcuni istituti della parte generale particolarmente incidenti sulla determinazione concreta delle sanzioni, cfr. F. VIGANÒ, *Verso una* "Parte generale europea"*?*, in G. GRASSO, G. ILLUMINATI, R. SICURELLA, S. ALLEGREZZA, *Le sfide dell'attuazione di una Procura europea: definizione di regole comuni e loro impatto sugli ordinamenti interni*, Milano, 2013, p. 123 ss., che evidenzia tuttavia la difficoltà di un tale intervento «per effetto dell'*imposizione dall'alto* di norme unitarie», ritenendo maggiormente probabile «un processo di graduale *osmosi – dal basso* – di tali principi e regole nella loro concreta declinazione da parte dei *giudici*» (in partic. cfr. p. 132).

140 Per un'ampia ricostruzione delle novità introdotte dall'intervento normativo in esame, si veda L. PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *DPP*, 2008, 6, p. 700 ss.; ID., *Ratifica della Convenzione* Cybercrime *e nuovi strumenti di contrasto contro la criminalità informatica*, in *DInt*, 2008, 5, p. 437ss., che si esprime invero in termini piuttosto critici sull'operato del legislatore nazionale che si sarebbe basato su autonome scelte piuttosto che sulle indicazioni derivanti dalla Convenzione, cogliendo l'occasione della legge in questione per rivedere alcune parti controverse della disciplina già vigente in materia.

Infine la novella del 2008 ha esteso la responsabilità da reato delle persone giuridiche e degli enti a tutte le nuove fattispecie delittuose in materia di criminalità informatica introdotte nel codice penale sia dalla stessa novella, sia dalla precedente legge 547/1993[141].

Prendendo le mosse, dunque, da tale assetto normativo emergente dalla novella del 2008, si può rilevare come, nonostante una tendenziale conformità del sistema normativo italiano alle disposizioni della direttiva, sussistano talune distonie - sia dal punto di vista della descrizione delle condotte incriminate, sia con riguardo alle sanzioni previste – che andrebbero corrette mediante un nuovo intervento del legislatore.

Non potendoci soffermare in questa sede sull'analisi puntuale delle singole fattispecie incriminatrici previste nell'ambito del nostro ordinamento che possono soddisfare le richieste di penalizzazione avanzate dal legislatore europeo, si metteranno in evidenza soltanto le difformità tra le due normative (nazionale e sovrannazionale) e le possibili soluzioni che si prospettano al legislatore o ai giudici nazionali per dare piena e completa attuazione agli obblighi previsti dalla direttiva entro il 4 settembre 2015, termine di scadenza per il recepimento di quest'ultima da parte degli Stati.

La fattispecie incriminatrice prevista dal codice penale italiano, che rappresenta un potenziale omologo della condotta di accesso illecito a sistemi di informazione prevista dall'art. 3 della direttiva in esame, risulta indubbiamente l'ipotesi disciplinata dall'art. 615 *ter* di accesso abusivo ad un sistema informatico o telematico[142]. Si tratta di fattispecie introdotta dalla legge 547/1993, che ha posto diversi dubbi interpretativi sin dalla sua entrata in vigore. Essa punisce la condotta di «chiunque abusivamente si *introduce* in un sistema informatico o telematico *protetto da misure di sicurezza* ovvero vi si *mantiene* contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.»[143].

Dalla stessa lettera della disposizione emergono talune difformità rispetto alla condotta descritta dalla direttiva, in primo luogo con riguardo alle stesse modalità di manifestazione della condotta che, ai sensi della norma interna, si articolano su due comportamenti, ovvero l'*introduzione* abusiva ma anche il *mantenimento* contro la volontà espressa o tacita di chi ha il diritto di escluderlo, che non trova invece alcun riscontro nell'art. 3 della direttiva. La condotta prevista dall'art. 615 *ter* cp è posta inoltre a presidio di un sistema informatico o telematico *protetto da misure di sicurezza*, di contro la direttiva europea richiede ai fini della punibilità dell'accesso che quest'ultimo sia avvenuto *in violazione di una misura di sicurezza*.

Nonostante *prima facie* le differenze terminologiche evidenziate possano apparire di poco momento, in effetti ad una più attenta analisi può rilevarsi come la formulazione dell'art. 3 della direttiva abbia proceduto ad una più selettiva valutazione della condotta da sottoporre a pena, in quanto

---

141 Rimangono tuttavia fuori da tale ampliamento della responsabilità da reato delle persone giuridiche e degli enti l'ipotesi di falsa attestazione al certificatore di cui all'art. 495 *bis* cp e quella di frode informatica di cui all'art. 640 *ter* cp, se non commessa in danno dello Stato o di altro ente pubblico.

142 Cfr. L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, cit., p. 77 ss.; M.B. MAGRO, Internet *e* Privacy. *L'utente consumatore e modelli di tutela penale della riservatezza*, in *Ind*P, 2005, 3, p. 961 ss.; G. MARINUCCI, E. DOLCINI, *Art. 615* ter, in *Codice penale*, Milano, 2011, p. 5978 ss.; G. FIANDACA, E. MUSCO, *Diritto Penale – Parte speciale*, vol. II, tomo I, Bologna, 2007, p. 249 ss.; R. FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di* "domicilio informatico" *e lo* jus excludendi alios, in *DPP*, 2005, n. 1, p. 81 ss.; ID., *Art. 615* ter *c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in *DPP*, 2008, n. 1, p. 106 ss.; ID., *Verso una rivalutazione dell'art. 615* ter *c.p.? Il reato di accesso abusivo a sistemi informatici o telematici fra la tutela di tradizionali e di nuovi diritti fondamentali nell'era di* Internet, in *DPC*, 2012, 2, p. 126 ss.; D. TRENTACAPILLI, *Accesso abusivo ad un sistema informatico e adeguatezza delle misure di protezione*, in *DPP*, 2002, 10, p. 1280 ss.; G. ARONICA, *L'accesso abusivo ad un sistema informatico o telematico (art. 615* ter *c.p.) nella giurisprudenza*, in *IndP*, 2010, 1, p. 199 ss.; S. PERRONE, *La (in)determinatezza della condotta di accesso abusivo ad un sistema informatico o telematico*, in *Ius 17@unibo.it: Studi e materiali di diritto penale*, 2010, 1, p. 77 ss.; D. FOTI, *Accesso abusivo a sistema informatico o telematico. Un* "pericoloso" *reato di pericolo.*, in *RIDPP*, 2010, 1, p. 456 ss.

143 Il secondo comma della disposizione in parola prevede poi una serie di circostanze aggravanti, che comportano l'innalzamento della pena della reclusione da uno a cinque anni, nei casi in cui il fatto sia commesso: da un soggetto qualificato (pubblico ufficiale, incaricato di pubblico servizio, investigatore privato o operatore del sistema), con abuso dei propri poteri o in violazione dei doveri inerenti la propria funzione); ovvero usando violenza sulle cose o alle persone o da soggetto armato. O ancora se dal fatto derivi la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione, o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Lo stesso aumento di pena viene stabilito dal terzo comma se la condotta di accesso abusivo viene perpetrata ai danni di sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico (ossia ad infrastrutture critiche dello Stato, per usare la terminologia della direttiva).

ha ricondotto alla sola ipotesi dell'accesso – caratterizzata certamente da maggior disvalore penale rispetto a quella del mantenimento (che necessariamente presuppone che quanto meno in un primo momento il soggetto agente fosse stato autorizzato all'accesso o fosse legittimamente in possesso di codici di accesso e *password* idonei a neutralizzare le misure di sicurezza, avendo poi travalicato i limiti dell'autorizzazione o delle regole relative all'accesso), in quanto posta in essere totalmente in assenza di un'autorizzazione ed inoltre in violazione delle misure di sicurezza apprestate a protezione del sistema informatico – la punibilità dell'agente, condizionandola altresì alla violazione di una misura di sicurezza, in tal modo richiedendo da una parte l'effettiva consapevolezza da parte del soggetto attivo della sussistenza di tale misura e dell'infrazione della stessa, e dall'altra l'idoneità della misura a proteggere il sistema informatico o telematico a tutela del quale è stata posta, così ulteriormente restringendo l'ambito della punibilità rispetto alla fattispecie nazionale che richiede esclusivamente l'accesso abusivo ad un sistema protetto da misure di sicurezza.

In altre parole, per quanto concerne la prima questione (duplicità di condotte incriminate dalla normativa nazionale), bisogna rilevare come la formulazione dell'art. 615 *ter* cp abbia dato vita a diversi contrasti interpretativi, soprattutto con riguardo alla sussumibilità in tale fattispecie dei casi nei quali soggetti legittimamente autorizzati all'accesso a sistemi informatici protetti (principalmente banche dati riservate) avessero contravvenuto alle regole previste da appositi codici di comportamento o derivanti da prassi consolidate, prendendo visione - ed eventualmente utilizzando per finalità personali (di carattere patrimoniale o meno) o comunque divergenti da quelle per le quali l'autorizzazione era stata concessa – i dati contenuti all'interno di tali sistemi. Tali contrasti hanno trovato finalmente soluzione nel 2011 allorché le Sezioni Unite della Corte di Cassazione[144] hanno ritenuto i casi predetti sussumibili nella condotta di *mantenimento* nel sistema informatico contro la volontà espressa o tacita di chi ha il diritto di escludere altri dallo stesso, in particolare ove fosse possibile accertare la sussistenza di norme appositamente recepite in regolamenti, codici di comportamento, contratti di lavoro, ecc., ovvero emergenti da prassi consolidate, volte alla predisposizione di prescrizioni e limiti in ordine all'utilizzo delle autorizzazioni concesse per l'accesso a determinati sistemi informatici o telematici protetti appunto da specifiche misure di sicurezza. Conseguentemente, la semplice violazione di tali norme da parte dei soggetti autorizzati risulta penalmente rilevante ai sensi dell'art. 615 *ter* cp, a prescindere dalle finalità perseguite da questi ultimi e dagli utilizzi successivi che essi abbiano intenzione di fare dei dati conosciuti. La rigorosa soluzione della questione interpretativa delineata dalle Sezioni Unite trova il suo fondamento logico-giuridico nell'individuazione del bene giuridico tutelato dalla fattispecie in esame nel diritto alla riservatezza informatica (o domicilio informatico, nell'ottica di mantenere un collegamento – quanto meno terminologico – con la collocazione topografica del reato tra i delitti contro l'inviolabilità del domicilio), declinato più specificamente nello *ius excludendi alios* del titolare del sistema informatico o telematico oggetto del mantenimento illegittimo da parte del soggetto attivo.

Tale impostazione ermeneutica risulta attualmente corroborata dalla previsione secondo la quale il sistema informatico o telematico sul quale ricade la condotta incriminata debba essere *protetto da misure di sicurezza*, con ciò intendendo che queste ultime vadano considerate esclusivamente come l'indice della volontà del titolare di escludere terzi non autorizzati dall'accesso al sistema, a nulla rilevando la natura e l'efficacia di esse, in quanto non è necessario, ai fini della configurabilità del reato, che le misure di sicurezza abbiano un elevato grado di efficacia, rimanendo tali anche nel caso siano facilmente superabili da una persona mediamente esperta, proprio perché la loro funzione è solo quella di manifestare lo *ius excludendi* dell'avente diritto. Sulla base di una tale interpretazione della natura e della funzione del requisito della misura di sicurezza, si è ritenuto che il reato di accesso abusivo venga a consumazione nel momento in cui vi sia «l'*introduzione abusiva*, consistente nel "contatto" logico o nel

144 Si tratta di Cass. pen., Sez. Un., ud. 27 ottobre 2011 (dep. 7 febbraio 2012), n. 4964, che opera una puntuale ricostruzione degli orientamenti giurisprudenziali precedenti, ampiamente delineati anche nell'ordinanza di rimessione di Cass. pen., sez. V, ud. 11 febbraio 2011 (dep. 23 marzo 2011). Sulla sentenza in parola, cfr. R. FLOR, *Verso una rivalutazione dell'art. 615* ter *c.p.? Il reato di accesso abusivo a sistemi informatici o telematici fra la tutela di tradizionali e di nuovi diritti fondamentali nell'era di* Internet, cit., p. 129 ss.; A. SCIRÈ, *Abuso del titolo di legittimazione all'accesso ad un sistema informatico: alle SS.UU. la questione della configurabilità del delitto di cui all'art. 615* ter *c.p.*, in *www.penalecontemporaneo.it*; G. ROMEO, *Le Sezioni unite sull'accesso abusivo a un sistema informatico o telematico*, *ivi.*

collegamento logico con il sistema protetto, senza che sia necessario il "superamento" delle misure di sicurezza, a condizione che sul piano formale esse esistano (ancorché siano inidonee ed inefficaci al fine di impedire l'accesso abusivo al sistema medesimo, ma percepibili)[145]».

Le predette impostazioni ermeneutiche (sia con riguardo alla condotta di *mantenimento*, sia con riguardo al requisito delle misure di sicurezza) risultano certamente in linea con l'attuale dato letterale dell'art. 615 *ter* cp, tuttavia ci si può legittimamente chiedere, alla luce della nuova formulazione dell'art. 3 della direttiva 2013/40/UE, che - discostandosi sia dalle indicazioni promananti dalla Convenzione *Cybercrime*, sia da quelle derivanti dalla decisione quadro 2005/222/GAI - rivela pertanto una precisa scelta in tal senso del legislatore europeo, prevedendo espressamente tra gli elementi costitutivi della fattispecie di accesso illegale la *violazione di una misura di sicurezza* apprestata a protezione del sistema informatico, se esse possano continuare a ritenersi in linea con le scelte operate a livello sovrannazionale.

In effetti, la previsione della necessaria violazione delle misure di sicurezza contenuta nella direttiva avrebbe l'effetto di restringere l'ambito di punibilità della fattispecie di cui all'art. 615 *ter* cp, così come interpretato dalla giurisprudenza, in quanto richiederebbe il superamento di misure poste a protezione del sistema informatico, efficaci ed idonee a tale scopo, con la duplice conseguenza di selezionare solo le condotte che denotino una particolare volontà aggressiva dell'agente, manifestata dalla necessità di profondere un certo impegno tecnico nel loro aggiramento e di responsabilizzare i titolari di sistemi informatici o telematici ad investire nella predisposizione e nell'aggiornamento di misure di sicurezza in grado di rendere davvero protetti i loro sistemi[146]. La *ratio* sottesa a tale previsione avvalorerebbe inoltre, con riguardo all'individuazione del bene giuridico protetto, la tesi secondo la quale tale fattispecie sarebbe posta a protezione non esclusivamente della riservatezza dei dati e dei programmi contenuti nel sistema informatico, ma altresì della sicurezza e integrità di quest'ultimo, ove il concetto di *sicurezza informatica* individua un livello anticipato e preventivo di protezione, rispetto all'effettiva lesione dell'integrità e utilizzabilità di dati, sistemi e prodotti informatici, ricomprendendo i dispositivi, le misure, le procedure strumentali di protezione, ecc.[147]

Alla luce di tali considerazioni, ci si può realisticamente chiedere ulteriormente se possa continuarsi a punire sotto la *copertura* normativa dell'art. 615 *ter* cp, comma 1, l'accesso da parte di soggetto autorizzato (che si introduce dunque nel rispetto delle misure di sicurezza apprestate dal legittimo titolare del sistema) ad un sistema informatico o telematico, nel caso in cui questi vi permanga contro la volontà espressa o tacita di colui che avrebbe diritto ad escluderlo, secondo quanto riconosciuto dalle Sezioni Unite della Corte di Cassazione; ipotesi nella quale non sussiste in alcun modo una violazione delle misure di sicurezza, requisito ritenuto indispensabile dalla normativa europea. Si potrebbero invero prospettare due distinte vie percorribili al fine di rendere la disciplina nazionale, così come interpretata dalla giurisprudenza intervenuta al riguardo, conforme alle

---

145 Cfr. R. FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di* "domicilio informatico" *e lo* jus excludendi alios, cit., p. 92, e giurisprudenza ivi citata; ID., *Art. 615* ter *c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, cit., pp. 109-110. Nello stesso senso, cfr. G. MARINUCCI, E. DOLCINI (a cura di), *Art. 615* ter, cit., pp. 5983-5985; G. FIANDACA, E. MUSCO, *Diritto penale – Parte speciale*, cit., p. 252.

146 La volontà di realizzare tale obiettivo, ribaltando quasi del tutto la prospettiva sposata dal legislatore nazionale nel codice penale (ma in parte già accolta in materia di protezione dei dati personali dal Codice della *Privacy*, artt. 31 ss., nonché art. 169), viene resa evidente dal considerando n. 26 della direttiva in esame, che rileva come, al fine di combattere efficacemente la criminalità informatica, sia necessario aumentare la resilienza dei sistemi di informazione, adottando le misure adeguate per proteggerli in modo più efficace contro gli attacchi informatici e sprona in primo luogo gli Stati ad adottare misure di sicurezza efficaci a protezione delle loro infrastrutture critiche. Con riguardo poi al settore privato, si prevede che «costituisce parte essenziale di un approccio globale a una lotta efficace contro la criminalità informatica assicurare un adeguato livello di protezione e di sicurezza dei sistemi di informazione a opera di persone giuridiche, ad esempio in relazione ai servizi di comunicazione elettronica di pubblico accesso, conformemente alla vigente legislazione dell'Unione in materia di vita privata e comunicazioni elettroniche e protezione dei dati. Dovrebbero essere forniti livelli di protezione adeguati contro le minacce e le vulnerabilità ragionevolmente individuabili in maniera corrispondente allo stato dell'arte degli specifici settori e alle specifiche situazioni di trattamento dei dati. Il costo e l'onere di tale protezione dovrebbero essere commisurati al danno potenziale procurato da un attacco informatico ai soggetti interessati. Gli Stati membri sono incoraggiati a prevedere, nell'ambito del loro diritto nazionale, pertinenti misure per l'attribuzione di responsabilità per i casi in cui una persona giuridica non abbia manifestamente fornito un adeguato livello di protezione contro gli attacchi informatici».

147 Cfr. in questo senso L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, cit., pp. 70-71.

disposizioni della direttiva. La prima, pure prospettata in parte da un certo filone interpretativo disatteso tuttavia dalle Sezioni Unite nel 2011, comporterebbe la disapplicazione da parte degli stessi giudici nazionali dell'art. 615 *ter* cp, con esclusivo riguardo alla condotta di *mantenimento* nel sistema informatico contro la volontà del titolare. Ferma restando, in ogni caso, la possibilità, in presenza dei requisiti richiesti dalle fattispecie incriminatrici di riferimento, di sussumere quest'ultimo comportamento in altra ipotesi di reato, configurabile con riguardo agli esiti successivi della permanenza non autorizzata nel sistema (ad esempio illecita diffusione di dati personali, frode informatica, rivelazione ed utilizzazione di segreti d'ufficio).

Ove, diversamente, alla luce di una rinnovata valutazione politico-criminale di meritevolezza e necessità di pena, il legislatore italiano dovesse decidere di voler legittimamente estendere la tutela penale richiesta dalla fonte sovrannazionale, potrebbe procedere ad una separazione dell'attuale formulazione del comma 1 dell'art. 615 *ter* cp, mantenendo sostanzialmente invariata l'ipotesi ordinaria di accesso illegale, salvo precisare in termini maggiormente dettagliati la nozione di *violazione di una misura di sicurezza*, di cui si dirà più avanti, ed introducendo una nuova ipotesi di reato proprio, ovvero posto in essere da soggetto autorizzato all'introduzione nel sistema informatico, che vi si mantenga in violazione delle prescrizioni impartitegli dal legittimo titolare – prescrizioni che dovrebbero trovare puntuale riscontro in appositi regolamenti, contratti di lavoro, codici di comportamento o prassi ben consolidate ed accertate -, perseguendo dunque finalità del tutto estranee a quelle per le quali era stato autorizzato all'accesso al sistema informatico. In tal modo, il legislatore si limiterebbe a positivizzare l'orientamento delineato dalla prassi giudiziaria nazionale degli anni più recenti, ampliando tuttavia l'ambito di punibilità delineato dalla direttiva. Indubbiamente il legislatore nazionale potrebbe legittimamente estendere tale ambito di punibilità, decidendo di apprestare una tutela maggiore rispetto a quella richiesta a livello sovrannazionale, tuttavia sarebbe opportuno riflettere sulla reale necessità di prevedere una sanzione penale per quelle condotte – residuali, in quanto non rientranti in differenti fattispecie incriminatrici sulla base delle finalità illecite perseguite e delle potenzialità lesive di diversi beni giuridici (*privacy*, patrimonio, pubblica amministrazione) – caratterizzate dalla mera disobbedienza alle prescrizioni di utilizzo del sistema informatico al quale l'agente risulta autorizzato ad accedere, per il disvalore delle quali potrebbe essere maggiormente proporzionato prevedere sanzioni disciplinari o amministrative.

Per quanto concerne, invece, la mancanza nell'attuale formulazione dell'art. 615 *ter* cp della previsione della *violazione di misure di sicurezza*, in attesa di un intervento del legislatore che introduca eventualmente una nozione autonoma di *misure di sicurezza* valevole esclusivamente per i reati informatici, potrebbe essere utile richiamare la definizione di misure di sicurezza minime delineata nell'art. 33 del d.lgs. 196/2003 (Codice della *Privacy*), in maniera tale da fornire ai giudici un parametro sulla base del quale valutare l'efficacia e l'idoneità delle misure di protezione predisposte e da orientare anche i titolari dei sistemi informatici e telematici sul livello di sicurezza che sarebbe opportuno apprestare, nell'ottica di una maggiore responsabilizzazione di questi ultimi.

Non sorgono invece particolari problemi interpretativi per le due ipotesi di interferenza illecita - rispettivamente relative ai sistemi e ai dati - previste dalla direttiva (artt. 4 e 5), che trovano una corrispondenza pressoché totale in termini di definizione della condotta nelle quattro ipotesi di danneggiamento informatico previste negli artt. 635 *bis* (*Danneggiamento di informazioni, dati e programmi informatici*), 635 *ter* (*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*), 635 *quater* (*Danneggiamento di sistemi informatici o telematici*) e 635 *quinquies* (*Danneggiamento di sistemi informatici o telematici di pubblica utilità*) cp. Va tuttavia rilevato che il recepimento della direttiva potrebbe costituire una buona occasione offerta al legislatore nazionale per provvedere ad una migliore sistematizzazione di tale disciplina, frutto del frettoloso intervento normativo del 2008, volto al recepimento della Convenzione *Cybercrime*[148], in modo tale da potere altresì

[148] Cfr. per una puntuale disamina anche in chiave critica delle fattispecie di danneggiamento modificate ed introdotte dalla legge 48/2008, L. PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale*, cit., p. 710 ss. Si veda altresì G. MARINUCCI, E. DOLCINI (a cura di), *Artt. 635* bis, ter, quater, quinquies, in *Codice penale*, Milano 2011, p. 6331 ss.

uniformare alle richieste sovrannazionali il trattamento sanzionatorio, tenendo conto tuttavia in tale operazione adeguatrice anche della formulazione degli artt. 635 *ter* e 635 *quinquies* come delitti di attentato, comportanti dunque una forte anticipazione della tutela penale[149].

Non si rilevano particolari problematiche neanche con riguardo all'ipotesi di intercettazione illecita che trova preciso riscontro nel nostro ordinamento nell'art. 617 *quater* cp (*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*).

Un intervento del legislatore nazionale potrebbe invece essere richiesto con riguardo alle ipotesi indicate dall'art. 7 della direttiva, concernenti gli strumenti utilizzati per commettere i reati, che corrispondono in larga parte a quanto previsto dall'art. 6 della Convenzione *Cybercrime*, per recepire la quale era già stato introdotto nel nostro codice penale il testo dell'art. 615 *quinquies* cp (*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*), duramente criticato da una parte della dottrina per la scelta di imperniare sul solo elemento finalistico (dolo specifico) l'intera illiceità penale del fatto, consistente nello scopo di danneggiare illecitamente, di favorire l'interruzione o l'alterazione del suo funzionamento un sistema informatico o telematico, senza di contro riferire tale scopo oggettivamente ai programmi, alle apparecchiature o ai dispositivi, come avrebbe richiesto la Convenzione e come richiede oggi la direttiva, che si riferisce ad un programma per computer, destinato o modificato principalmente al fine di commettere uno dei reati previsti dalla direttiva[150]. Anche la formulazione dell'art. 615 *quater* cp (*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*) ha sollevato numerose critiche per la forte anticipazione della tutela penale che esso comporta. Esso sostanzialmente risponde alle richieste della direttiva, pur presentando talune difformità con riguardo all'oggetto del dolo specifico, individuato nel procurare a sé o ad altri un profitto ovvero nell'arrecare ad altri un danno, mentre nel testo sovrannazionale sembra essere riferito esclusivamente alla commissione dei reati di accesso illegale, interferenza illecita e intercettazione illecita.

La direttiva richiede inoltre la punibilità del tentativo con riguardo a tutte le ipotesi delineate, tuttavia qualche problema potrebbe porsi nel nostro ordinamento con riguardo alle fattispecie di cui agli artt. 615 *ter*, *quater* e *quinquies*, costruite dal legislatore come reati di pericolo.

5. Considerazioni conclusive

La breve analisi condotta con riguardo agli strumenti normativi adottati e in corso di adozione nell'ambito dell'Unione europea sembra dimostrare come la tendenza del legislatore europeo sia nel senso di una maggiore attenzione alle questioni concernenti la tutela della riservatezza e la protezione dei dati personali, che rappresentano attualmente una priorità nell'agenda europea. Tale maggiore attenzione trova riscontro anche nella *law in action*, come emerge dalla recentissima pronuncia della Corte di giustizia sulla invalidità della direttiva 2006/24/UE.

Sembra che le istituzioni dell'Unione, consapevoli delle preoccupazioni che nel corso degli scorsi anni erano sorte con riguardo a un approccio eccessivamente securitario dovuto alle sentite esigenze di contrastare i fenomeni della criminalità organizzata e del terrorismo internazionale talvolta anche mediante una forte compressione dei diritti fondamentali delle persone, abbiano colto l'occasione fornita loro dalla *costituzionalizzazione* del diritto alla riservatezza e alla protezione dei dati personali, mediante la Carta ed il Trattato stesso, per riequilibrare tale approccio, attraverso concrete azioni legislative e giudiziarie.

Valutazioni altrettanto positive sembra che possano riguardare anche l'esercizio delle competenze penali attribuite all'Unione dall'art. 83 TFUE, par. 1, in quanto il legislatore europeo sembra aver compiutamente rispettato i principi di necessità e proporzione nell'operare le scelte di criminalizzazione relative agli attacchi informatici, talvolta restringendo l'ambito della punibilità di fattispecie

[149] Cfr. in questo senso S. CIVELLO CONIGLIARO, *La nuova tutela penale europea dei sistemi di informazione*, in *www.penalecontemporaneo.it*.
[150] Cfr. L. PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale*, cit., p. 710.

incriminatrici nazionali in un'ottica di intervento dello strumento punitivo come *extrema ratio*, così in parte sedando le inquietudini di quanti paventavano un uso spregiudicato di tali competenze in ambito sovrannazionale.

Non resta che auspicare un intervento del legislatore nazionale altrettanto ispirato ai principi di necessità e proporzionalità e caratterizzato da un approccio sistematico alla legislazione penale esistente, nell'ottica di eliminare sovrapposizioni e duplicazioni tra le fattispecie e rendere il quadro normativo in materia maggiormente coerente.

III. I PRINCIPI FONDANTI LA CIRCOLAZIONE INTERNAZIONALE DELLE INFORMAZIONI NELLO SPAZIO DI LIBERTÀ, SICUREZZA E GIUSTIZIA: A PROPOSITO DELLA COOPERAZIONE FRA LE AUTORITÀ NAZIONALI ED EUROPEE INCARICATE DELL'APPLICAZIONE DELLA LEGGE

di Nicoletta Parisi

Sommario: 1. Premessa. - **I. La dimensione garantista dello spazio europeo di giustizia**. **-** 2. Aspetti formali e sostanziali determinati dalla revisione di Lisbona. - 3. Le modifiche di tipo formale-istituzionale. In particolare: la riunificazione delle questioni relative alla costruzione di uno spazio di libertà, sicurezza e giustizia. - 4. *(Segue)* Una più marcata democratizzazione del processo decisionale. - 5. *(Segue)* Un più articolato controllo giurisdizionale. - 6. Il rapporto fra diversa elencazione dei fini dell'Organizzazione e catalogo dei diritti fondamentali dell'Unione europea. – 7. Le modifiche d'ordine sostanziale. In particolare: l'ampliamento di competenze normative ed operative dell'Unione nello spazio di libertà, sicurezza e giustizia. - 8. *(Segue)* Le responsabilità normative dell'Unione nella costruzione di uno spazio europeo di giustizia penale - **II. La sua dimensione securitaria**. **-** 9. La cooperazione europea di polizia. - 10. La stretta collaborazione fra le autorità incaricate dell'applicazione della legge negli Stati e nell'Unione … - 11. *(Segue)* L'impiego di nuove tecnologie: le banche-dati … - 12. … e la disciplina pertinente. In particolare: il principio di disponibilità delle informazioni. - **III. Le implicazioni per il rispetto dei diritti della persona. -** 13. I principi applicati entro l'ordinamento dell'Unione. - 14. A proposito di sicurezza versus libertà. - 15. La giurisprudenza internazionale europea in materia. **- IV. La riforma del sistema europeo di trattamento automatizzato dei dati personali**. **-** 16. Primi rilievi sulla prospettata riforma in materia.

1. Premessa

«(…) [L]a raccolta e soprattutto la conservazione, all'interno di gigantesche banche dati, di molteplici dati generati o trattati nell'ambito della maggior parte delle usuali comunicazioni elettroniche tra i cittadini dell'Unione costituisce una grave ingerenza nella loro vita privata, anche quando si limiti a creare le condizioni per un possibile controllo *ex* post delle loro attività personali e professionali. La raccolta di tali dati crea le condizioni per un controllo che, seppur esercitato soltanto a posteriori in occasione del loro impiego, minaccia tuttavia in modo permanente, per tutto il periodo della loro conservazione, il diritto dei cittadini dell'Unione alla riservatezza della loro vita privata. La diffusa sensazione di controllo così generata solleva in modo particolarmente acuto la questione del periodo di conservazione dei dati.

(…) A tal proposito, occorre anzitutto tener conto del fatto che gli effetti di tale ingerenza sono rafforzati dall'importanza acquisita dai mezzi di comunicazione elettronica nelle società moderne, che si tratti di reti digitali mobili o di *internet*, e dal loro utilizzo massiccio e intensivo da una parte molto cospicua dei cittadini europei in tutti i campi delle loro attività private o professionali».

Ho volutamente premesso al mio contributo le parole dell'Avvocato generale P. Cruz Villalón espresse nelle Conclusioni presentate alla Corte di giustizia dell'Unione europea il 12 dicembre 2013[151:] trattando, in particolare, dell'obbligo imposto alle autorità nazionali dalla direttiva 2006/24/CE di raccogliere e conservare dati tratti dal traffico telefonico per via elettronica[152] anche a fini di contrasto di condotte penalmente rilevanti, queste poche frasi riassumono la problematicità dell'intero contesto fattuale nel quale si colloca il principio di disponibilità delle informazioni, sostenuto dall'ordinamento dell'Unione europea come principio sottostante al tessuto della cooperazione fra le autorità nazionali ed europee incaricate dell'applicazione della legge, appunto a quegli stessi fini.

A partire da queste constatazioni il contributo si dipanerà trattando della componente garantista e della componente securitaria sottese alla cooperazione giudiziaria penale, di polizia, doganale e di *intelligence* e valutando le implicazioni per il rispetto dei diritti della persona derivanti dalla stretta cooperazione fra queste autorità e dal congiunto utilizzo delle moderne tecnologie informatiche.

I. LA DIMENSIONE GARANTISTA DELLO SPAZIO EUROPEO DI GIUSTIZIA

2. Aspetti formali e sostanziali determinati dalla revisione di Lisbona

La costruzione e il governo di uno spazio penale europeo si fondano su un'efficace azione di contrasto di condotte illecite «in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni»[153], con specifica attenzione anche alla «frode e [al]le altre attività illegali (...) [suscettibili di ledere] gli interessi finanziari dell'Unione»[154,] nonché a quelle pregiudizievoli per l' «attuazione efficace di una politica (...) in un settore (...) [già] oggetto di misure di armonizzazione»[155.]

Una così vasta azione esige, tra le altre misure, un dialogo fra le autorità coinvolte nell'applicazione della legge nella fase tanto della prevenzione quanto dell'esercizio dell'azione penale. Si tratta di un dialogo che deve vederle impegnate in una triplice direzione: una prima – orizzontale – organizzata fra le autorità degli Stati membri incaricati in ciascuno di essi di funzioni omologhe; una seconda – ancora orizzontale – sviluppata a livello transnazionale fra tutte queste autorità, titolari di compiti pur diversi ma indirizzati al medesimo scopo; una terza – verticale – coinvolgente esse e gli enti, organi e organismi via via istituiti entro l'Unione europea con finalità e funzioni per tanti aspetti analoghe a quelle conferite alle autorità nazionali. E' un dialogo necessitato perché imposto da esigenze di efficienza (dell'azione di contrasto al crimine) e di economia processuale (nell'amministrare la giustizia là dove sia più utile e dia maggiori garanzie di successo). Di queste necessità prende atto il Trattato sul funzionamento dell'Unione traducendole in diritto positivo[156.]

E' importante interrogarsi sulle modalità secondo le quali questo dialogo viene intessuto: non si può infatti escludere – anche sulla base di risultanze tratte dalla prassi di Stati pur di consolidata tradizione costituzionale – il rischio di un abbassamento delle garanzie individuali che, pur affermate e tutelate entro il singolo ordinamento nazionale quando si tratta di attività domestica, potrebbero essere aggirate nelle procedure di cooperazione transnazionale. Non occorre spendere molte parole per ricordare che queste ultime, quando intessute sul piano penale, sono state dall'origine e per tanto tempo (almeno fino alle soglie del XIX secolo) esclusivamente improntate alle necessità del reciproco sostegno fra sovranità; e che soltanto con l'introduzione della fase giurisdizionale, conseguente alla mutata

151 Causa C-293/12, *Digital Rights Ireland Ltd,* e causa C-594/12, *Kärntner Landesregierung,* punti 72-74.
152 Direttiva 2006/24/CE del 15 marzo 2006 *riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE* (*GUUE* L 105, 13 aprile 2006, p. 54 ss.).
153 Art. 83, n. 1, TFUE.
154 Art. 325, n. 1, TFUE.
155 Art. 83, n. 2, TFUE.
156 V. *infra*, par. 3.1.

funzione che sono state chiamate ad assolvere, hanno visto via via stemperata (ancorché non soppressa) quella primitiva funzione[157]. Quando queste forme di cooperazione interessano il piano delle attività di investigazione e di intelligence sono ancor oggi assai poco trasparenti, poiché improntate alla primaria esigenza di garantire, rispettivamente, l'ordine interno della comunità nazionale e la sicurezza internazionale dello Stato[158].

E' indubbio che, con la revisione di Lisbona, l'Unione europea abbia visto rafforzata la propria dimensione garantista anche nell'ambito dei settori che riguardano l'amministrazione della giustizia - che, come noto, concorrono alla costruzione dell'Organizzazione quale spazio di libertà, sicurezza e giustizia (SLSG)[159] - in virtù del gioco incrociato di fattori sia formali-istituzionali che sostanziali.

3. Le modifiche di tipo formale-istituzionale. In particolare: la riunificazione delle questioni relative alla costruzione di uno spazio di libertà, sicurezza e giustizia

Una prima importante modifica ascrivibile al campo delle revisioni istituzionali consiste nell'aver voluto eliminare formalmente la struttura in "pilastri" e, conseguentemente, nell'aver ricondotto tutte le competenze - anche quelle afferenti allo spazio di libertà, sicurezza e giustizia invece divise fra primo e terzo "pilastro" nella pregressa versione del Trattato di Unione - al cosiddetto "metodo comunitario", con la sola esclusione di quelle esercitate a titolo PESC/PESD[160].

Ciò sortisce una serie di conseguenze positive.

Anzitutto l'unificazione entro un unico "contenitore" - l'Unione - di tutte le materie funzionali alla costruzione e gestione dello Spazio di libertà, sicurezza e giustizia rappresenta una significativa razionalizzazione del sistema, la cui logica di ripartizione non era stata rigorosamente tracciata[161]. Si tratta di un assetto istituzionale e procedimentale che sembra già aver potuto consentire una sinergia fra le diverse anime che concorrono al conseguimento di questo obiettivo, contribuendo a mantenere un equilibrio fra esse, in particolare fra imperativi di libertà, emergenze dettate dalla ricerca della sicurezza e rafforzamento della tutela dei singoli; sinergia che il solo principio di coerenza[162] non è sembrato sufficiente a garantire per il passato.

Tuttavia non si può sottovalutare il rischio derivante da un elemento di incoerenza ancor oggi interno allo Spazio di libertà, sicurezza e giustizia, introdotto dalla decisione di ripartire in due diverse

---

157 Sui profili che contraddistinguono gli istituti della cooperazione giudiziaria internazionale in materia penale e sull'evoluzione codicistica di essi nell'ordinamento italiano si vedano P. LASZLOCZKY, *Rapporti giurisdizionali con autorità straniere*, in *DigPen*, XI (1996), p. 22 ss.; e M. PISANI, *Le coordinate*, in ID., *Temi e casi di procedura penale internazionale*, Milano (Led), 2001, pp. 33-42. A proposito del «qualcosa di nuovo» che avanza nel Continente europeo si veda A. GAITO, *Un processo penale verso il modello europeo,* in ID., *Procedura penale e garanzie europee*, Torino, 2006, pp. 1-9. Per un sintetico quadro di siffatta cooperazione nel Trattato costituzionale europeo (i cui contenuti, come noto, sono stati ampiamente ripresi dal Trattato di Lisbona) rinvio al solo V. GREVI, *Linee di cooperazione giudiziaria in materia penale nella Costituzione europea*, in *Studi in onore di Giorgio Marinucci*, Milano, 2006, III. vol., p. 2783 ss. Per un approfondimento della prassi attuale v. A. DAMATO, P. DE PASQUALE, N. PARISI, *Argomenti di diritto penale europeo*, Torino, 2014.

158 J.P. PIERINI, G. PASQUA, *Police cooperation in the European Union: an overview*, in M.CH. BASSIOUNI, V. MILITELLO, H. SATZGER (eds.), *European Cooperation in Penal Matters: Issues and Perspectives*, Padova, 2008, p. 403 ss.

159 L'obiettivo è espresso nell'art. 3, n. 2, TUE, ed è sostanziato dalle competenze attribuite *ex* artt. 4, n. 2, lett. j, e 67-89 TFUE.

160 Il settore relativo alla politica estera e di sicurezza comune è ancora soggetto alle logiche intergovernative (e dunque disciplinato interamente dal TUE – artt. 23-46 TUE - e non dal TFUE), sottratto al "metodo comunitario" dalla prospettiva sia delle procedure decisionali che del controllo giurisdizionale esercitato dalla Corte di giustizia dell'Unione europea. La problematicità dell'aver conservato quest'assetto deriva dall'intreccio di talune azioni PESC con le questioni interessate dallo SLSG: si pensi, se non altro, all'azione di contrasto al terrorismo transnazionale, come affrontata sulla base degli artt. 83 e 222 TFUE.

161 Come noto, in più di un'occasione nel passato è stata posta la questione di una ricognizione dei confini dell'azione della Comunità europea (oggi estinta in virtù del Trattato di Lisbona) a fronte di un'esercitata attività normativa dell'Unione ai sensi di competenze attribuite nei cd. secondo e terzo "pilastro", ambedue suscettibili di incidere tramite l'attività normativa delle istituzioni dell'Unione nelle materie afferenti allo spazio di libertà, sicurezza e giustizia. La Corte aveva risolto la questione sulla base di quanto disponeva l'allora art. 47 (oggi 40) TUE, nel senso di proteggere l'integrità del diritto comunitario: v. le sentenze sulla validità dell'azione comune PESC 2002/589 e della decisione-quadro 2005/667/GAI, rispettivamente del 20 maggio 2008, causa C-91/05, *Commissione c. Consiglio*, e del 23 ottobre 2007, causa C-440/05, *Commissione c. Consiglio*.

162 Oggi espresso nell'art. 7 TFUE, e reiteratamente affermato nei due Trattati: v. esemplificativamente artt. 11, n. 3; 13, n. 1; 16, n. 6, co. 3; 17, n. 6, TUE; 121, n. 3; 181, n. 1; 197, n. 3, lett. a); 256, n. 3, co. 2 e 3, TFUE. Un forte richiamo a migliorare la coerenza entro lo SLSG viene dal *Programma di Stoccolma,* adottato dal Consiglio GAI il 10-11 dicembre 2009 (*GUUE* C 115, 4 maggio 2010, punto 1).

direzioni generali della Commissione – con due diversi Responsabili, per di più appartenenti ad aree politiche non affini - le questioni riguardanti, da una parte, la "Giustizia" e, dall'altra, gli "Affari interni".

4. *(Segue)* Una più marcata democratizzazione del processo decisionale

Sul piano procedimentale l'assetto descritto consegue anche il risultato di sottoporre, in via di principio[163], la relativa attività normativa alla procedura legislativa ordinaria (che si modella sul pregresso procedimento di codecisione) aumentando il tasso di legittimazione democratica dell'Unione.

L'inventario degli atti tipici ai quali le istituzioni ricorrono è quello stabilito fin dalle origini per l'esercizio dell'attività normativa della Comunità economica europea, essendo così anche caduta l'esplicita esclusione circa la legittimità di atti suscettibili di esplicare effetti direttamente applicabili entro gli ordinamenti nazionali quando adottati in materie allora comprese entro il terzo "pilastro"[164]; e, anzi, prevedendosi un certo margine di discrezionalità in capo alle istituzioni circa l'adozione di «misure», dunque di atti normativi ai quali potrebbero essere anche ricollegati effetti diretti[165]; e, ancora, espressamente disponendosi in alcuni limitati casi l'adozione di regolamenti[166.]

Questa è modifica che marca una partecipazione più piena nell'esercizio della funzione normativa dell'istituzione depositaria dell'interesse corporativo (dei cittadini europei, ma anche di chi, pur straniero, ha diritto a uno statuto riconosciutogli dall'ordinamento dell'Unione), potendo così contribuire a migliorare l'equilibrio fra le esigenze garantistiche e securitarie, delle quali ultime sono principalmente depositari gli Stati membri e, dunque, l'organo che li rappresenta individualmente[167.]

Sempre nella direzione di una maggiore legittimazione democratica operano le disposizioni convenzionali che associano, in misura maggiore rispetto al passato, le assemblee parlamentari nazionali all'attività normativa europea, con particolare riguardo al rispetto dei principi di sussidiarietà e di proporzionalità[168,] sui quali di recente si è avuto occasione di registrare un'interessante prassi proprio in riferimento ad ambiti pertinenti allo spazio di libertà, sicurezza e giustizia specificamente a proposito dell'istituzione della Procura europea[169.]

---

163 Restano importanti eccezioni per questioni in ordine alle quali Consiglio e Parlamento europeo decidono secondo procedure legislative speciali che privilegiano l'apporto decisionale del primo: v. in partic. artt. 74; 77, n. 3, 78, n. 3; 81, n. 3; 86, n. 1; art. 87, n. 3, co. 1; 89 TFUE.

164 Presente invece nell'art. 34 TUE-versioni di Amsterdam e di Nizza.

165 L'art. 82, n. 2, co. 2, TFUE indica l'adozione di «misure» per facilitare il riconoscimento di decisioni giudiziarie e sentenze penali e per favorire la cooperazione di polizia e giudiziaria nelle materie penali aventi dimensione transnazionale; nello stesso senso dispone l'art. 84 TFUE, che disciplina il caso di «misure per incentivare e sostenere l'azione degli Stati membri nel campo della prevenzione della criminalità, ad esclusione di qualsiasi armonizzazione delle disposizioni legislative e regolamentari degli Stati membri» (v. anche *infra*, note 167 e 215). L'impiego del termine «misure» quale strumento utile al perseguimento delle tre principali competenze indica un'estesa discrezionalità conferita a Parlamento europeo e Consiglio, i quali possono ricorrere in tal modo sia ad atti di *soft law* come ad atti vincolati (e, fra essi, graduando fra disposizioni direttamente applicabili e non direttamente applicabili).

166 L'impiego del regolamento è previsto soltanto per l'approvazione della disciplina relativa alla costituzione e al funzionamento della Procura europea, di Eurojust e di Europol (rispettivamente artt. 86, n. 1, co.1; 85, n. 1, co. 2, e 88, n. 2, TFUE). Sulla questione, sottesa al discorso, relativa alla competenza penale diretta in capo alle istituzioni dell'Unione v., anche per una ricognizione del dibattito dottrinale in materia, D. RINOLDI, *Lo spazio di libertà, sicurezza e giustizia nel diritto dell'integrazione europea. I. Principi generali e aspetti penalistici*, Napoli, 2012, p. 207 ss.

167 Occorre tuttavia non sottovalutare la portata della clausola contenuta nell'artt. 82, n. 3, e 83, n. 3, TFUE, che tiene conto di quanto acquisito nel corso del negoziato del Trattato che adotta una Costituzione per l'Europa (29 ottobre 2004). Queste disposizioni consentono a ciascuno Stato membro di imporre una sospensione dell'attività normativa dell'Unione in materia di riconoscimento reciproco delle decisioni giudiziarie e delle sentenze penali, in materia di definizione dei reati e delle relative sanzioni, nonché di ravvicinamento delle disposizioni legislative e regolamentari penali nazionali in settori già oggetto di armonizzazione comunitaria, quando esso ritenga che «un progetto di direttiva [nelle materie indicate] (…) incida su aspetti fondamentali del proprio ordinamento giuridico penale»: sospesa la procedura legislativa ordinaria, il Consiglio europeo è investito della questione che viene risolta con il rinvio della procedura al Consiglio per l'adozione della delibera, ovvero – in caso di disaccordo ma con il consenso di almeno nove Stati membri – con l'avvio di un procedimento di cooperazione rafforzata. In modo analogo quanto all'assunzione di misure operative tra le autorità di polizia e le altre autorità incaricate negli Stati membri dell'applicazione della legge dispone l'art. 87, n. 3, co. 2, TFUE.

168 V. al riguardo gli artt. 12 TUE e 70 TFUE, nonché art. 8 Protocollo (n. 2).

169 A proposito dello "yellow card" opposto da tante amministrazioni nazionali alla proposta di regolamento istitutiva di una Procura europea (perché presuntivamente lesiva del principio di sussidiarietà) v. in termini riassuntivi dell'intera questione la Comunicazione della

5. *(Segue)* Un più articolato controllo giurisdizionale

Occorre inoltre segnalare che ai sensi della disciplina introdotta dal Trattato di Lisbona l'attività normativa dell'Unione in materia penale e, conseguentemente ad essa, quella degli Stati membri che intervenga in suo adempimento sono oggi soggette pienamente[170] al controllo della Corte di giustizia, dalla prospettiva del vaglio, rispettivamente, della sua legalità e del pieno dispiegarsi dei suoi effetti entro gli ordinamenti nazionali. Si aggiunga che tale vaglio si avvale di un parametro di legalità costituito dalla Carta dei diritti fondamentali; e che questo parametro uscirà sicuramente rafforzato dall'adesione dell'Unione alla Convenzione europea dei diritti dell'uomo[171.] E' questo un dato assai rilevante se si considera che, come si vedrà, con la revisione di Lisbona le competenze comuni sono suscettibili di incidere nella condizione della persona in misura ancora maggiore di quanto non sia stato nel passato.

A questa estensione materiale delle competenze della Corte si affianca un'ampliata legittimazione attiva delle persone fisiche (nonché giuridiche) per l'apprezzamento della legittimità della normativa dell'Unione[172,] e una maggior rapidità di decisione su rinvio pregiudiziale per la sua interpretazione e validità quando la Corte si trovi a dover affrontare situazioni che si caratterizzano per l'urgenza della loro soluzione o che riguardano persone detenute in uno degli Stati membri[173.]

6. Il rapporto fra diversa elencazione dei fini dell'Organizzazione e catalogo dei diritti fondamentali dell'Unione europea

In funzione di cerniera fra revisioni d'ordine istituzionale e d'ordine sostanziale sta un dato che ne rappresenta il necessario punto di snodo. Con la riforma dei Trattati istitutivi dell'Unione gli Stati membri hanno voluto ribaltare l'ordine dei fini dell'Organizzazione espressi in essi: ordine che fino ad allora[174] aveva dato conto, in relazione al loro ampliarsi, di una logica di tipo cronologico e dunque facendo seguire, nelle relative disposizioni convenzionali, agli obiettivi mercantili (la costruzione di un mercato interno) fini più squisitamente politici che erano venuti aggiungendosi a partire (timidamente) dall'Atto Unico europeo e (infine più convincentemente) dal Trattato di Maastricht, quali il perseguimento della sicurezza interna ("pilastro giustizia e affari interni") e internazionale ("pilastro PESC/PESD") degli Stati membri e dell'Unione europea.

Oggi l'art. 3 TUE lega al fine generale relativo alla promozione della pace, dei valori dell'Unione e del benessere dei popoli degli Stati membri (n. 1) quello che può essere considerato per certi aspetti una sua specificazione sul piano interno dell'Organizzazione, ovvero il conseguimento di uno spazio europeo di libertà, sicurezza e giustizia (n. 2); solo dopo vengono indicate le originarie finalità mercantili (n. 3) articolate in successivi obiettivi quali specificamente il conseguimento di un'unione economica e monetaria (n. 4), per poi terminare con l'indicazione dell'obiettivo relativo alla dimensione internazionale dell'Unione (n. 5)

La descritta inversione di priorità fra fini mercantili e fini ispirati al principio personalistico non può essere considerata casuale, bensì l'immediata traduzione da parte dei Paesi membri della propria volontà di considerare l'Unione europea quale ente di governo fondato sui «valori del rispetto della dignità umana, della libertà, della democrazia, dell'eguaglianza, dello Stato di diritto, della democrazia e

---

Commissione *on the review of the proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office with regard to the principle of subsidiarity, in accordance with Protocol No 2*, COM(2013) 851 final, 27 novembre 2013.

170 Occorre tener conto tuttavia che per gli atti adottati prima dell'entrata in vigore del Trattato il controllo della Corte si estenderà nelle modalità descritte soltanto dopo un periodo di cinque anni dall'entrata in vigore del Trattato di Lisbona: art. 10, nn. 1 e 3 Protocollo (n. 36) sulle disposizioni transitorie.

171 Art. 6, n. 2, TUE. Sulla questione del rapporto fra le diverse fonti di tutela dei diritti dell'uomo nell'ordinamento dell'Unione (Carta di Nizza, CEDU, tradizioni costituzionali comuni agli Stati membri) mi permetto di rinviare al mio *Funzione e ruolo della Carta dei diritti fondamentali nel sistema delle fonti alla luce del Trattato di Lisbona*, in *DUE*, 2009, p. 653 ss.

172 Art. 263 TFUE.

173 Il nuovo procedimento di cui all'art. 267, n. 4, TFUE si salda con la riforma del regolamento di procedura della Corte che ha introdotto - a partire dal 1° marzo 2008 – il rinvio d'urgenza per le materie afferenti lo spazio di libertà sicurezza e giustizia.

174 Art. B TUE-versione di Maastricht; art. 2 TUE-versione di Amsterdam e di Nizza.

del rispetto dei diritti umani (...)», come espressi nell'art. 2 TUE, così da rendere esplicito che ogni altra politica comune deve essere dipanata nel quadro del loro rispetto.

L'indicata motivazione sottesa all'inversione nell'elencazione dei fini dell'Organizzazione sembra poter essere corroborata da un altro dato testuale. Non si tratta soltanto del fatto che si è voluti addivenire all'adozione di un catalogo di diritti fondamentali proprio dell'Unione. Si tratta anche di alcune precipue caratteristiche di questo catalogo, prime fra tutte quella che - innovando rispetto alle tradizionali modalità utilizzate nel diritto internazionale – vede per la Carta di Nizza-Strasburgo l'impiego di una tecnica redazionale alla cui base è posto il principio dell'indivisibilità dei diritti, siano essi di libertà, civili, giudiziari, economici, sociali o culturali[175]: fra tutti essi viene attuata una pari-ordinazione intorno al valore centrale della dignità della persona[176], non espresso nemmeno nello strumento normativo principe per l'Europa, la Convenzione di salvaguardia del 4 novembre 1950. Tale assetto si traduce sul piano sostanziale in una più incisiva e uniforme tutela di tutti essi, che, a motivo di questa loro pariordinazione, si sostengono ed entrano in bilanciamento come termini paritari e non gerarchicamente ordinati.

Per la materia che qui interessa, vengono in rilievo anzitutto i diritti raccolti entro il Titolo VI della Carta, intitolato alla "Giustizia", dunque le disposizioni che, nell'amministrazione della giustizia penale, garantiscono il diritto a un ricorso effettivo e a un giudice imparziale (art. 47), la presunzione di innocenza (art. 48, n. 1), i diritti della difesa (art. 48, n. 2), il principio di legalità e di proporzionalità dei reati e delle pene (art. 49) e di *ne bis in idem* (art. 50). A fianco a questi vengono in rilievo i diritti alla libertà e alla sicurezza personali (art. 6), presidiati dalla norma che tutela l'inviolabilità della dignità umana (art. 1), esplicitamente protetta da tortura e trattamenti inumani e degradanti, nonché dall'applicazione ed esecuzione della pena di morte (artt. 3-4) anche quando questa derivi dalla consegna della persona a situazioni di tal fatta che si producano fuori dai confini nazionali (art. 19). Né minore importanza assumono i principi di eguaglianza formale davanti alla legge (art. 20) e di non discriminazione (art. 21). Sempre ai fini della materia che qui si intende approfondire viene infine in rilievo la norma che protegge la vita privata della persona anche a fronte del trattamento che dei suoi dati personali possa essere fatto tanto dalle pubbliche autorità che da privati (art. 8). Com'è agevole notare da una piana interpretazione del disposto delle norme richiamate, tutte esse si indirizzano alla protezione della persona, e non del cittadino o del residente, ciò implicando che abbia diritto a fruirne chiunque sia raggiunto dalla giurisdizione dell'Unione (o degli Stati membri «nell'attuazione del diritto dell'Unione»[177]).

A quanto detto si aggiunge che, con il Trattato di Lisbona, la Carta dei diritti fondamentali assume anche formalmente valore giuridicamente vincolante: la portata delle sue norme è assimilata espressamente a quelle di natura convenzionale contenute nei Trattati istitutivi e di funzionamento dell'Unione europea. Nelle more dell'entrata in vigore del Trattato di Lisbona è stata da molti valutata l'importanza e l'utilità di siffatta norma - che, tra l'altro, accompagnandosi all'art. 6, n. 2, TUE, ha fatto venire meno gli impedimenti giuridici che per il passato avevano precluso l'adesione della stessa Unione alla Convenzione di salvaguardia[178] -, dandone diverse giustificazioni. Qui non interessa entrare nel

---

175 In verità il principio della indivisibilità è immanente nella stessa categoria concettuale del diritto fondamentale (così A. FACCHI, *Breve storia dei diritti umani*, Bologna-Roma, 2007, pp. 125-127). Tuttavia la sua concreta utilizzabilità è stata sempre negata a livello internazionale; in particolare, ascrivendo i diritti economico-sociali alla sfera dei diritti programmatici, si è considerato necessario affidarne la tutela a meccanismi internazionali di garanzia meno significativi (perché meno incidenti nell'ambito della libera determinazione delle autorità politiche nazionali) rispetto a quelli predisposti per i diritti di libertà, civili e politici; e se è conseguentemente scorporata la compilazione in uno strumento specificamente ad essi dedicato.

176 Art. 1 Carta dei diritti fondamentali.

177 Art. 51 Carta dei diritti fondamentali. Sul significato di tale ultima disposizione la giurisprudenza della Corte di giustizia europea è ormai assai articolata: a suo commento si rinvia a K. LENAERTS, *The EU Charter of Fundamental Rights: Scope of Application and Methods of Interpretation,* in *De Rome à Lisbonne: les juridictions de l'Union européenne à la croisée des chemins*, Bruxelles, 2013, p. 107 ss.

178 Esplicitati nel parere CGUE 28 marzo 1996, n. 2/94. La Corte di giustizia dell'Unione europea ha visto di recente sottoporre alla propria competenza consultiva il progetto di accordo di adesione dell'Organizzazione alla Convenzione europea dei diritti dell'uomo (appunto legittimata dall'art. 6, n. 2, TUE), sulla cui utilità e perfezionabilità v. A. TIZZANO, *Les Cours européennes et l'adhésion del l'Union à la CEDH,* in *DUE,* 2011, p. 29 ss.; V. PETRALIA, *L'adesione dell'Unione europea alla Convenzione europea dei diritti dell'uomo*, in N. PARISI, V. PETRALIA (a cura di), *L'Unione europea dopo il Trattato di Lisbona*, cit., p. 287 ss.; e L. CARRASCO MARCO, *Adhesión de la Unión Europea al Convenio Europeo de Derechos Humanos*, Editorial Académica Española, 2013.

ricco dibattito in argomento[179], quanto piuttosto registrare che le evoluzioni istituzionali conseguenti alla revisione di Lisbona hanno consentito di aggiungere a quelle valutazioni prospettiche la constatazione di una effettiva miglior tutela dei diritti della persona, in virtù tanto di una prassi delle istituzioni normative, quanto di una giurisprudenza che (risolti i dubbi sulla portata giuridica delle norme della Carta[180]) ha potuto finalmente valorizzarne le implicazioni[181].

Si aggiunge che l'azione dell'Unione nella sua globalità è incardinata entro un contesto di osservanza dei diritti e delle libertà fondamentali delle persone che ha come punti di riferimento normativo la Convenzione europea dei diritti dell'uomo e le tradizioni costituzionali comuni agli Stati membri[182]. A tutto ciò si affianca un ormai diffuso e proficuo dialogo fra le corti internazionali europee e nazionali[183], che si è dimostrato capace di valorizzare l'applicazione di un alto *standard* di rispetto di diritti e libertà individuali fondamentali[184].

7. Le modifiche d'ordine sostanziale. In particolare: l'ampliamento di competenze normative ed operative dell'Unione nello spazio di libertà, sicurezza e giustizia

Il rafforzato sistema di garanzie – attuato sia tramite correzioni istituzionali che tramite il menzionato spostamento del baricentro dell'Unione dal dato mercantile al principio personalistico indotto dalla centralità assunta dalla Carta dei diritti fondamentali – è in grado di sorreggere credibilmente l'aumentata responsabilità dell'Organizzazione nella costruzione e, poi, nell'amministrazione di uno spazio di libertà, sicurezza e giustizia.

Si tratta, com'è evidente, di un terreno ove la tutela dei diritti e delle libertà fondamentali della persona si presenta costantemente, in modo talvolta anche drammatico; ed è questo un ambito che contribuisce ad affrancare l'attività dell'Unione dalla mera prospettiva del buon funzionamento del mercato interno, per assumere una dimensione generale, senza con ciò contraddire l'assunto secondo il quale essa opera sulla base del principio di attribuzione delle competenze.

---

179 Sulla Carta come strumento di visibilità politica dell'Unione in relazione all'obiettivo SLSG v., fra i tanti, A. TORRES PÉREZ, *The Dual System of Rights Protection in the European Union in Light of US Federalism,* in E. CLOOTS, G. DE PAERE, S. SOTTIAUX (eds.), *Federalism in the European Union*, Oxford-Portland, 2012, p. 110 ss. Sui valori condivisi sottostanti v. U. VILLANI, *Valori comuni e rilevanza delle identità nazionali e locali nel processo d'integrazione europea*, Napoli, 2011. Sul costante puntuale richiamo della Corte di giustizia al rispetto dei principi di democrazia, libertà, Stato di diritto e tutela dei diritti fondamentali della persona rinvio al mio *Ancora in tema di riconoscimento reciproco e principio di stretta legalità penale nell'Unione europea: alcune considerazioni a partire dal Trattato di Lisbona*, in *Studi in onore di Mario Romano*, Napoli, 2011, p. 2541 ss. Sul processo di costituzionalizzazione dell'Unione tramite la Carta v. K. BLAIRON, *La Carta dei diritti fondamentali dell'Unione europea: verso la costituzionalizzazione di un* "diritto comune europeo"*?,* in S. GAMBINO (a cura di), *Trattato che adotta una costituzione per l'Europa, costituzioni nazionali, diritti fondamentali*, Milano, 2006, p. 225 ss.. Sul fatto che con la redazione di un catalogo di diritti fondamentali si sia conseguito un rafforzamento del principio di certezza del diritto entro l'Unione, pur senza accantonare la tutela in via pretoria — così ben articolata sul piano giurisprudenziale a partire dalla sentenza *Stauder* (CGCE, sentenza 12 novembre 1969, causa 29/69) —, grazie al saldo ancoramento alla giurisprudenza della Corte di giustizia delle Comunità (oltre che a quella della Corte di Strasburgo) secondo il chiaro disposto del 5° cpv. Preambolo e degli artt. 52, n. 3 e 53 Carta di Nizza; nonché sul fatto che l'attività di codificazione sia stata accompagnata dall'intento di contribuire all'evoluzione progressiva del diritto v. mio *Funzione e ruolo della Carta*, cit. Sul costante puntuale richiamo della Corte di giustizia al rispetto dei principi di democrazia, libertà, Stato di diritto e tutela dei diritti fondamentali della persona rinvio al mio *Ancora in tema di riconoscimento reciproco e principio di stretta legalità penale nell'Unione europea: alcune considerazioni a partire dal Trattato di Lisbona*, in *Studi in onore di Mario Romano*, Napoli, 2011, p. 2541 ss.

180 V. op. ult. cit.

181 Al proposito v. A. ROISAS, H. KAILA, *L'application de la Charte des droits fondamentaux de l'Union européenne par la Cour de Justice: un premier bilan,* in *DUE*, 2011, p. 1 ss.

182 Art. 6, n. 3, TUE (in attesa che la Convenzione di salvaguardia diventi fonte normativa interna all'Unione *ex* art. 6, n. 2, TUE).

183 Il tema è assai esplorato e non solo in tempi recenti. V. anche in termini ricognitivi della precedente dottrina G. MARTINICO, O. POLLICINO (eds.), *The National Judicial Treatment of the ECHR and EU Laws. A Comparative Constitutional Perspective*, Groningen, 2010; IDD., *The Interaction between Europe's Legal Systems. Judicial Dialogue and the Creation of Supranational Laws*, Cheltenham-Northampton, 2012.

184 Sul circuito virtuoso che si è innestato nella tutela dei diritti a partire dal dialogo fra le Corti internazionali europee e nazionali, v. fra i molti: M. DELMAS-MARTY, *Le pluralisme ordonné. Les forces imaginantes du droit,* Paris, 2006; A. TIZZANO, *Introduzione alla sessione: La tutela dei diritti nell'Unione europea*, in N. PARISI, V. PETRALIA (a cura di), *L'Unione europea dopo il Trattato di Lisbona,* cit., p. 161 ss.; L. POTVIN-SOLIS (sous la dir. de), *Le principe d'autonomie et le dialogue entre les juridictions nationales et européennes dans la conciliation des droits et libertés*, in ID., *La conciliation des droits et libertés dans l'ordre juridiques européens,* Bruxelles, 2012, p. 509 ss.; U. VILLANI, *La cooperazione tra i giudici nazionali, la Corte di giustizia dell'Unione europea e la Corte europea dei diritti dell'uomo*, in M. FRAGOLA (a cura di), *La cooperazione fra Corti in Europa nella tutela dei diritti dell'uomo*, Napoli, 2012, p. 1 ss.

Si tenga conto che la responsabilità di cui qui si tratta si sostanzia nel coerentemente gestire uno "spazio" che richiede l'esercizio di competenze normative (e, seppure in misura più limitata, operative) assai estese, dovendo a questo titolo l'Unione intervenire in materia di immigrazione, asilo, rifugiati, diritto internazionale privato, armonizzazione del diritto (sostanziale e strumentale) penale, cooperazione fra le autorità nazionali nell'amministrazione della giustizia civile e penale, nonché nell'attività di prevenzione del crimine, da attuarsi anche attraverso il coordinamento di azioni di polizia, doganali e di *intelligence*.

8. *(Segue)* Le responsabilità normative dell'Unione nella costruzione di uno spazio europeo di giustizia penale

Se poi si considera il solo spazio penale europeo, l'ampliamento delle responsabilità dell'Unione risulta evidente: con la revisione di Lisbona si assiste a un aumento delle forme di criminalità in relazione alle quali l'Unione deve esercitare poteri normativi in funzione di loro contrasto.

E' anzitutto caduto il riferimento alla criminalità organizzata, sostituito dall'indicazione di «sfere di criminalità particolarmente grave» di «dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni»[185]. La vaghezza e indeterminatezza delle espressioni impiegate nelle norme che riguardano l'esercizio delle competenze in materia penalistica[186] determina un potenzialmente indifferenziato ambito di intervento dell'Unione, sebbene esso sia circoscritto da un'elencazione che in prima battuta sembra rivestita del carattere della tassatività; a parte la considerazione che l'inventario tracciato è ben più ampio rispetto alle indicazioni contenute nel pregresso TUE[187], non si può evitare di considerare anche che esso è passibile di ampliamento per decisione del Consiglio, in relazione alle evoluzioni del fenomeno criminoso[188].

Sempre a proposito delle aumentate competenze normative dell'Unione utili alla costruzione di uno spazio di giustizia penale, occorre infine considerare come il cerchio idealmente si chiuda con la previsione di una forte componente garantistica sostenuta dall'adozione di direttive contenenti norme minime in materia di diritto processuale, quando ciò si renda necessario «per facilitare il riconoscimento delle sentenze e delle decisioni giudiziarie nelle materie penali aventi dimensione transnazionale»[189]: gli Stati hanno così conferito una competenza fondata su una più certa base giuridica rispetto a quella individuabile nelle precedenti versioni dei Trattati europei e comunitari[190] e tendenzialmente indeterminata, come la prassi sta dimostrando.

Occorre qui una seppure sintetica digressione relativa al principio di mutuo riconoscimento implicato dalla disposizione in questione, per consentire di apprezzare l'importanza della menzionata previsione. E' noto che la premessa sulla quale si fonda l'operare del reciproco riconoscimento è l'esistenza di una *confiance mutuelle* che ciascuno Stato dovrebbe poter riporre negli ordinamenti degli altri Paesi membri dell'Unione da una duplice prospettiva: sul piano legislativo, quanto all'adeguatezza della normativa nazionale in materia penale sia sostanziale che processuale; sul piano esecutivo e giudiziario, in ordine alla corretta applicazione di quest'ultima da parte degli organi interni a ciò preposti[191]. Tale

185 Art. 83, n. 1, co. 1, TFUE.
186 Al proposito v. D. RINOLDI, *Lo spazio di libertà, sicurezza e giustizia nel diritto dell'integrazione europea*, cit., pp. 199 ss., 214 e 285.
187 Art. 29, n. 1, co. 2, TUE-versioni di Amsterdam e Nizza; oggi art. 83, n. 1, co. 2, TFUE.
188 Art. 83, n. 1, co. 3, TFUE.
189 Art. 82, n. 2, co. 1, TFUE.
190 Ci si riferisce agli artt. K.1, co. 2, 3 al., e K.3, lett. c), TUE-versione di Maastricht (ove la previsione di siffatta armonizzazione era assai implicita); e agli artt. 29, co. 2, 3 al., e 31, lett. c, TUE- versioni di Amsterdam e di Nizza.
191 Ciò è ben chiarito dall'Avvocato generale Ruiz-Jarabo Colomer, allorché spiega che la «nozione [di reciproca fiducia], sebbene recente nella costruzione di una giustizia penale europea, rientra nel principio del reciproco riconoscimento, introdotto al punto 33 delle conclusioni del Consiglio europeo di Tampere del 16 ottobre 1999» (in causa C-297/07, *Bourquain).* Continua lo stesso Avvocato generale*:* il reciproco riconoscimento opera un collegamento fra ordinamenti che «non si instaura tra compartimenti stagni, essendo necessaria una verifica *ad casum,* volta ad assicurare che la prestazione dell'assistenza richiesta non comporti un'inosservanza dei princìpi fondamentali dell'organizzazione sociale»; esso si instaura invece quando «si desidera prestare appoggio a chi condivide gli *stessi principi, valori ed impegni*, costruendo una struttura istituzionale dotata di proprie fonti del diritto, di efficacia diversa, ma pur sempre vincolanti, che mirano a

reciproca fiducia nei rispettivi sistemi di giustizia penale comporta che ciascuno Stato membro «accetti l'applicazione del diritto penale vigente negli altri Stati contraenti, anche quando il ricorso al proprio diritto nazionale condurrebbe a soluzioni diverse»[192].

Nella prospettiva, qui utilizzata, di valutazione dello spessore della dimensione garantista dell'Unione europea, occorre considerare un altro piano della *confiance mutuelle* implicata: è un piano che prescinde dal rapporto di cooperazione fra enti, riguardando invece quello relativo ai rapporti fra persona e Unione. Si vuole cioè dire che la normativa europea di contrasto al crimine attuata mediante l'utilizzo del principio di riconoscimento reciproco risulta accettabile alla luce dei principi dello Stato di diritto se è indirizzata anche a consentire che i cittadini europei (e, più latamente, ogni persona implicata in un procedimento penale) possa riporre fiducia nell'ordinamento dell'Unione[193.]

Il fondamento della reciproca fiducia (fra Stati; fra persone ed Unione) - capace di far funzionare la *full faith and credit clause* anche entro l'ordinamento dell'Unione, al pari di quanto accade negli ordinamenti di tipo federale – viene individuato nei valori e principi espressi, rispettivamente, dagli artt. 2 e 6, par.1, TUE, come rilevati dalla Corte di giustizia e condivisi da tutti gli Stati membri in quanto comuni ad essi (perché originati dalle tradizioni costituzionali comuni e dalle vigenti norme internazionali pertinenti).

Da parte di alcuni studiosi si reputa che, così fondata, la reciproca fiducia sia concetto dai confini ancora molto sfumati dal momento che nello spazio europeo esistono non trascurabili differenziali di tutela fra gli ordinamenti nazionali e livelli non omogenei di diritti e libertà della persona. Se tuttavia si guarda alla prassi giurisprudenziale interna e internazionale europea è possibile sostenere che già da tempo esista e operi un «meccanismo idoneo a creare una fiducia reciproca»[194,] rappresentato dalla Convenzione europea dei diritti dell'uomo, strumento vivente, continuamente adattato all'evoluzione della società europea ad opera della Corte che presiede alla sua interpretazione e applicazione anche entro gli Stati membri dell'Unione. La Convenzione, infatti, pretende di conseguire la conformità (non l'uniformità) della tutela assicurata in ciascun ordinamento nazionale ai diritti da essa garantiti e agli *standards* via via individuati dalla Corte europea nell'attività di interpretazione della Convenzione stessa; quest'ultima, per ciò stesso, presuppone livelli di tutela sostanzialmente equivalenti.

Tuttavia è pure evidente come tale garanzia non sia, di per sé sola, pienamente appagante, allorché ci si situa sul terreno del diritto penale; la Convenzione, così come la Carta di Nizza-Strasburgo che alla tutela ivi espressa si ispira, non esclude (anzi auspica) che ciascuno Stato voglia garantire un livello di tutela superiore e dunque, per ciò stesso, pone le premesse di una diminuita fiducia in questo o quell'ordinamento di altro Stato, anche in relazione a singole situazioni: ciò, infine, determinerebbe un ostacolo – certo non generalizzato, ma pur sempre operante – al funzionamento del principio di reciproco riconoscimento, pur nella consapevolezza di una generale equivalenza fra ordinamenti nazionali e del buon funzionamento del sistema europeo di tutela messo in campo dalla Convenzione europea dei diritti dell'uomo, ma pur sempre successivo, capace cioè di intervenire a violazione perpetrata. In questo senso ragiona, per esempio la Corte di Cassazione italiana quando – nel valutare la compatibilità fra i sistemi (italiano e tedesco) relativi alle misure detentive cautelari a fine di esecuzione del mandato d'arresto europeo – osserva che occorre anzitutto «sfuggire alla tentazione di parametrare al significato di nozioni ed espressioni evocative di precisi istituti dell'ordinamento interno dettati normativi concepiti dal legislatore italiano ai fini di una loro proiezione interstatuale»; occorre poi «verificare se l'ordinamento processuale dello Stato di emissione offra (…) "garanzie equivalenti" a quelle derivanti dal nostro sistema di termini di durata massima della custodia», ma nel contempo anche

---

prevenire e combattere la criminalità, in uno *spazio comune di libertà, di sicurezza e di giustizia*, mediante la facilitazione della cooperazione tra gli Stati membri e l'armonizzazione delle loro normative in materia penale» (Conclusioni in causa C-303/05, *Advocated voor de Wereld VZW*; corsivi aggiunti).

192 Sentenze 11 febbraio 2003, cause riunite C-187/01 e C-385/01, *Gözütok e Brügge*, punto 33; 28 settembre 2006, causa C-150/05, *Van Straaten*, punto 43; 11 dicembre 2008, causa C-297/07, *Bourquain*, punto 37.

193 Così anche Cons., *Programma di Stoccolma*, cit., punti 2.4. e 1.1.

194 Comm., *Libro verde sulle garanzie procedurali a favore di indagati e imputati in procedimenti penali nel territorio dell'Unione europea*, COM(2003)75 def., parr. 1.7 e 2.5

«puntualmente verificare se le ben determinate condizioni che si sono appena precisate siano in concreto soddisfatte dalla legislazione di quello Stato»[195].

Risulta perciò immediatamente evidente come la reciproca fiducia abbia una doppia faccia: essa è il presupposto del funzionamento del reciproco riconoscimento e, contemporaneamente, un obiettivo da conseguire al fine di consentirne il fisiologico funzionamento. Sebbene, dunque, il ravvicinamento normativo non sia finalità propria degli strumenti internazionali di tutela dei diritti della persona nonché di quelli di cooperazione giudiziaria penale e, ancora, sebbene il Trattato di Unione sembri per certi aspetti privilegiare il reciproco riconoscimento a vantaggio dell'armonizzazione del diritto[196], una motivazione d'ordine logico consiglia di perseguire parallelamente la via della più stretta cooperazione tra le autorità nazionali ed europee e quella dell'armonizzazione delle normative nazionali procedurali e sostanziali, valorizzando tanto la reciproca autonomia quanto la loro complementarità ai fini della creazione di uno spazio penale europeo. Non a caso nel corso dei lavori che, infine, portarono alla redazione del progetto di Trattato costituzionale si propose la previsione di un nuovo criterio utile a legittimare l'attività di armonizzazione delle norme nazionali penali sostanziali svolta dalle istituzioni dell'Unione: a ciò ci si sarebbe dovuti determinare «quando il ravvicinamento (…) [fosse risultato] necessario per suscitare una mutua fiducia sufficiente a permettere la piena applicazione del mutuo riconoscimento delle decisioni giudiziarie o per garantire l'efficacia degli strumenti comuni di cooperazione di polizia o giudiziaria predisposti dall'Unione»[197]: formula più ampia di quella accolta nell'attuale norma convenzionale da essa originata[198].

A questa stessa logica risponde, dunque, la predisposizione di norme minime sulle garanzie processuali - dalle quali questo lungo ragionamento ha preso le mosse -, le quali, da una parte, siano capaci di «accrescere la fiducia reciproca negli ordinamenti giudiziari degli Stati membri», dall'altra possano rappresentare il «logico contrappeso ad altre misure di riconoscimento reciproco»[199].

Su questo fronte il lavoro normativo è già iniziato, ancorché l'obiettivo sia ben più denso di aspettative di quanto proposto dalla Tabella di marcia adottata dal Consiglio[200]. Il suddetto processo di armonizzazione delle garanzie procedurali delle persone coinvolte in procedimenti penali (di respiro sia meramente interno che transnazionale) si segnala per la decisione (non del tutto scontata all'inizio del processo normativo in questione) di prendere in conto anche la fase che precede il processo penale in senso stretto, dunque anche quella relativa all'investigazione e all'esercizio di altre competenze da parte delle autorità nazionali di polizia, alla quale vengono allargate le garanzie processuali tipicamente utilizzate nella fase dell'esercizio dell'azione penale[201].

---

195 S.U., 30 gennaio 2007-5 febbraio 2007, n. 4614, punto 9.

196 Sulla portata non esattamente coincidente degli artt. 67, n. 3, e 82, n. 1, v. D. RINOLDI, *Introduzione. Per un diritto penale europeo: i Trattati di Unione e sul suo funzionamento nonché la Carta dei diritti fondamentali,* in A. DAMATO, P. DE PASQUALE, N. PARISI, *Argomenti*, cit., par. 3.1.

197 Rapporto finale del Gruppo di lavoro X, 2 dicembre 2002, p. 10.

198 *Supra*, nota 189.

199 Così *Libro verde sulle garanzie procedurali*, cit.

200 La risoluzione del Consiglio (del 30 novembre 2009) *relativa a una tabella di marcia per il rafforzamento dei diritti procedurali di indagati o imputati in procedimenti penali*: ha avviato il processo di adozione di direttive indirizzate a stabilire uno *standard* minimo di tutela per la persona in tutti gli ordinamenti degli Stati membri dell'Unione (rimettendo allo Stato membro la decisione «di mantenere o introdurre un livello più elevato di tutela delle persone»: art. 82, par. 2, TFUE). Sono vigenti le direttive del Parlamento europeo e del Consiglio 2010/64/UE del 20 ottobre 2010 *sul diritto all'interpretazione e alla traduzione nei procedimenti penali;* 2012/13/UE del 22 maggio 2012 *sul diritto all'informazione nei procedimenti penali;* del 22 ottobre 2013 *relativa al diritto di avvalersi di un difensore nel procedimento penale e nel procedimento di esecuzione del mandato d'arresto europeo, al diritto di informare un terzo al momento della privazione della libertà personale e al diritto delle persone private della libertà personale di comunicare con terzi e con le autorità consolari.* Con la Comunicazione del 27 novembre 2013 *Progredire nell'attuazione dell'agenda dell'Unione europea sulle garanzie procedurali per indagati e imputati — Rafforzare le basi dello spazio europeo di giustizia,* COM(2013) 820 final, la Commissione propone cinque nuove misure: tre proposte di direttiva sul rafforzamento della presunzione di innocenza (COM(2013) 821 final), sulle garanzie procedurali di minori imputati e indagati (COM(2013) 822 final), sull'ammissione provvisoria al patrocinio a spese dello Stato per indagati e imputati (COM(2013) 824 final), accompagnate da due raccomandazioni sulle due ultime questioni (*GUUE* L 378, 24 dicembre 2013, pp. 8 ss. e 1 ss.). Sul processo in atto fra i tanti contributi v. N. PARISI, *Tecniche di costruzione di uno spazio penale europeo. In tema di reciproco riconoscimento delle decisioni giudiziarie e di armonizzazione delle garanzie processuali,* in *St. int. eur.*, 2012, p. 33 ss.; S. MIETTINEN, *Criminal Law and Policy in the European Union*, London-New York, 2013, p. 199 ss.

201 Significativo al proposito è l'Annesso I della seconda direttiva di armonizzazione, intervenuta in materia di diritto all'informazione nei procedimenti penali: essa, nel predisporre ad uso delle autorità giudiziarie nazionali una "model letter of rights" in cui sono contenuti appunto i diritti di cui devono godere le persone coinvolte nel procedimento, elenca: "assistance of a lawyer", "information about the accusation", "right to remain in silent" («while questioned by the Police and judicial authorities»), "informing someone else about

Occorre infine aggiungere che le direttive attuali e le decisioni quadro che hanno accolto già prima della riforma di Lisbona il principio del mutuo riconoscimento sono intervenute esse stesse con un'attività di armonizzazione del diritto penale nazionale, sia sostanziale (per quanto riguarda i principi che stabiliscono garanzie anche non processuali a favore delle persone coinvolte nel procedimento) che procedurale (per esempio quanto ai termini entro i quali il provvedimento dello Stato richiedente deve essere eseguito), contribuendo a rafforzare la dimensione garantista dello spazio di giustizia penale.

II. LA SUA DIMENSIONE SECURITARIA

9. La cooperazione europea di polizia

Passando a trattare dell'ambito della sicurezza - come espresso negli artt. 3, n. 2, TUE e 67, n. 3, TFUE - è palese l'asimmetria sul fronte garantistico rispetto all'ambito della giustizia. Quanto sino ad ora scritto dà conto, infatti, di un sicuro rafforzamento della tutela dei diritti della persona nello spazio europeo di giustizia penale; rafforzamento non ugualmente conseguito nella politica comune di sicurezza, ove si registra un avanzamento a tappe che certo non possono essere apprezzate come forzate. Allo stato vi sono soltanto sintomi dell'avvio di un processo di bilanciamento fra esigenze della sicurezza (interna e internazionale degli Stati e dell'Unione) e rispetto dei diritti fondamentali della persona.

Un primo segnale può essere rintracciato nelle norme europee che ormai da tempo tendono a incardinare alcune di tali forme entro il perimetro della cooperazione giudiziaria penale, mentre, come noto, le modalità di siffatta cooperazione internazionale sono tradizionalmente ascritte all'ambito dell'attività amministrativa degli Stati: così avviene per la disciplina delle operazioni sotto copertura[202] e delle squadre investigative speciali[203]. Con ciò si sortisce un duplice effetto virtuoso. Anzitutto si riconduce al piano legislativo l'individuazione della disciplina che si riferisce a tali forme di cooperazione pur amministrativa, in virtù dell'esigenza di dare pienezza al principio di stretta legalità penale, comune alle tradizioni costituzionali degli Stati membri e per questo principio generale dell'ordinamento dell'Unione. Inoltre si áncora più solidamente al quadro delle garanzie giurisdizionali l'impiego di strumenti che vengono utilizzati nell'attività svolta dalle autorità di polizia europee e nazionali, in questo modo consentendo una penetrazione dei principi di tutela dei diritti dell'uomo accolti in sede di cooperazione giudiziaria penale anche nel settore della cooperazione di polizia.

Un secondo progresso nella direzione descritta è costituito dall'adozione delle menzionate[204] direttive di armonizzazione delle garanzie procedurali, le quali estendono il proprio ambito di applicazione anche alla fase pre-processuale e, quindi, introducono tutele del singolo implicato nell'attività di polizia che sono tradizionalmente tipiche della fase giurisdizionale.

A fronte di tale primo tentativo di bilanciamento permangono non pochi dati che suscitano perplessità e giustificano preoccupazioni circa un possibile abbassamento delle garanzie individuali previste nella fase relativa all'attività di investigazione, di intelligence, di polizia anche nei suoi collegamenti con l'attività giurisdizionale. Sono preoccupazioni che emergono dall'esame della disciplina giuridica stabilita nella dimensione securitaria dell'Unione in relazione a due diversi profili: in ordine, cioè, sia allo stretto coordinamento richiesto a tutte le autorità nazionali ed europee implicate nell'attività di contrasto delle condotte di reato, sia all'incisività che hanno assunto alcuni degli strumenti utilizzati per il conseguimento dei compiti ad esse conferiti.

---

detention", e così via: si tratta, evidentemente, di situazioni tutte proprie anche di una condizione precedente all'apertura del dibattimento penale in senso stretto.

202 Così accade ai sensi dell'art. 14 della Convenzione (di Bruxelles) adottata il 29 maggio 2000 dagli Stati membri dell'Unione europea in materia di cooperazione giudiziaria penale. Si tratta di una scelta che è stata poi "esportata" all'ambito del Consiglio d'Europa: v. l'art. 14 del II Protocollo addizionale alla Convenzione europea sulla mutua assistenza penale, firmata a Strasburgo l'8 novembre 2011.

203 Art. 13 della Convenzione di Bruxelles, cit.; disciplina in modo analogo l'art. 20 del II Protocollo addizionale, cit. La scelta, per il vero, era stata anticipata dall'art. 19 della Convenzione di Palermo sulla criminalità organizzata transnazionale (del 16 dicembre 2000).

204 *Supra,* nel testo all'altezza dell'esponente di nota 200 e nota stessa.

10. La stretta collaborazione fra le autorità incaricate dell'applicazione della legge negli Stati e nell'Unione

Anzitutto quanto al primo profilo occorre affrontare una questione terminologica, necessaria alla comprensione del principio di reciproco riconoscimento che ha preso piede anche nell'ambito della cooperazione di polizia, in particolare tramite la tecnica della circolazione internazionale di dati e informazioni utili all'attività delle autorità incaricate dell'applicazione della legge.

Nonostante i Trattati di Unione continuino – come per il passato – a intitolare alla sola «cooperazione di polizia» le norme raccolte entro la Parte III, Titolo V, Capo V TFUE, l'attività delle autorità di polizia è sempre stata intrecciata a quella svolta (in sede nazionale ed europea) da organi e organismi incaricati dell'esercizio di altre competenze. Di ciò dà conto la disposizione contenuta nell'art. 87, n. 1, del Trattato sul funzionamento dell'Unione, che alla cooperazione di polizia «associa tutte le autorità competenti (…) dell'applicazione della legge».

La locuzione manifesta due preliminari scelte politiche attuate dagli Stati membri all'atto della redazione delle disposizioni convenzionali. E' reso evidente dall'andamento della disposizione convenzionale che l'elenco delle autorità coinvolte nel circuito cooperativo è del tutto esemplificativo e non esaustivo, indirizzandosi essa non esclusivamente a quelle ivi esplicitate. Si è voluto, dunque, implicare nella cooperazione in questione anche le autorità nazionali competenti per l'applicazione della legge diversa da quella penale: tanto è vero che tale ultima qualificazione non è espressa dalla disposizione convenzionale, dovendosi concludere che la cooperazione che sulla base di essa si intreccia possa riguardare anche condotte che si situano in un ambito differente, per esempio in quello amministrativo[205].

Sono, così e anzitutto, considerate destinatarie dell'obbligo di cooperazione le autorità che operano nell'amministrazione doganale degli Stati membri. Questa forma di cooperazione è stata considerata cruciale fin dal Trattato CEE, utile tra l'altro a intercettare le condotte di criminalità transnazionale nel settore in questione. Essa era tuttavia priva di una base giuridica propria, e dunque fu inizialmente frutto di misure frammentarie fondate sulla competenza comunitaria in materia di politica commerciale comune (art. 113 TCEE) o relative al «buon funzionamento del mercato interno» (art. 100A TCEE): basi giuridiche utilizzate in collegamento con la norma che consentiva (allora, come ora[206)] l'adozione di misure normative in materie non attribuite alla competenza dell'Organizzazione ma necessarie al conseguimento dei suoi fini.

Con gli sviluppi determinati (ad opera del Trattato di Maastricht) dall'istituzione dell'Unione europea e con l'ampliamento delle competenze trasferite dagli Stati all'Organizzazione, nonché con la "comunitarizzazione" (ad opera del Trattato di Amsterdam) degli Accordi di Schengen, nel Trattato istitutivo della Comunità europea fu introdotta una disposizione ad *hoc* – l'art. 116, rinumerato art. 135 TCE – nella quale si intendeva riassumere l'ambito della cooperazione doganale fra Stati membri e tra questi e la Commissione europea, con esclusione delle misure che «riguardano l'applicazione del diritto penale nazionale o l'amministrazione della giustizia negli Stati membri»[207]. Peraltro tale competenza in materia doganale trovava un avallo nell'operare degli strumenti predisposti dagli Accordi di Schengen che, istituendo un controllo alle frontiere esterne dell'Unione, incidono anche sulle attività doganali relative al movimento delle merci. Soccorrevano ancora strumenti di natura convenzionale, quali la cd. «Convenzione di Napoli del 1967»[208], rivista il 18 dicembre 1997[209]. Essa è corredata da un "sistema di informazione doganale" (SID), istituito dalla Convenzione sull'uso dell'informatica nel settore doganale[210,] completata dal Protocollo del 29 novembre 1996 concernente l'interpretazione, in via

---

205 Sul punto v. N. PARISI, *Commento art. 87 TFUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea,* Milano, 2014², p. 931 ss.

206 La "clausola di flessibilità" era prevista nell'art. 235 TCEE, poi art. 308 TCE, ora art. 352 TFUE.

207 Corsivi aggiunti.

208 Convenzione degli Stati membri della Comunità economica europea per la mutua assistenza tra amministrazioni doganali, Roma, 7 settembre 1967 (*GURI*, 11 ottobre 1971, n. 256).

209 Convenzione stabilita in base all'articolo K.3 del Trattato sull'Unione europea, *relativa alla mutua assistenza e alla cooperazione tra amministrazioni doganali*, cd. «Convenzione di Napoli II», Bruxelles, 18 dicembre 1997 (*GUCE* C 24, 23 gennaio 1998, p. 1).

210 Firmata a Bruxelles, 26 luglio 1995 (*GUCE* C 316, 27 novembre 1995, p. 34 ss.).

pregiudiziale, da parte della Corte di giustizia delle Comunità europee[211], nonché dal regolamento (CE) n. 766/2009 relativo alla mutua assistenza tra le autorità amministrative degli Stati membri e alla collaborazione tra queste e la Commissione per assicurare la corretta applicazione delle normative doganale e agricola[212], rafforzato dalla decisione quadro 2009/917/GAI relativa agli aspetti che per tale collaborazione implicano lo spazio di libertà, sicurezza e giustizia.

Allo stato attuale la situazione è dunque assai chiara: da una parte - nell'attuale art. 35 TFUE, che sostituisce l'art. 135 TCE - è caduta l'esclusione (di cui si è appena detto) della materia *lato sensu* penale, cosicché la cooperazione doganale fondata su questa disposizione non incontra più un limite *ratione materiae*; dall'altra si prevede espressamente (come peraltro nel precedente art. 30 TUE) che la cooperazione di polizia debba associare anche le autorità doganali.

Dall'art. 87, n. 1, TFUE si ricava un altro dato importante per l'individuazione delle autorità nazionali coinvolte nel circuito della cooperazione di polizia: l'ampia formula terminologica utilizzata sembra, infatti, includere fra i «servizi incaricati dell'applicazione della legge specializzati nel settore della prevenzione (…) dei reati e delle relative indagini» anche le autorità di *intelligence*: il diverso obiettivo che esse hanno rispetto alle autorità di polizia non è di ostacolo a siffatta interpretazione[213].

Infine, occorre anche considerare che fin dalla prima introduzione della dimensione securitaria nell'Unione la cooperazione di polizia è stata considerata indissolubilmente legata alla cooperazione con le autorità giudiziarie penali degli Stati membri, prendendo atto che la sicurezza è conseguibile tramite un'azione congiunta espressa sul piano della prevenzione e su quello della repressione.

Significativamente la Convenzione di applicazione dell'Accordo di Schengen affianca alla cooperazione di polizia la cooperazione giudiziaria penale. Questi due differenti ambiti di concertazione hanno sempre seguito lo stesso percorso istituzionale: estranei alla cooperazione intessuta con i tre originari Trattati comunitari, sono stati introdotti dal Trattato di Maastricht fra le responsabilità dell'Unione grazie alla costruzione di un terzo "pilastro" di essa, idoneo ad accogliere – in virtù del metodo intergovernativo ivi utilizzato – i settori riguardanti la circolazione degli stranieri, la cooperazione giudiziaria civile e penale, la cooperazione di polizia e doganale. Vi sono rimasti anche quando si è proceduto, con il Trattato di Amsterdam, ad enucleare esplicitamente la finalità di dotare l'Unione di uno spazio di libertà, sicurezza e giustizia e a "comunitarizzare" in una certa misura i settori riguardanti ingresso, soggiorno e spostamento interstatuale dello straniero nel territorio degli Stati membri, le correlate (ma anche non) questioni di conflitto di leggi e di giurisdizione e la cooperazione doganale. Oggi, ad avvenuta unificazione di tutte le materie relative allo spazio di libertà, sicurezza e giustizia entro un unico Titolo della Parte III del Trattato sul funzionamento dell'Unione, cooperazione giudiziaria e di polizia condividono il medesimo assetto, sottoposte come sono in via di principio al "metodo comunitario" e contraddistinte da analoghe specificità derogatorie rispetto ad esso. È peraltro scontato che, in un contesto di Stato di diritto, le autorità di polizia debbano continuamente riferirsi alle autorità giudiziarie penali: di qui l'opportunità della scelta istituzionale descritta, alla quale tuttavia non sembra aver corrisposto una parallela capacità di farsi penetrare da principi e disposizioni a tutela dei diritti della persona coinvolta nei procedimenti[214].

A questi sviluppi per così dire orizzontali – capaci cioè di coinvolgere nella cooperazione con le autorità di polizia altri organi nazionali preposti a differenti compiti, ma pur sempre in funzione di prevenzione e di individuazione dei reati, nonché di investigazione penale – se ne aggiunge un altro, frutto della prassi più recente. Lo sviluppo della cooperazione avviata entro il terzo "pilastro"

---

211 Concluso in base all'art. K.3 TUE (*GUCE* C 151, 20 maggio 1997, p. 16 ss.).

212 Regolamento (CE) n. 766/2008 del PE e del Consiglio, del 9 luglio 2008, *recante modifica del regolamento (CE) n. 515/97 del Consiglio relativo alla mutua assistenza tra le autorità amministrative degli Stati membri e alla collaborazione tra queste e la Commissione per assicurare la corretta applicazione delle normative doganale e agricola* (*GUUE* L 218, 13 agosto 2008, p. 48 ss.), a propria volta attualmente sotto revisione: COM(2013) 796 final.

213 In questo senso J.P. PIERINI, G. PASQUA, *Police cooperation in the European Union: an overview*, cit., p. 408; J.A.E. VERVAELE, *Terrorismo* versus *scambio di informazioni tra* intelligence *e autorità investigative giudiziarie: diritto penale* sub rosa?, in U. DRAETTA, N. PARISI, D. RINOLDI (a cura di), *Lo spazio di libertà, sicurezza e giustizia nell'Unione europea*, Napoli, 2007, p. 321 ss.; *contra* M. WINKLER, *Attività europea di* intelligence, *cooperazione di polizia e diritti umani*, *ibid.,* p. 293 ss.

214 V. *infra*, parr. 13 e 15.

dell'Unione aveva già dato vita a organi con compiti latamente riconducibili a quelli di polizia: incaricati cioè del mantenimento dell'ordine, della sicurezza pubblica e di indagine al fine del contrasto di attività illegali, quali esemplificativamente Europol, Olaf e Frontex; ovvero a organi con compiti funzionali amministrazione della giustizia penale, quale è Eurojust e quale sarà, in adempimento del Trattato di Lisbona, la futura (ancora eventuale) Procura europea. Si tratta di organi che sono chiamati a cooperare reciprocamente entro l'Unione, ma anche a collegarsi con le autorità nazionali di cui si è detto e che dunque partecipano alla disciplina stabilita dall'art. 87 TFUE.

Le «misure»[215] che Parlamento europeo e Consiglio adottano sulla base della procedura legislativa ordinaria fanno proprio l'obbligo di cooperazione fra tutte le autorità e gli organismi coinvolti nella prevenzione o nell'individuazione dei reati e delle relative indagini, siano essi nazionali o europei.

Limitando l'esemplificazione a pochi simbolici casi, si consideri anzitutto la disciplina stabilita dall'ormai estinta Comunità europea per assicurare la mutua assistenza tra le autorità amministrative degli Stati membri e tra queste e la Commissione al fine di assicurare l'applicazione corretta della normativa agricola e doganale d'origine comunitaria: già nei *considerandа* del regolamento[216] si afferma la necessità di «assicurare una maggior complementarità con le azioni effettuate al livello della cooperazione doganale intergovernativa e della cooperazione con gli altri organi e agenzie dell'Unione europea (…) nell'attuazione» di strategie stabilite dall'Unione e dalla Comunità europea in relazione ad altri organismi di esse, quali Europol e Olaf.

Nello stesso senso si dispone in ordine allo scambio di dati personali tra gli Stati membri ed Europol[217]; o, ancora, in relazione allo scambio di informazioni e dati fra Eurojust e Stati membri: la disciplina normativa europea[218] autorizza i ventotto membri nazionali che compongono il collegio ad accedere (nel rispetto del mandato e, dunque, delle funzioni che tale organo europeo deve assolvere) a taluni dati[219] che riguardano indagati e autori di reati conferiti dagli stessi Stati membri entro un sistema automatizzato (cd. TESTA) condiviso da Eurojust e a disposizione anche delle autorità di Stati terzi sulla base di accordi bilaterali con Eurojust stesso[220].

Al proposito si può concordare con chi rileva che lo stretto coordinamento sia orizzontale che verticale fra le autorità incaricate «dell'applicazione della legge specializzat[e] (…) nel settore della prevenzione e dell'individuazione dei reati e delle relative indagini»[221] manifesta la vocazione alla *multilevel governance* anche nel settore della cooperazione di polizia[222], che si situa al termine (auspicabilmente non compiuto) di un processo lungo e articolato. Sul piano delle forme giuridiche si tratta di un processo che ha inizialmente dato avvio a un primo sviluppo di forme di internazionalizzazione dell'investigazione penale, tramite la stipulazione di intese bilaterali[223], per poi determinare anzitutto la condivisione di esse su di un piano multilaterale[224], il passaggio in breve tempo a forme istituzionali[225] e, infine, l'annuncio di forme integrate di attività di polizia espresse da strutture

---

215 Art. 87, n. 2, TFUE. Ancora a «misure» il Consiglio (che delibera all'unanimità, previa consultazione del Parlamento europeo) ricorre quando si tratti di stabilire in materia di cooperazione operativa tra le autorità coinvolte nella cooperazione di polizia (art. 87, n. 3, co. 1, TFUE).

216 Regolamento (CE) n. 766/2008, cit., 10° *considerando*.

217 Decisione quadro 2008/977/GAI (*GUUE* L 350, 30 dicembre 2008, p. 60).

218 Decisioni quadro 2002/187/GAI (*GUCE* L 63, 6 marzo 2002, p. 1) e 2009/426/GAI (*GUUE* L 138, 4 giugno 2009, p. 14 ss.).

219 Le informazioni oggetto di condivisione e scambio sono: i dati anagrafici, i recapiti, i dati di immatricolazione dei veicoli, i profili DNA, le fotografie, le impronte digitali i dati conferiti dai gestori di telecomunicazioni relativi agli abbonati, al traffico e all'ubicazione.

220 La circolazione dei dati con Paesi terzi è possibile con il consenso dello Stato membro che ha conferito i dati stessi alla rete TESTA.

221 Per utilizzare l'ampia e onnicomprensiva locuzione impiegata dall'art. 87, n. 1, TFUE.

222 S. BRONITT, *Conclusion: Shifting paradigms: jurisdiction and criminal justice cooperation in the shadow of law*, in S. HUFNAGEL, C. HARFIELD, S. BRONITT (eds.), *Cross-border Law Enforcement*, London, 2012, p. 275.

223 Per un richiamo puntuale ad esse v. J.P. PIERINI, G. PASQUA, *Police cooperation*, cit., p. 403 ss.

224 Op. loc. ult. cit. A proposito di Interpol v. P. MILAZZO, *Quadro costituzionale italiano e cooperazione europea di polizia. Elementi istituzionali e ricostruttivi per un bilanciamento complesso,* Napoli, 2012, p. 348 ss.

225 Nel processo d'integrazione europea questo passaggio è significativamente espresso dall'istituzione di Olaf. Sull'istituzionalizzazione delle forme di investigazione e coordinamento delle operazioni di investigazione v. R. KENDALL, *Goals, Functions and Limits of Interpol*, in C. ELIAERTS, E. ENHUS, R. SENDEN (eds.), *Politie in beweging*, Arnhem, 1990.

istituzionali non soltanto di coordinamento della cooperazione internazionale bensì anche di integrazione delle autorità nazionali entro un ente internazionale[226].

Sul piano degli obiettivi e dei contenuti si è assistito a un passaggio dal primo sviluppo di forme di internazionalizzazione dell'investigazione penale con l'obiettivo di risolvere singole situazioni problematiche anche interne a un solo Stato ma capaci di estendere effetti pregiudizievoli ad altri Paesi[227], a forme indirizzate a contrastare ad ampio raggio le condotte transnazionali di criminalità[228]. In tempi recenti la cooperazione di polizia si è estesa anche all'ambito tradizionalmente occupato dalla cooperazione militare: sono frequenti i casi in cui le forze civili di polizia di un gruppo di Stati sono utilizzate per operazioni internazionali di gestione di gravi crisi entro Paesi terzi rispetto ad essi, a supporto delle attività di forze di polizia locali del territorio da pacificare[229]. Analogamente è previsto anche nell'ordinamento dell'Unione, dove con il Trattato di Lisbona[230] si è dato maggior spessore alla dimensione civile della politica di sicurezza e difesa comune (PSDC)[231].

11. *(Segue)* L'impiego di nuove tecnologie: le banche-dati…

Per quanto attiene al secondo profilo, si consideri che ai servizi nazionali e agli organismi europei che collaborano entro il circuito della cooperazione di polizia sono stati affiancati sistemi istituzionali di raccolta, archiviazione, trattamento, analisi e scambio di dati messi a disposizione dalle amministrazioni pubbliche nazionali ed europea. Emerge complessivamente, nel contesto dell'Unione europea, una struttura assai articolata principalmente fondata sul criterio del decentramento: infatti - ad eccezione di SIS (e SIS II)[232], VIS[233], Eurodac[234], SID[235], Europol[236], Eurojust[237] - ogni altra banca-dati funzionante

---

226 Nel contesto europeo si v. al proposito la costituzione di Europol.

227 In via esemplificativa si ricorda che la Conferenza di Roma del 1898 aveva inteso affrontare e risolvere il problema degli attentati anarchici in territorio italiano: v. J.P. PIERINI, G. PASQUA, *Police cooperation in the European Union*, cit.

228 Attuale art. 87 TFUE.

229 In argomento si rinvia a J. DOBBINS ET AL., *The Beginner's Guide to N-Building*, Santa Monica (Rand Corporation), 2007; W.J. DURCH ET AL., *The Brahimi Report and the Future of UN Peace Operations*, New York-Washington (The Henry L. Stimson Center), 2003.

230 Ai sensi degli artt. 42-43 TUE.

231 Peraltro tale dimensione era già presente in precedenza, ai sensi degli obiettivi individuati dal Consiglio europeo di Santa Maria di Feira (19-20 giugno 2000, Allegato I, appendici 3 e 4 delle Conclusioni), confermati nel Consiglio europeo di Göteborg (15-16 giugno 2001), nonché dal Consiglio dell'Unione, con il *Nuovo obiettivo primario civile 2010*, 9 dicembre 2007, doc. 14823/07; in argomento v. G. GIUDICELLI-DELAGE, *Fonctions de police judiciaire des forces arme à l'étranger*, in *http://www.defensesociale.org/warandpiece/GENEVIEVE%20GIUDICELLI-DELAGE.pdf*.

232 Il Sistema d'informazione Schengen di seconda generazione è istituito dal regolamento (CE) n. 1987/2006 e dalla decisione 2007/533/GAI; si fonda sui principi contenuti nella direttiva 95/46/CE. Esso contiene segnalazioni su persone, oggetti, un archivio per la conservazione delle impronte digitali, fotografie, copie dei mandati di arresto europei; costituisce una misura compensativa all'abolizione delle frontiere interne allo "spazio Schengen"; è corredato dagli uffici SIRENE (costituiti in ciascuno Stato membro). Vi hanno accesso tutti gli Stati membri che partecipano anche ad Europol e Eurojust.

233 Il Sistema d'informazione visti (VIS) (v. *supra,* par. 3.1) è un sistema informatizzato costituito da una sezione nazionale (presso ciascuno Stato partecipante, anche non membro dell'Unione) e da un'unità di supporto tecnico: a fini di prevenzione di fatti di terrorismo e di altri gravi forme di criminalità, ha come compito il confronto biometrico delle impronte digitali utile alla verifica dell'identità dei titolari di visto alle frontiere esterne dell'area coinvolta nella cooperazione: accedono a tale banca-dati le autorità nazionali competenti in materia di visti e di immigrazione, le autorità nazionali di frontiera e di polizia, nonché Europol.

234 Eurodac è istituito dal regolamento (CE) n. 343/2003, oggi rivisto dal regolamento (UE) n. 603/2013: è un sistema informatizzato di identificazione delle impronte digitali a fini di controllo dell'immigrazione irregolare a fini di prevenzione, individuazione e investigazione di condotte di terrorismo e di altri gravi reati.

235 Il Sistema di informazione doganale (SID) - istituito dalla Convenzione di "Napoli II", cit. – è utilizzato per facilitare la prevenzione, la ricerca e il perseguimento di gravi infrazioni alle norme nazionali in materia doganale. E' un sistema informatizzato gestito dalla Commissione europea, al quale accedono Europol, Eurojust e le autorità nazionali competenti in materia doganale. I dati trattati consistono in: nomi (e *alias*), cittadinanza, data e luogo di nascita, sesso, segni particolari, documenti di identità, indirizzo, eventuali segnalazioni relative ad atti di violenza, dati di immatricolazione del mezzo di trasporto, motivo dell'inclusione dei dati; essi riguardano le merci, i mezzi di trasporto, le imprese, le persone, i provvedimenti di blocco, sequestro e confisca di beni e denaro. I dati SID sono conservati in un archivio (*Fichier d'Identification de Dossiers d'Enquêtes douanières - FIDE*) che consente a ciascuna autorità nazionale che avvii un'indagine in materia doganale di individuare le altre autorità nazionali che abbiano indagato su persone, imprese, attività. Con regolamento (CE) 515/97, cit., sono state predisposte AFIS (Antifraud Information System) e CIS (Custom Information System), messi a disposizione di Olaf per la raccolta e archiviazione di dati doganali e agricoli, in funzione antifrode.

nell'Unione a presidio della sicurezza[238] è costituita a livello nazionale: le norme dell'Unione intervengono per rendere possibile lo scambio di dati e informazioni fra tutte esse reciprocamente e con le autorità nazionali ed europee interessate a quei dati, prevedendosi anche il trasferimento di questi anche verso Stati terzi.

12. … e la disciplina pertinente. In particolare: il principio di disponibilità delle informazioni

Ora, l'attività normativa alla quale sono chiamate le istituzioni dell'Unione consiste, per quanto qui interessa, nel determinare le modalità dell'attività di raccolta, archiviazione, trattamento, analisi e scambio di informazioni pertinenti secondo linee direttrici stabilite nel Trattato sul funzionamento dell'Unione, che innovano rispetto al passato: l'art. 30, n. 1, lett. b, TUE-Amsterdam, infatti, già prevedeva una stretta cooperazione in materia fra le autorità competenti ad attuare la cooperazione nel settore della polizia; ma l'art. 87 TFUE aggiunge la previsione circa la messa a disposizione dei dati, tramite lo scambio di essi fra tali autorità.

La modifica cui si è fatto cenno è già di per sé importante. Tuttavia occorre considerare che essa si inserisce in un contesto divenuto assai originale rispetto al tradizionale impianto che contraddistingue le relazioni internazionali nel settore della cooperazione di polizia. Non sono, dunque, tanto gli strumenti e le modalità impiegati nel settore della cooperazione (internazionale) di polizia a diversificare l'esperienza che va svolgendosi nell'ambito del processo di integrazione europea, poiché, come già rilevato, si tratta di strumenti e modalità che si ritrovano anche in altri ambiti istituzionali di cooperazione[239]. Ciò che muta è, da una parte, il fatto che tale cooperazione si inserisce in un contesto istituzionale e, da un'altra parte, che tale contesto è assai sofisticato e manifesta modalità particolari dal punto di vista strutturale, funzionale e organizzativo, anche in relazione all'assetto dei rapporti fra organi nazionali, nonché fra essi e organi e organismi europei.

Non è poi indifferente il fatto che con il Trattato di Lisbona sia stata predisposta una base giuridica di rango costituzionale e di portata generale - prima inesistente - che fonda la competenza delle istituzioni dell'Unione a intervenire nell'intera materia del trattamento automatizzato dei dati personali (con la sola eccezione del settore relativo alla politica estera di sicurezza e difesa comuni); e che tale base giuridica sia strettamente collegata alle norme - anch'esse di rango primario - stabilite entro la Carta dei diritti fondamentali[240].

Vi è, anzitutto, la convinzione secondo la quale «il semplice fatto che l'informazione attraversi i confini non dovrebbe più assumere rilevanza» nei rapporti tra le autorità degli Stati membri[241].

Conseguentemente, attenzione preminente deve essere posta sul principio di disponibilità delle informazioni e sugli strumenti messi in campo dall'Unione in tema di raccolta, archiviazione e

---

236 Europol (decisione 2009/371/GAI) gestisce una banca-dati contenente principalmente informazioni sui reati (di competenza Europol) a dimensione transnazionale e sulle persone in essi coinvolte fornite delle amministrazioni nazionali: ciascuno Stato designa (oltre all'unità nazionale di Europol – UNE) le altre autorità che possono accedere a questa piattaforma informativa.

237 Eurojust (istituito con decisione 2002/187/GAI, del 28 febbraio 2002, più volte modificato, infine con decisione 2009/426/GAI) detiene una banca-dati al fine di sostenere e potenziare il coordinamento e la cooperazione tra le autorità nazionali responsabili delle indagini e dell'azione penale, migliorando la cooperazione giudiziaria tra gli Stati membri, in particolare nella lotta contro le forme gravi di criminalità transnazionale, anche assistendo le autorità nazionali per facilitare le indagini e l'azione penale.

238 Una sintesi delle banche-dati funzionanti entro lo SLSG è nella Comunicazione della Commissione in materia di *Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia*, COM(2010) 385 def., 20 luglio 2010: le utili tavole contenute in appendice (p. 47 ss.) indicano, a fianco del singolo strumento informatizzato, il contesto in cui è stato creato, la finalità, la struttura, i dati interessati al trattamento, le modalità di accesso, di protezione e di conservazione di essi, lo stato di attuazione della norma che lo istituisce, le prospettive di revisione. Un'integrazione di esse si rinviene nella più sintetica Comunicazione della Commissione su *Rafforzare la cooperazione in materia di applicazione della legge nell'UE: il modello europeo di scambio di informazioni (EIXM)*, COM(2012) 735 def., 7 dicembre 2012, p. 4 ss. Su di esse v. da ultimo, P. MILAZZO, *Quadro costituzionale italiano,* cit., cap. V, con particolare attenzione a Europol.

239 Concordano sulla non originalità di molte delle forme che nell'Unione europea va assumendo la cooperazione di polizia J.P. PIERINI, G. PASQUA, *Police cooperation,* cit., p. 406.

240 Si tratta dell'art. 16 TFUE (il quale contempla l'eccezione di cui si è detto nel testo a proposito dei PESC e PESD: v. art. 39 TUE) e degli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

241 Parte 2, punto 2.1, 2° cpv. Programma dell'Aja, del 4-5 novembre 2004 (*GUUE* C 53, 3 marzo 2005, p. 1 ss.)

circolazione di dati a fini di prevenzione, indagine, accertamento e perseguimento dei reati, nonché di esecuzione di sanzioni penali. Si tratta di un principio peraltro non completamente nuovo nel contesto europeo in quanto accolto in altri strumenti convenzionali[242].

Vi è, poi, da valutare la dimensione del fenomeno: l'accoglimento così pervasivo dell'utilizzo di strumenti informatici di raccolta, archiviazione, trattamento e circolazione delle informazioni costituisce la differenza qualificante. Ai sensi del Trattato di Lisbona e del Programma dell'Aja (coevo al Trattato che adotta una Costituzione per l'Europa, la cui disciplina in materia di cooperazione di polizia è accolta integralmente nella revisione di Lisbona) muta infatti la prospettiva di ricorso a tale principio, che da criterio di non diffuso impiego diventa la regola nelle relazioni fra le autorità incaricate dell'applicazione della legge ai fini di contrasto delle condotte di reato. Inoltre, nello spazio di libertà, sicurezza e giustizia tale regola comporta l'accesso reciproco e l'interoperabilità delle banche-dati nazionali[243], nonché l'accesso diretto (*on-line*) alle banche-dati dell'Unione da parte di autorità nazionali ed europee.

Si tratta di una delle tante occasioni nelle quali si concreta l'applicazione del principio di riconoscimento reciproco che, ai sensi delle Conclusioni del Consiglio europeo di Tampere del 16-17 ottobre 1999, «dovrebbe diventare il fondamento della cooperazione giudiziaria nell'Unione tanto in materia civile quanto in materia penale»[244] e che nell'ordinamento dell'Unione ha assunto ormai portata di principio di portata costituzionale[245;] esso ha visto la propria ultima concretizzazione di diritto positivo nel regolamento (UE) n. 883/2013 che modifica i poteri di indagine di Olaf: ivi si stabiliscono regole che rispondono al criterio secondo il quale «Per il successo della cooperazione tra l'Ufficio, le istituzioni, gli organi e gli organismi dell'Unione pertinenti, le autorità competenti degli Stati membri, le autorità competenti dei Paesi terzi e le organizzazioni internazionali, dovrebbe essere organizzato un reciproco scambio di informazioni»[246].

(A) Prima dell'entrata in vigore del Trattato di Lisbona, il ricorso al principio di disponibilità delle informazioni era già stato avanzato con una logica di tipo anzitutto settoriale e spingendosi assai più in là rispetto agli auspici espressi a Tampere.

Si sono stabilite norme in materia di scambio di informazioni: tra le cd. Unità di Informazione Finanziaria (UFI) costituite in ciascuno Stato membro ai fini di contrasto del riciclaggio e di finanziamento del terrorismo, determinando l'obbligo di condivisione dei dati finanziari anche utilizzabili nelle indagini e nelle azioni penali, a meno che lo Stato di conferimento di essi non ne vieti tali ultimi usi[247]; fra gli Uffici per il recupero dei beni (ARO), anch'essi costituiti in ciascuno Stato membro con lo scopo di reperire e identificare proventi di reato sulla base di informazioni relative alle persone (fisiche e giuridiche implicate) e ai beni (immobili, conti correnti, veicoli); fra le autorità giudiziarie nazionali, le quali sono tenute a prendere in conto precedenti decisioni giudiziarie di condanna nell'occasione di un nuovo procedimento penale[248], determinando i contenuti e le modalità dei reciproci contatti[249] e istituendo la rete cd. ECRIS per lo scambio delle informazioni[250]; fra autorità

---

242 V. al riguardo la Convenzione di Strasburgo dell'8 novembre 1990 *sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato*. Nell'ambito dell'Unione europea si segnala la più volte citata Convenzione *di applicazione dell'Accordo di Schengen*, al proprio art. 30, n. 1; nonché la Convenzione *stabilita dal Consiglio conformemente all'articolo 34 del trattato sull'Unione europea, relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea*, Bruxelles, 29 maggio 2000 (*GUCE* C 197, 12 luglio 2000, p. 3). Sull'importanza degli sviluppi tecnologici a fini di raccolta delle informazioni in relazione all'attività investigativa v. fra gli altri P. GULLY-HART, *Cooperation between central authorities and police official: the changing face of international legal assistance in criminal matters*, in *RIDP,* 2005, p. 27 ss.

243 Per interoperabilità si intende «la capacità dei sistemi informatici, e dei processi operativi da questi supportati, di scambiare dati e di condividere informazioni e conoscenza»: COM(2005) 597, 24 novembre 2005.

244 Punto 33 delle suddette Conclusioni (*http://www.europarl.europa.eu/summits/tam_it.htm*).

245 Su origini, sviluppi e implicazioni del principio di reciproco riconoscimento (anche per richiami ad altra importante dottrina) v. il mio *Centralità della persona e spazio di libertà, sicurezza e giustizia: il ruolo della Procura europea,* in *Studi in onore di Giuseppe Tesauro* (di prossima pubblicazione).

246 Regolamento cit. (*GUUE* L 248, 18 settembre 2013, p. 1 ss.), punto 35 del Preambolo.

247 Decisione 2000/642/GAI (*GUCE* L 271, 24 ottobre 2000, p. 4 ss.).

248 Decisione quadro 2008/675/GAI (*GUUE* L 220, 15 agosto 2008, p. 32 ss.).

249 Decisione quadro 2009/315/GAI (*GUUE* L 93, 7 aprile 2009, p. 23 ss.).

250 Decisione 2009/316/GAI (*ibid*., p. 33 ss.).

di polizia ai fini dello scambio di informazioni su reati informatici: a partire dal 2008 venne per passi successivi costruita una "piattaforma europea in materia di criminalità informatica" (sotto la responsabilità di Europol), collegata alle "piattaforme nazionali" gestite da ogni singolo Stato[251].

Si consideri, poi, la proposta della Commissione del 12 giugno 2012 di applicare lo scambio automatico dei dati delle amministrazioni fiscali nazionali a fini di lotta all'evasione fiscale, alla frode e la cosiddetta pianificazione fiscale aggressiva[252]. La penetrazione del principio anche nell'ambito amministrativo è segnato pure dalla disciplina (per la verità assai discutibile dalla prospettiva della propria complessiva linearità applicativa) stabilita in materia di ordine europeo di protezione, che evidentemente comporta decisioni nazionali di natura non sempre penalistica né civilistica, essendo implicato un titolo giuridico destinato a circolare sulla base della qualificazione di esso data da ciascuna amministrazione nazionale[253]. Ugualmente deve dirsi per la disciplina stabilita in materia di infrazioni stradali[254].

Si sono aggiunti provvedimenti sulla conservazione dei dati da parte dei gestori di servizi telefonici e di *internet*, a fini di indagine, accertamento e perseguimento di reati gravi[255], nonché sulla protezione di essi nel quadro della cooperazione di polizia e giudiziaria in materia penale[256].

Ancora, si segnala la proposta di direttiva che si applica alla trasmissione dei dati relativi ai passeggeri nel traffico aereo entro lo spazio interno europeo a fini di prevenzione, accertamento, indagine e azione penale per reati di terrorismo e altri gravi condotte illecite[257].

Nelle relazioni internazionali il principio ha preso ugualmente piede: significativi sono al riguardo gli accordi intercorsi con gli Stati Uniti d'America in materia di trasferimento di dati del codice di prenotazione (PNR)[258] e di transazioni finanziarie dei terroristi (TFTP)[259]; in modo analogo si sta procedendo con altri Stati, quali Canada e Australia.[260]

(B) Con una finalità di portata generale – con l'intento di dare unità di indirizzi alla disponibilità delle informazioni nello spazio di libertà , sicurezza e giustizia - era stata proposta l'adozione di una decisione quadro (del 12 ottobre 2005[261]) sullo scambio di informazioni nell'ambito della cooperazione giudiziaria e di polizia, abbandonata per irriducibili contrasti opposti da alcuni Stati membri in sede di Consiglio dell'Unione: in verità il meccanismo di attuazione del principio di disponibilità è stato non a torto valutato come il «più audace ed avanzato» fino ad allora proposto[262].

Superate le difficoltà d'ordine politico sulla base di una piattaforma normativa meno coraggiosa, si poté procedere all'adozione di un provvedimento - la cosiddetta "iniziativa svedese" – in materia di

---

251 V. i lavori del Consiglio "Giustizia e affari interni" del 24 ottobre 2008 e del Consiglio "Affari generali" del 26 aprile 2010.

252 *http://ec.europa.eu/taxation/tax_cooperation/mutual_assistance/direct_tax_directive/index_en.htm*.

253 Direttiva 2011/99/UE del 13 dicembre 2011 (*GUUE* L 338, 21 dicembre 2011, p. 2 ss.) e regolamento (UE) n. 606/2013 del 12 giugno 2013 (*ibid.* L 181, 29 giugno 2013, p. 4 ss.).

254 Direttiva (UE) 2011/82 del 25 ottobre 2011 (*GUUE* L 288, 5 novembre 2011, p. 1 ss.), adottata sulla base dell'art. 87, n. 2, TFUE. Interessante il dibattito che va svolgendosi fra le istituzioni europee in relazione alla base giuridica scelta (da PE e Consiglio, concordemente) per l'adozione dell'atto, contestata dalla Commissione (che privilegia l'art. 901 TFUE, in materia di sicurezza dei trasporti). Le Conclusioni (con il quale peraltro si concorda) dell'Avvocato generale Bot (adottate il 10 settembre 2013, in causa C-43/12) mettono in rilievo lo scopo della direttiva, rappresentato dall'esigenza di rendere più efficiente il sistema di contrasto delle infrazioni stradali, tramite anche una migliore azione di repressione: punto 40)

255 Direttiva 2006/24/CE (*GUUE* L 105, 13 aprile 2006, p. 54 ss.).

256 Decisione quadro 2008/977/GAI (*GUUE* L 350, p. 60 ss.).

257 COM(2011) 32, 2 febbraio 2011; la proposta è fortemente osteggiata dal Parlamento europeo, la cui commissione "Libe" (per le libertà civili, la giustizia e gli affari interni) ne propone il rigetto radicale (*Report* del 23 aprile 2013, PE 480.855v02-00). Questa disciplina è destinata a saldarsi con le norme convenzionali, stabilite con accordi internazionali stipulati dall'Unione con Stati terzi (*infra,* nel testo). Al proposito v. A. GUTIÉRREZ ZARZA, *Nuevas tecnologías, protección de datos personales y proceso penal,* Madrid, 2012, p. 120 ss.

258 V. da ultimo l'Accordo del 14 dicembre 2011 (*GUUE* L 215, 11 agosto 2012, p. 5 ss.).

259 Accordo del 28 giugno 2010 (*GUUE* L 195, 27 luglio 2010, p. 5 ss.).

260 V. infine l'Accordo con l'Australia del 29 settembre 2011 (*GUUE* L 186, 14 luglio 2012, p. 4 ss.). Su tutta la prassi convenzionale presa così sinteticamente in considerazione v. M. SPATTI, *Il trasferimento dei dati relativi al* Passenger Name Record: *gli Accordi dell'Unione europea con Australia e Stati Uniti d'America*, in *DCI,* 2013, p. 683 ss.

261 COM(2005) 490 def.

262 Il giudizio è di P. TROISI, *La circolazione di informazioni per le investigazioni penali nello spazio giuridico europeo*, Padova, 2012, p. 25.

semplificazione dello scambio di informazioni e *intelligence* tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge[263]. Con esso si sono poste le regole per lo scambio di qualsiasi dato utile in possesso delle autorità richieste sulla base vuoi del principio dell' «accesso equivalente»[264], vuoi «su richiesta»: lo scambio di informazioni avviene tra le autorità nazionali incaricate dell'applicazione della legge, per il tramite di uno qualsiasi dei canali europei esistenti[265]; vengono coinvolte nel circuito anche Europol ed Eurojust se sono implicate condotte che ricadono nel loro ambito di competenza[266]; l'autorità richiesta deve rispondere entro termini assai stretti[267], avendo a disposizione enumerati motivi di rifiuto della cooperazione[268].

Al di fuori del contesto dell'Unione, intanto, sette Stati membri di essa (Germania, Spagna, Francia, Austria, Belgio, Paesi Bassi e Lussemburgo) si erano determinati a stipulare il Trattato di Prüm del 27 maggio 2005, relativo all'approfondimento della cooperazione transfrontaliera, in particolare allo scopo di contrastare il terrorismo, la criminalità transfrontaliera e la migrazione illegale, accogliendo il principio di disponibilità delle informazioni al fine di rendere maggiormente efficace la cooperazione fra le autorità nazionali incaricate dell'attività di prevenzione del crimine transnazionale[269]. La disciplina di esso è ora incorporata entro l'Unione con decisione 2008/615/GAI[270]: essa stabilisce le modalità di scambio transfrontaliero di profili DNA, impronte digitali, dati di immatricolazione dei veicoli, informazioni relative a persone sospette di terrorismo e a ogni evento considerato rilevante a fini di prevenzione dei reati e mantenimento della pubblica sicurezza, dati che gli Stati membri sono tenuti a conservare in una propria dedicata banca-dati. Lo scambio avviene sulla base di una duplice procedura a seconda dei dati oggetto del trasferimento: su «accesso diretto» alle singole banche nazionali ad opera del punto di contatto nazionale [271], ovvero «su richiesta»[272].

Resta da dire che la normativa adottata per le questioni che coinvolgono lo spazio di libertà, sicurezza e giustizia non avrebbe dovuto avere, ai sensi dell'assetto precedente al Trattato di Lisbona, punti di sovrapposizione con la disciplina stabilita per il mercato interno, stante la divisione in "pilastri" delle competenze allora esercitate nell'ambito dell'Unione. Viceversa, una qual certa confusione si è verificata. Infatti, a proposito del mercato interno rilevava (e rileva) la disciplina stabilita con direttiva 95/46/CE, preordinata a dettare un regime generale per la protezione dei dati personali trattati in via automatizzata per quest'ambito[273]; ad essa si affiancava (l'imperfetto è d'obbligo, vista la pronuncia di invalidità intervenuta con sentenza della Corte di giustizia[274]) la direttiva 2006/24/CE relativa alla conservazione di dati generali o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione[275], con lo scopo espresso di armonizzare le regole nazionali a garanzia del miglior funzionamento del mercato interno in questo specifico ambito, ma in definitiva preordinata – come da essa stessa contemplato[276] - al contrasto di gravi condotte di criminalità: ciò che ha determinato, appunto, una scarsa chiarezza nella ripartizione

263 Decisione quadro 2006/960/GAI (*GUUE* L 386, 29 dicembre 2006, p. 89 ss.).
264 Per il quale v. *infra,* par.13, testo all'altezza dell'esponente di nota 291.
265 *Supra*, in apertura par. 3.2.
266 Artt. 3, 5 e 6 decisione ult. cit.
267 Art. 4 (la tempistica di risposta è compresa fra le otto ore e i quattordici giorni).
268 Art. 10: il diniego può essere opposto se vi è pregiudizio per la sicurezza nazionale o di persone fisiche, per indagini od operazioni di *intelligence* già avviate nello Stato richiesto, ovvero se la richiesta sia sproporzionata o irrilevante.
269 *GURI* 13 luglio 2009, n. 160, suppl. ord. n. 108. In argomento v. ancora P. MILAZZO, *Quadro costituzionale italiano,* cit., p. 227 ss.
270 Decisione del 23 giugno 2008*, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera,* in *GUUE* L 210, 6 agosto 2008, p. 1 ss.
271 Artt. 6 e 12 decisione ult. cit.
272 Art. 13 decisione ult. cit.; l'atto è accompagnato dalla decisione 2008/616/GAI, che contiene misure necessarie all'attuazione della decisione 2008/615/GAI.
273 *GUCE* L 281, 23 novembre 1995, p. 31 ss.
274 *Infra,* parr. 15-16.
275 La direttiva introduce deroghe al regime generale stabilito per il mercato interno in materia di comunicazioni elettroniche dalla direttiva 2002/58/CE.
276 Ai sensi dell'art. 1, par. 1, della direttiva, essa «ha *l'obiettivo di armonizzare* le disposizioni degli Stati membri relative agli obblighi, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, relativi alla conservazione di determinati dati da essi generati o trattati, *allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi,* quali definiti da ciascuno Stato membro nella propria legislazione nazionale» (il corsivo è aggiunto); v. anche i *considerando* nn. 9 e 21.

delle responsabilità fra primo e terzo "pilastro", oggi peraltro eliminata dalla generale base giuridica contemplata nell'art. 16 TFUE.

E' stata infine istituita un'agenzia *per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia*[277], ai fini di un «esercizio efficace, sicuro e continuo» e di una «gestione efficiente e finanziariamente responsabile» del sistema, di una «qualità adeguatamente elevata», di «continuità e (…) servizio ininterrotto», di un «livello elevato di protezione (…) e di sicurezza dei dati»[278]. Si tratta di un organismo dell'Unione dotato di personalità giuridica[279], responsabile della gestione operativa di SIS II, VIS e Eurodac e di eventuali altri sistemi IT nello SLSG[280], così da assicurare sinergie fra tutti essi[281].

Nonostante tale tentativo di razionalizzazione, in ambito europeo si avverte l'esigenza di rendere più coerente l'approccio utilizzato nella circolazione delle informazioni, propendendo a individuare in capo a Europol un ruolo centrale, come canale privilegiato per raccogliere informazioni provenienti dalle altre autorità europee incaricate di compiti investigativi: ciò dovrebbe poter garantire, a parere della Commissione[282], un'efficacia degli strumenti informatici e dell'attività di contrasto delle condotte di criminalità maggiore rispetto a quanto consentito dall'attuale approccio, valutato come assai dispersivo. Il tentativo è quello di mettere in campo un «modello europeo di scambio di informazioni»[283], improntato anche a «maggior rigore (…) che preveda sanzioni credibili per assicurare il rispetto delle norme europee» anche nei rapporti con Stati terzi[284].

III. LE IMPLICAZIONI PER IL RISPETTO DEI DIRITTI DELLA PERSONA

13. I principi applicati entro l'ordinamento dell'Unione

La cornice entro la quale deve mantenersi la disciplina delle banche-dati utilizzate nella cooperazione entro lo spazio europeo di libertà, sicurezza e giustizia è determinata, anzitutto, dal principio di sussidiarietà[285], secondo il quale è necessario valutare preventivamente se le istituzioni dell'Unione non debbano astenersi dall'adottare una disciplina comune quando il livello di governo nazionale sia più indicato. A questo proposito la Commissione ha accertato di recente la complessiva efficienza del sistema di scambio delle informazioni funzionali allo spazio di libertà, sicurezza e giustizia e la sua sufficienza, non ravvisandosi «la necessità – a questo stadio – di introdurre a livello dell'UE nuove banche dati o nuovi strumenti per lo scambio di informazioni nel settore della lotta alla criminalità»[286].

Un secondo indefettibile principio è costituito dall'obbligo del rispetto dei diritti fondamentali della persona da parte della normativa dell'Unione, all'atto della sua applicazione entro l'Unione stessa ed entro gli Stati membri[287]. I parametri di riferimento sono costituiti dall'art. 8 della Convenzione europea di salvaguardia (con il quale concorre la pertinente Convenzione europea del 28 gennaio 1981[288]) e dagli artt. 16 TFUE, nonché 7 e 8 della Carta dei diritti fondamentali (con la quale concorrono le tradizioni costituzionali comuni agli Stati membri e i principi generali del diritto

277 Regolamento (UE) n. 1077/2011 del 25 ottobre 2011 (*GUUE* L 286, 1° novembre 2011, p. 1 ss.).
278 Art. 2, lett. a-f, regolamento ult. cit.
279 Art. 10 regolamento ult. cit.
280 Art. 1, nn. 2-3, regolamento ult. cit.
281 5° *considerando* regolamento ult. cit.
282 Siffatta valutazione della Commissione è espressa in COM(2012) 735 def., cit., p. 11.
283 *Supra,* nota 238.
284 European Commission IP/14/70, del 28 gennaio 2014.
285 Art. 5 TUE.
286 COM(2012) 735, cit., p. 2.
287 Esemplificativamente v. l'art. 28 del regolamento (UE) n. 1077/2011, cit., rinvia alla disciplina contenuta nel regolamento (CE) 45/2001, del 18 dicembre 2000 (*GUCE* L 8, 12 gennaio 2001, p. 1 ss.), in materia di protezione dei dati personali.
288 *Convention pour la protection des personnes à l'egard du traitement automatisé des données à caractère personnel,* n. 108.

germinati da queste e dalla giurisprudenza applicativa della Convenzione di salvaguardia dei diritti e delle libertà fondamentali).

I principi generalissimi espressi in queste disposizioni hanno trovato concretizzazione nella normativa di diritto positivo, che utilizza oggi l'approccio detto della *Privacy by Design:* elaborato a partire dal parere del Garante europeo della protezione dei dati personali del 2010, esso pretende che «privacy and data protection are embedded within the entire life cycle of the tecnology, from the very early design stage, right through to their ultimate deployment, use and ultimate disposal»[289]. Tutto ciò si traduce nelle norme peraltro già vigenti) secondo le quali, quanto all'attività di raccolta e trattamento delle informazioni, ogni sistema informatizzato può ottenere e trattare in modo leale soltanto le informazioni utili a conseguire la finalità per la quale esse sono raccolte, al fine di perseguire uno scopo legittimo (che, nello spazio europeo di libertà, sicurezza e giustizia, è rappresentato dall'esigenza di perseguire la sicurezza nazionale, la pubblica sicurezza e la prevenzione dei reati: cd. *test* di necessità), secondo il criterio dell'accesso "stretto" (cd. *test* di proporzionalità), consentendo l'esercizio del diritto di accesso, di opposizione e di ricorso giurisdizionale a vantaggio delle persone interessate[290]. Quanto allo scambio delle informazioni, si applica il principio dell'«accesso equivalente», secondo il quale queste possono (e devono, se del caso) essere fornite dallo Stato richiesto alle autorità richiedenti a condizione che non siano più severe di quelle applicate a livello nazionale[291]. Quando lo scambio intervenga fra autorità di polizia, doganali e di *intelligence* verso autorità giudiziarie, si applica il principio secondo il quale tale materiale non può costituire fonte di prova, facendosi obbligo alle autorità richiedenti di rivolgersi all'autorità giudiziaria dello Stato richiesto, quando ciò sia necessario in analoga situazione che ricorra per i casi domestici[292].

14. A proposito di sicurezza *versus* libertà

Le soluzioni giuridiche adottate a quest'ultimo riguardo sono reputate utili a superare o almeno a mitigare gli ostacoli che affliggono la cooperazione transfrontaliera degli organi e organismi coinvolti, che in via generale soffre delle limitazioni determinate dalla perdurante sovranità nazionale, particolarmente presidiata nell'occasione di situazioni suscettibili di coinvolgere la sicurezza interna e internazionale dello Stato. La funzionalità dei sistemi informatizzati descritti è evidente: la raccolta e l'archiviazione non manuali di dati consente una più efficiente conoscenza dei fattori di rischio per la sicurezza pubblica. Nella stessa direzione dell'efficienza milita il rapporto di stretto coordinamento fra tutte le autorità (nazionali ed europee) preposte all'attività di applicazione della legge entro gli Stati membri, entro l'Unione e anche nei rapporti con Stati terzi, come auspicato dalla disciplina europea: tramite l'utilizzo di sistemi informatici «[l]e autorità di contrasto della criminalità si scambiano informazioni [in modo maggiormente efficace ed efficiente] per (…) lo svolgimento di indagini penali, la prevenzione del crimine, l'individuazione dei reati (…) e il mantenimento dell'ordine e della sicurezza pubblica»[293].

Tuttavia il rafforzamento della dimensione securitaria dell'Unione conseguito nello spazio europeo di libertà, sicurezza e giustizia mediante l'utilizzo di tali sistemi informatici e la stretta reciproca collaborazione fra tutte le autorità coinvolte nell'applicazione della legge devono far riflettere sulla compatibilità fra siffatte modalità di cooperazione e rispetto dei diritti della persona coinvolta. Non a caso è stato affermato in giurisprudenza che «in linea di principio qualsiasi trattamento dei dati

289 Opinion of the European Data Protection Supervisor *on Promoting Trust in Information Society by Fostering Data Protection and Privacy,* 18 marzo 2010, parr. 6 e 19.

290 Tale complesso di principi è riflesso negli artt. 6-7, 12, 14 e 22 della direttiva 95/46/CE, cit., e ben inquadrato nelle Conclusioni dell'Avv. gen. Mengozzi, in causa C-291/12, *Schwarz,* punto 39. Al proposito, anche per il richiamo a norme internazionali di portata universale, si rinvia da ultimo a M. SPATTI, *Il trasferimento dei dati,* cit., p. 687 ss.

291 Decisione quadro 2006/960/GAI, cit.

292 Decisione quadro ult. cit., art. 1, n. 4.

293 COM(2012) 735, cit., p. 3.

personali effettuato da un terzo è idoneo a costituire pregiudizio a tali diritti»[294]. A maggior ragione una raccolta su larga scala di dati personali mette a rischio l'integrità e la correttezza nell'archiviazione delle informazioni. E una così diffusa, pervasiva, rapida circolazione di dati può pregiudicare il rispetto di alcuni diritti fondamentali della persona: il travaso di informazioni da una banca-dati all'altra e l'incrocio fra esse possono infatti incidere negativamente sul diritto alla riservatezza; il passaggio di informazioni dall'attività di *intelligence*, a quella di polizia e doganale, infine a quella penale rischia di contraddire i principi dell'equo processo e di contravvenire al principio del rispetto delle finalità per le quali i dati vengono raccolti e trattati.

Ciò introduce al nocciolo duro della questione, quello che riguarda il bilanciamento fra diritti fondamentali della persona implicata nel trattamento automatizzato dei dati personali[295], bilanciamento reso necessario dalla non assolutezza che essi rivestono. Si tratta di un bilanciamento reso oltremodo complesso anche a motivo del fatto che diritto alla sicurezza individuale e collettiva e diritti fondamentali implicati nel trattamento automatizzato dei dati personali sono termini non omogenei, sostanziandosi in responsabilità delle autorità pubbliche che implicano, l'uno, obblighi di risultato, l'altro, obblighi di mezzi[296].

Non serve, al proposito, confermare antichi steccati e, dunque, interrogarsi sul se la sicurezza individuale e collettiva sostanzi un diritto fondamentale dotato di propria autonomia o meno. La negazione di tale qualità, nel passato ideologicamente fondata[297], era sostenuta anche utilizzando la rubrica dell'art. 5 della Convenzione europea dei diritti dell'uomo, secondo cui ogni persona ha «diritto alla libertà e alla sicurezza». Non vi è dubbio, infatti, che nella prospettiva degli accordi internazionali stipulati a tutela di diritti individuali i due termini devono essere intesi come privi di reciproca autonomia, considerandosi la sicurezza una modalità di rafforzamento del diritto alla libertà personale: insomma, allorché si tratta dei limiti che possono essere legittimamente introdotti alla libertà personale, nella stessa norma si vuole affermare l'esigenza che questi si informino al criterio della non arbitrarietà.

Nel caso ci si situa entro una nozione di sicurezza assai limitata, quella appunto connessa all'altrettanto limitato significato di libertà ivi considerato, quello della libertà dagli arresti[298].

Questo approccio nulla ha a che vedere con la dimensione, rispettivamente, di libertà e di sicurezza che qui si utilizza e che sostanzia l'obiettivo dell'Unione europea di costruire uno spazio di libertà, sicurezza e giustizia. I due termini identificano due ambiti paritari nei quali, in modo reciprocamente correlato, pubbliche autorità nazionali ed europee concorrono a stabilire le regole della libera circolazione delle persone e del godimento da parte di esse di diritti e libertà fondamentali, ivi compreso il diritto individuale e collettivo alla sicurezza[299].

---

294 Concordano sul punto sia la Corte del Lussemburgo (la citazione nel testo è tratta dalla sentenza di questa Corte del 17 ottobre 2013, causa C-291/12, *Schwarz,* punto 25), che la Corte di Strasburgo: v. le sentenze del 4 dicembre 2008, *S. e Marper c. Regno Unito*, ricc. nn. 30562/04 e 30566/04, punto 86; e del 18 aprile 2013, *M.K. c. Francia,* ric. n. 19522/09, punto 21, secondo la quale ultima «la conservazione, in uno schedario tenuto dalle autorità nazionali, delle impronte digitali di un individuo identificato o identificabile costituisce un'ingerenza nel diritto al rispetto della vita privata». Altra significativa giurisprudenza della Corte EDU è rappresentata dalle sentenze del 26 marzo 1987, *Laender c. Svezia*, ric. n. 9248/81; del 16 febbraio 2000, *Amann c. Svizzera,* ric. n. 27798/95; e del 4 maggio 2000, *Rotaru c. Romania,* ric. n. 28341.

295 Sulle specificità della tutela dei diritti della persona nello spazio penale europeo v. D. RINOLDI, *Lo spazio di libertà, sicurezza e giustizia,* cit., p. 124 ss.; E. PISTOIA, *Diritti fondamentali e cooperazione penale tra Stati membri dell'Unione europea*, in A. CELOTTO (a cura di), *Processo costituente europeo e diritti fondamentali*, Torino, 2004, p. 329 ss.

296 Al riguardo ci si permette di rinviare a N. PARISI, *Lo statuto europeo dello straniero: il contributo della giurisprudenza internazionale e nazionale,* in B. MONTANARI (a cura di), *La costruzione dell'identità europea: sicurezza collettiva, libertà individuali e modelli di regolazione sociale,* tomo II, Torino, 2013, specific. p. 186.

297 Fra i tanti v. A. BARATTA, *Diritto alla sicurezza o sicurezza dei diritti?*, in M. PALMA, S. ANASTASIA (a cura di), *La bilancia e la misura*, Milano, 2001. Ripropone il problema in tempi a noi più vicini M. DOGLIANI, *Il volto costituzionale della sicurezza,* in G. COCCO (a cura di), *I diversi volti della sicurezza*, Milano, 2012, pp. 6 e 8-9.

298 Così per tutti M. GIALUZ, *Art. 5*, in S. BARTOLE, P. DE SENA, V. ZAGREBELSKY (a cura di), *Commentario breve alla Convenzione europea dei diritti dell'uomo,* Padova, 2012, pp. 107-109. A una simile conclusione si perviene anche sulla base della *Guide on Article 5 - Right to Liberty and Security. Article 5 of the Convention,* predisposta dal Consiglio d'Europa*,* Strasbourg, 2012, p. 7, par. II.1.

299 Sulla qualificazione di libertà e di sicurezza nello spazio europeo v. (oltre a D. RINOLDI, *Lo spazio di libertà,* cit., cap. I) K. TUORI, *Chapter 2. A European Security Constitution?,* in M. FICHERA, J. KREMER (eds.), *Law and Security in Europe: Reconsidering the Security Constitution*, Cambridge-Antwerp-Portland, 2013, p. 39 ss., specific. p. 72 ss.

Il bilanciamento fra i due ordini di diritti nello spazio europeo di giustizia penale deve avvenire alla stregua, rispettivamente dell'art. 8, n. 2, CEDU e dell'art. 52, n. 1, Carta dei diritti fondamentali dell'Unione, che utilizzano la stessa tecnica di soluzione dei possibili conflitti fra diritti confliggenti: si tratta, dunque, di valutare la base legale dell'ingerenza, nonché la sua necessità e proporzionalità nel contesto di una società democratica. Il bilanciamento è una categoria giuridica che si applica al caso concreto, e dunque non è possibile tracciare una gerarchica fra libertà e sicurezza, anche nel caso della compressione che alla prima deriva dall'esigenza di dotare le autorità pubbliche di strumenti tecnologicamente avanzati di investigazione e prevenzione dei reati.

15. La giurisprudenza internazionale europea in materia

Proprio nell'attività delle Corti europee intervenuta a valutare la regolarità, necessità, proporzionalità e legittimità delle misure limitative del diritto alla riservatezza dei propri dati – dunque nella prassi applicativa delle norme europee in materia – emergono taluni aspetti di inadeguatezza rispetto agli *standard* richiesti tanto dalla Convenzione europea dei diritti dell'uomo quanto dalle fonti che nell'Unione europea con essa concorrono nella tutela del diritto. Sia la Corte di Strasburgo, alla luce dell'art. 8 CEDU, che la Corte del Lussemburgo, alla luce degli artt. 7-8 della Carta dei diritti fondamentali dell'Unione, hanno affrontato la questione[300], con un'evidente concordanza nell'approccio e nelle soluzioni giuridiche. Diversamente, peraltro, potrebbe difficilmente essere dal momento che, ai sensi della Carta dei diritti fondamentali dell'Unione europea, quando essa contenga diritti corrispondenti a quelli garantiti dalla Convenzione di salvaguardia, «il significato e la portata degli stessi sono uguali»[301]; il *Praesidium*, infine, ne ha accertato la corrispondenza[302].

Se il principio di legalità e la legittimità dello scopo sono stati diffusamente riconosciuti come complessivamente osservati[303], le censure delle due Corti si sono ad oggi concentrate sull'impiego non corretto del margine di apprezzamento di cui, in principio, godono le autorità pubbliche (nazionali ed europee) nel ricorso a ingerenze pur in via di principio legittime.

Così, a proposito dell'assetto stabilito dal Trattato di Prüm - la cui disciplina è, come noto, oggi trasfusa nella decisione quadro 615/2008/GAI – la Corte di Strasburgo osserva che «il carattere generale ed indifferenziato con cui opera il meccanismo di conservazione delle impronte digitali, dei campioni di cellule e dei profili di DNA di individui sospettati (…) non (…) poi condannati (…) non garantisce un corretto bilanciamento dei concorrenti interessi pubblici e privati in gioco; (…) lo Stato convenuto ha oltrepassato qualsiasi margine di apprezzamento in proposito (…) [ricorrendo a un'] ingerenza sproporzionata (…) non (…) necessaria in una società democratica»[304].

---

300 La giurisprudenza della Corte EDU è richiamata in nota 290. Senza pretese di esaustività la giurisprudenza della CGUE è costituita dalle sentenze: 18 dicembre 2007, causa C-137/05, *Irlanda c. Consiglio dell'Unione europea* (sulle norme in materia di caratteristiche di sicurezza e sugli elementi biometrici di passaporti e documenti di viaggio); del 16 dicembre 2008, causa C-524/06, *Huber* (sul criterio della necessità del trattamento dei dati personali); 26 ottobre 2010, causa C-482/08, *Regno Unito di Gran Bretagna e Irlanda del Nord* (in materia di accesso al sistema di informazione visti-VIS); 20 novembre 2010, cause riunite C-92-09 e C-93/09, *Schecke Gb*R e *Eifert* (che affronta la questione del bilanciamento fra diritto alla protezione dei dati personali e interessi di portata generale, nel caso rappresentati dall'esigenza di garantire trasparenza nell'assegnazione di finanziamenti comunitari); 30 maggio 2013, causa C-342/12, *Worten* (sulla nozione di dati personali e di loro trattamento)*;* 17 ottobre 2013, causa C-291/12, *Schwarz* (in materia di legittimità della rilevazione delle impronte digitali a fini di rilascio di passaporto); sono al momento sottoposti all'attenzione della Corte di giustizia quattro rinvii pregiudiziali (in cause C- da 446 a 449/12) in materia di utilizzo dei dati biometrici raccolti per passaporti e documenti di viaggio a fini diversi da quelli previsti. Una interessante rassegna della giurisprudenza delle due Corti europee in materia di sicurezza è proposta da M. FICHERA, *Chapter 3. Security Issues as an Existential Threat to the Community,* in M. FICHERA, J. KREMER (eds.), *Law and Security in Europe,* cit., p. 85 ss.

301 Art. 52, n. 3, Carta diritti fondamentali UE.

302 *Spiegazioni relative alla Carta dei diritti fondamentali*, *sub* Art. 8.

303 Sentenze Corte EDU, *S. e Marper c. Regno Unito*, cit., rispettivamente punto 97 (anche se la Corte riscontra che le norme sono formulate «in termini piuttosto generici» e si prestano «a una interpretazione eccessivamente larga»: punto 99) e punto 100; e CGUE, *Schecke Gb*R e *Eifert,* cit., punti 35, 38 e 45. Diversamente potrebbe accadere se la CGUE accoglierà le acute considerazioni dell'Avvocato generale Cruz Villalón (del 12 dicembre 2013, cit.) relativamente al fondamento legale dell'ingerenza nella vita privata attuata con la disciplina stabilita nella direttiva (CE) 2006/24 (punti 108-132).

304 Sentenza Corte EDU nel caso *S. e Marper*, cit. punto 125.

In altra situazione la Corte di giustizia dell'Unione ha ugualmente ricostruito un non corretto uso del margine di apprezzamento nella normativa comunitaria. Si trattava nel caso - che non riguarda la cooperazione di polizia ma mette in campo principi fondamentali nel trattamento dei dati personali - di trovare il giusto bilanciamento fra il diritto dei singoli alla riservatezza e l'esigenza pubblica costituita dalla pubblicazione di informazioni dei beneficiari di fondi PAC. Quest'ultima è definita dalla Corte di giustizia misura «"necessaria in una società democratica", in quanto risponde a un'esigenza sociale imperativa (…) [promuovendo] (…) la trasparenza del processo democratico [che] costituisce un "fondamento legittimo" del trattamento dei dati (…) e rientra tra le "finalità di interesse generale riconosciute dall'Unione"»[305]. Nonostante questa valenza, la Corte ha concluso nel senso che la normativa dell'Unione non rispetta il principio di proporzionalità fra regime della pubblicità e scopo che essa si propone di conseguire, concludendo che le istituzioni avrebbero dovuto individuare «un tipo diverso di pubblicazione», meno intrusivo e più appropriato in relazione alla tutela della riservatezza delle persone beneficiarie dei pubblici finanziamenti[306].

Ugualmente per il mancato rispetto del principio di proporzionalità si è pronunciata la Corte di giustizia con la recentissima sentenza in cause riunite C-293/12 e C-594/12[307], che ha dichiarato invalida (su rinvio pregiudiziale) la disciplina europea stabilita in materia di raccolta, trattamento, trasferimento e conservazione di tutti i dati del traffico telefonico e di *internet* nei confronti di tutti gli abbonati e gli utilizzatori di servizi di comunicazione elettronica e di reti di comunicazione[308]. Ciò che la Corte di giustizia ha nel caso stigmatizzato è la sproporzione di una generalizzata (a tutti gli strumenti di comunicazione elettronica) e indiscriminata (nei confronti di tutti gli utilizzatori di esse) raccolta di meta-dati, la cui conservazione era, inoltre, resa obbligatoria per un periodo compreso (a discrezione di ciascuno degli Stati membri) fra i sei e i ventiquattro mesi[309]. Tanto che ora c'è da chiedersi se non debbano essere riviste tutte le disposizioni, anche di natura convenzionale[310], vigenti nell'ordinamento dell'Unione e affette da analoga sproporzione fra ingerenza necessaria dell'autorità pubblica e rispetto dei diritti delle persone.

In altra situazione ancora, la Corte di giustizia europea ha viceversa accertato un corretto utilizzo del margine di apprezzamento da parte delle norme comunitarie relative alla raccolta e archiviazione dei dati necessari al rilascio del passaporto biometrico[311]. L'occasione si è anche utilmente proposta per valutare il rispetto del principio secondo il quale i dati devono essere utilizzati ai soli fini stabiliti in relazione alla loro raccolta[312].

Quanto all'autorità nazionale garante della riservatezza, la censura della Corte di giustizia é intervenuta a proposito del mancato rispetto da parte di uno Stato membro delle caratteristiche di indipendenza di cui essa deve godere, ai sensi della direttiva 1995/46/CE: avendo posto anticipatamente fine al mandato del commissario incaricato della protezione dei dati personali (al quale è seguita l'adozione di una legge che riserva al Presidente della Repubblica la nomina di questi), la Corte sostiene che l'Ungheria abbia violato il principio di indipendenza delle autorità responsabili della protezione dei dati personali, principio che obbliga gli Stati membri a rispettare la durata del mandato ad esse conferito[313]. Il caso ha riguardato, come si comprende, il mercato interno e tuttavia si segnala per la propria significatività alla luce della riforma avviata nell'Unione e fondata su di una base giuridica generale quale è l'art. 16 TFUE: la sentenza è certamente una precisa indicazione circa le qualità di cui devono godere le autorità preposte alla protezione dei dati personali.

---

305 Sentenza CGUE nel caso *Schecke GbR* e *Eifert,* cit., punto 95.
306 Sent. ult. cit., punti 118 e 121.
307 Sentenza 8 aprile 2014, *Digital Rights Ireland Ltd./Kärntner Landesregierung e altri.*
308 Direttiva 2006/24/CE, cit.
309 Punti 44-64 sent. ult. cit.
310 Per le quali v. *supra*, par. 12 (A).
311 CGUE, sentenza *Schwarz*, cit., punti 53-54.
312 CGUE, sentenza *Schwarz*, cit., punto 61.
313 CGUE, sentenza 8 aprile 2014, causa C-288/12, *Commissione c. Ungheria.*

Vi sono altre questioni che, a parere di chi scrive, si segnalano come sensibili e richiederebbero l'intervento chiarificatore delle giurisdizioni internazionali europee: prima fra tutte quella che non a caso determina la necessità di modifica del regolamento (UE) 515/97, in particolare del suo art. 12 che individua le condizioni di ammissibilità del materiale raccolto a fini investigativi nello Stato richiesto e trasmesso allo Stato richiedente a fini di suo utilizzo nei procedimenti amministrativi e giudiziari. La questione merita un'attenzione maggiore di quanta ad oggi riservata[314], al fine - come riconosce la stessa Commissione europea – di «eliminare l'attuale incertezza giuridica in merito alla possibilità di utilizzare le informazioni raccolte nell'ambito della mutua assistenza come elementi di prova nei procedimenti nazionali»[315]. Ancora, ci si dovrebbe meglio interrogare sulla differente portata dei diritti (e delle relative ingerenze) espressi, rispettivamente, negli artt. 7 e 8 della Carta dei diritti fondamentali, potendosi giungere a soluzioni giuridiche che, pur riconoscendo la legittimità della restrizione determinata dalla raccolta e dal trattamento dei dati personali, si debba però concludere che essa nel caso possa non essere in relazione al rispetto di quel nocciolo duro costituito dalla tutela della vita privata[316].

IV. LA RIFORMA DEL SISTEMA EUROPEO DI TRATTAMENTO AUTOMATIZZATO DEI DATI PERSONALI

16. Primi rilievi sulla prospettata riforma in materia

La problematicità della tutela dei diritti fondamentali implicati nel trattamento dei dati personali è dunque presente alle istituzioni dell'Unione[317]: si avverte un'attenzione (conseguente a una diffusa preoccupazione) anche favorita dalle censure emerse dalla giurisprudenza delle Corti europee[318] e dalla costante attività consultiva ricoperta dal comitato "Articolo 29", il Garante europeo della protezione dei dati, istituito a partire dall'omonimo articolo della direttiva 95/46/CE[319]. Si tratta indubbiamente di un terreno privilegiato per la verifica della tenuta dei principi dello Stato di diritto entro l'Unione europea.

È stata così avviata una complessiva riforma dell'intero regime giuridico di trattamento dei dati personali in relazione alle situazioni ricadenti tanto nell'ambito civile e amministrativo, quanto nelle attività di cooperazione giudiziaria penale e di polizia. Essa si articola su due diversi atti normativi: un regolamento che dovrebbe sostituire la disciplina di portata generale stabilita con la direttiva 95/46/CE e applicarsi specificamente al mercato interno; una direttiva indirizzata a dettare norme per le questioni relative alla sicurezza interna e internazionale di Unione e Stati membri[320]. Di una tale riforma si avverte, a maggior ragione, l'urgenza oggi, a motivo della pronuncia di invalidità della disciplina

---

314 Per una critica puntuale alla prassi nazionale in materia si richiama il solo J.A.E. VERVAELE, *Terrorismo* versus *scambio di informazioni tra* intelligence *e autorità investigative giudiziarie,* cit.

315 Comunicazione sulla *Modifica il regolamento (CE) n. 515/97 del 13 marzo 1997,* COM(2013) 796 cit., punto 3.4.2.

316 Lo si è fatto nel caso *Volker*, cit., punti 52 ss.; lo si sta facendo nel corso del procedimento aperto davanti alla CGUE in cause riunite C-293/12 e C-294/12, cit.: per la questione implicata v. le Conclusioni dell'Avvocato generale Cruz Villalón, cit., punto 62 ss.

317 COM(2012)09 def., p. 13.

318 A proposito delle quali v. immediatamente dopo nel testo.

319 V., fra gli altri, *The Future of Privacy. Joint Contribution to the Consultation of the European Commission on the legal Framework for the Fundamental Rights to Protection of Personal Data*, 1 December 2009, 02356/09/EN, WP 168; Parere 10/2011 sulla proposta di direttiva del Parlamento europeo e del Consiglio sull'uso dei dati del codice di prenotazione ai fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, 5 aprile 2011, 00664/11/IT, WP 181; Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High representative of the European Union for Foreign Affairs and Security Policy on a "Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace", and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, 14 June 2013, punti 31-34. Sull'intera problematica v. F. BOEHM, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice,* Berlin-Heidelberg, 2012; e M. KAIAFA-GBANDI, *Harmonisation of Criminal Procedure on the Basis of Common Principles : the EU's Challenge for Rule-of-Law Transnational Crime Control*, in C. FIJNAUT, J. OUWERKERK (eds.), *The Future of Police and Judicial Cooperation in the European Union*, Leiden, 2010, pp. 366-369.

320 V. le Comunicazioni della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Salvaguardare la *privacy* in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo, COM(2012)9 def., e sulla Proposta di direttiva del Parlamento europeo e del Consiglio *concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati*, COM(2012)10 def., entrambe del 25 gennaio 2012.

contemplata nella direttiva 2006/24/CE, che ha riconsegnato agli Stato membri la competenza a legiferare in materia in attesa che l'Unione eserciti nuovamente la propria[321].

I caratteri salienti del complesso normativo proposto, con particolare riguardo alla tutela dei diritti della persona implicata nelle attività di cooperazione giudiziaria penale e di polizia, consistono anzitutto nel fatto che il nuovo regime complessivamente inteso si applicherà al trattamento tanto nazionale che transnazionale di dati personali: riducendo le differenze fra legislazioni nazionali, questo approccio dovrebbe poter garantire una maggior certezza del diritto entro l'intera Unione e una maggior fiducia fra amministrazioni nazionali, agevolando la cooperazione nell'attività di contrasto del crimine. La proposta di direttiva intende dettare un livello uniforme ed elevato di protezione dei dati, individuando specificità per i singoli settori della cooperazione giudiziaria penale e di polizia, stabilendo criteri armonizzati per il trattamento dei dati, distinguendo le modalità del trattamento in relazione alle diverse categorie delle persone implicate, determinando le condizioni del trasferimento dei dati verso Paesi terzi.

Trascorsi due anni dalle proposte della Commissione, la riforma si trova in uno stadio non così avanzato da poter consentire valutazioni definitive sui suoi contenuti[322]. Al momento il Consiglio ha predisposto un testo di compromesso che accoglie tutti i principi fondamentali in tema di protezione dei dati personali[323]. E' fatto proprio (sebbene con qualche aggiustamento) l'approccio – cd. "by design" – contenuto nella proposta di regolamento della Commissione, secondo il quale «the notification obligation [accepted in Directive 95/46/EC] is abolished, and replaced by procedure and mechanism which focus (…) on processing operations likely to present specific risks to the rights and freedom of data subjects»[324]; ciò dovrebbe garantire un approccio maggiormente sostanziale nella tutela dei diritti della persona. Il Consiglio sembra anche sostenere il principio "one-stop-shop", secondo il quale, quando il trattamento dei dati coinvolga non un solo Stato membro, deve essere identificata una sola autorità nazionale competente alla sorveglianza sull'intero processo[325]. Non sembra invece essere stata accolta la proposta avanzata da alcuni Stati membri[326] di riversare nella direttiva tutti gli aspetti pubblicistici riducendo l'ambito d'applicazione della disciplina regolamentare[327].

Dai lavori del Parlamento europeo – che ha discusso in aula i contenuti della proposta direttiva nel mese di marzo di quest'anno[328] – vengono i perfezionamenti più significativi, che incidono principalmente nella proposta di direttiva presentando profili di interesse specifico per la questione del rispetto dei diritti della persona. Si conferma il principio "by design" a fondamento generale del trattamento dei dati personali (artt. 4 e 19); si perfeziona il criterio secondo il quale i dati devono essere trattati distinguendo le differenti categorie di persone ai quali essi si riferiscono (articoli 5 e 6); si circostanzia meglio il criterio della necessità e proporzionalità nel trattamento (art. 5) e del limitato trattamento dei dati sensibili, con particolare attenzione ai dati genetici (articoli 8 e 8a); si perfezionano le disposizioni in tema di accesso ai dati (articoli 12-14), diritto di rettifica (art. 15), cancellazione (art. 16) e tutela giurisdizionale (art. 51); si introduce un processo di "impact assessment" (art. 25); si chiariscono i criteri e le modalità di trasferimento dei dati sia internamente all'Unione (art. 55) che verso

---

321 Supra, nota 307.

322 Il calendario dei lavori può essere consultato in *www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0010(COD).*

323 V., a proposito della cooperazione giudiziaria penale e di polizia, l'art. 5 prop. dir.

324 Council of the EU, Interinstitutional File: 2012/0011 (COD) Dataprotect 14, 31 January 2014, p. 1. Il dibattito sulla proposta (avvenuto il 7 ottobre 2012) è consultabile in *http://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CDEQFjAA&url=http%3A%2F%2Fwww.consilium.europa.eu%2Fuedocs%2Fcms_data%2Fdocs%2Fpressdata%2Fen%2Fjha%2F138925.pdf&ei=Prr8UofjA8Hx4gTHtICoAg&usg=AFQjCNG9qqzEesMACjvWfq8uI15tfR0pNg.*

325 V. Working Group on Information Exchange and Data Protection, *One-stop-shop mechanism,* 6 marzo 2014, Doc. 5882/3/14 REV 3.

326 Doc. Consiglio UE 7 dicembre 2012, n. 16497/12 ADD 2, p. 4.

327 Sinteticamente v. *Progress on the data protection reform package*, Doc. 14 February 2014 PH/ABu/mk/ D(2014)0375 C2011-1104

328 Il dibattito in aula si è tenuto il 10 marzo. La relazione della Commissione parlamentare "Libe" del 22 novembre 2013 – che ha preparato il dibattito in aula - è consultabile in *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0403+0+DOC+XML+V0//IT*. In seduta plenaria il Parlamento europeo ha adottato (il 12 marzo 2014) una risoluzione legislativa su *Processing of personal data for the purposes of crime prevention. Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data,* P7_TA-PROV(2014)0219.

Stati terzi (articoli 33-38); si introduce la disposizione secondo la quale le norme dell'Unione rappresentano uno *standard* minimo, rispetto al quale gli Stati membri possono garantire una più alta protezione (art. 2*bis*).

Il dibattito interistituzionale serrato che ha contraddistinto il processo decisionale e che non è vicino alla propria conclusione[329] sarà interrotto dalla fine della legislatura europea. Poiché il giudizio che di esso si dà è positivo, si auspica che le istituzioni, in particolare Parlamento europeo e Commissione rinnovate nella propria composizione, possano con l'autunno di quest'anno riprendere i lavori legislativi facendo tesoro di quanto a oggi acquisito grazie principalmente ai lavori parlamentari.

[329] Il calendario del dibattito interistituzionale relativo alla direttiva è consultabile in *http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0010(COD).*

IV. DIRITTO ALL'OBLIO: LA SENTENZA DELLA CORTE DI CASSAZIONE ITALIANA N. 5525/2012, TAPPA FONDAMENTALE DI UNA CONFIGURAZIONE IN *FIERI*

di Giuseppe Versaci

Sommario: 1. Introduzione. - 2. Il fatto e l'*iter* processuale. - 3. Il diritto all'oblio: il "battesimo" nella sentenza n. 3679/1998 della Corte di Cassazione. - 4. La controversa configurazione del diritto all'oblio nel caso di specie. - 5. Le conclusioni della Suprema Corte. - 6. Il "peso" della Cassazione sulle decisioni del Garante della protezione dei dati personali. - 7. Uno sguardo europeo: la qualificazione del fornitore di servizi di motore di ricerca e la configurabilità di un diritto all'oblio nella causa C-131/12. - *7.1. La sentenza n. 5525/2012 al "vaglio" delle Conclusioni dell'Avvocato generale: un confronto proficuo*. 8. - Prospettive di regolamentazione del diritto all'oblio: l'art. 17 della proposta di regolamento in materia di protezione di dati personali. - 9. Qualche motivo di riflessione.

«Per ogni agire ci vuole oblio: come per la vita di ogni essere organico ci vuole non solo luce ma anche oscurità. La serenità, la buona coscienza, la lieta azione, la fiducia nel futuro dipendono dal fatto che si sappia dimenticare al tempo giusto, quanto ricordare al tempo giusto».

NIETZSCHE, *Considerazioni inattuali.*

1. Introduzione

La sentenza della Corte di Cassazione, n. 5525/2012[330], trattando la problematica relativa al bilanciamento tra diritti nel quadro della normativa sulla *privacy,* ha sancito principi che possono costituire una tappa di particolare rilievo in un ambito dai contorni ancora non ben definiti sia in ambito nazionale che in ambito europeo. Nello specifico, la Suprema Corte ha dovuto determinare le forme di tutela del c.d. diritto all'oblio nella complessa realtà del "mare di internet".

Nel commentare la sentenza, dopo una descrizione del fatto e dell'*iter* processuale, sarà d'obbligo innanzitutto soffermarsi sulla genesi del diritto all'oblio, diritto ancora giovane e in via di modellazione.

Si risalirà, pertanto, al primo riconoscimento giurisprudenziale da parte della Suprema Corte nella sentenza n. 3679/1998. Consci delle sue origini, si esaminerà, in secondo luogo, la particolare configurazione data dalla Corte di Cassazione nella sentenza in esame: essa, infatti, trattando un caso in cui si richiedeva la peculiare tutela della riservatezza in *internet*, ha dovuto connotare il diritto all'oblio con contributi nuovi rispetto a quelli forniti in precedenti pronunce, nelle quali la tutela della riservatezza veniva in rilievo in relazione ad articoli di giornale su carta stampata.

L'esame della sentenza proseguirà riportando le conclusioni cui è giunta la Cassazione: conclusioni destinate a diventare (almeno per il momento) l'orientamento giurisprudenziale di riferimento, considerata la funzione nomofilattica propria della Suprema Corte.

Dimostrazione in tal senso è data dalle recenti decisioni del Garante della *privacy* che, rimettendosi a quanto sancito dalla Corte di Cassazione nella sentenza in questione, ha mutato orientamento sul punto.

Inoltre, allargando lo sguardo all'ambito europeo, si è ritenuto opportuno confrontare le conclusioni cui è giunta la Suprema Corte con quelle rese dall'Avvocato generale Jääskinen in ordine a un rinvio pregiudiziale – riguardante, da una parte, la qualificazione dei fornitori di servizi di motore di ricerca e, dall'altra, la possibilità di riconoscere un diritto all'oblio - sul quale la Corte di giustizia non si è ancora pronunciata.

Infine, si prenderà in considerazione anche il disegno di positivizzazione del diritto all'oblio all'interno della proposta di regolamento europeo in materia di protezione dei dati personali. Uno sguardo più ampio della tematica, che tenga conto altresì delle prospettive di riforma in materia, si ritiene necessario prima di dare spazio ad alcune riflessioni sulle ricadute della sentenza esaminata relativamente al dibattito filosofico, prima ancora che giuridico, avente ad oggetto il complesso

[330]Cass. civ., III sez., sentenza 5 aprile 2012, n. 5525.

rapporto tra memoria e oblio nella società dell'informazione.

2. Il fatto e l'*iter* processuale

Nella sentenza n. 5525 la Corte di Cassazione si sofferma brevemente sul fatto che ha dato origine alla controversia. Nel particolare, la Suprema Corte si limita ad accennare ad un'istanza di blocco dei dati personali contenuti in un articolo giornalistico che, in prima battuta, era stato pubblicato su un giornale di cui si omette il nome e, in seconda battuta, era stato inserito a fini consultivi nell'archivio storico *on-line* del medesimo giornale. Il soggetto interessato proponeva ricorso al Garante della protezione dei dati personali, godendo della possibilità concessa dall'art. 145 del c.d. Codice della *Privacy*[331], facendo valere il presunto diritto all'aggiornamento, rettificazione e integrazione dei dati *ex* art. 7 del medesimo Codice.

Di fronte al rigetto del ricorso da parte dall'Autorità garante, il ricorrente presentava opposizione al Tribunale di Milano senza sortire, tuttavia, esito migliore. Il Tribunale di Milano, infatti, con sentenza del 6 aprile del 2010 respingeva l'opposizione rigettando sia la domanda di «spostamento dell'articolo pubblicato molti anni prima in un'area di un sito *web* non indicizzabile dai motori di ricerca» sia la domanda di «integrazione dell'articolo con le notizie inerenti agli sviluppi successivi della vicenda narrata, con apposite modalità tecniche, anche non modificative della struttura originaria dello scritto»[332].

La sentenza del Tribunale si basava sulle seguenti motivazioni: in primo luogo, si rilevava «l'intrinseca contraddittorietà logica sussistente tra la richiesta applicazione del diritto a essere dimenticato e l'ineludibile funzione - espressione della stessa ragione d'essere di un'emeroteca - di offrire memoria storica delle vicende salienti di un'epoca, attraverso documenti redatti esercitando il diritto di cronaca giornalistica»; in secondo luogo, si giungeva a escludere anche «la configurabilità [in capo al ricorrente] dell'"invocato diritto all'oblio", essendo il medesimo soggetto che svolge attività di rilievo pubblico, contiguo ad ambienti di politico imprenditoriale». Inoltre, si escludeva che dal «mancato aggiornamento delle notizie a suo tempo pubblicate [potesse] all'interessato derivare l'ingiustificata lesione all'onore e alla reputazione» e, per di più, si osservava che «l'aggiornamento richiesto mediante l'inserimento di una sorta di *sequel* nell'articolo contenuto in archivio [avrebbe fatto venir meno] il valore di documento del testo stesso, vanificandone così la funzione storico-documentaristica»[333]. Contro tale sentenza, infine, il soggetto interessato proponeva ricorso per cassazione ai sensi del precedente art. 152, comma 13, del Codice[334], giungendo così alla sentenza in questione. In particolare, il ricorrente affidandosi a un unico complesso motivo, da una parte, si duole che il rigetto della prima domanda di spostamento dell'articolo in un'area del sito *web* non indicizzabile dai motori di ricerca sia stato viziato dall'erroneo rilievo secondo cui la ricerca effettuata attraverso i comuni motori desse in realtà contezza degli esiti processualmente favorevoli, e, dall'altra, si lamenta che il rigetto della domanda di integrazione dell'articolo si sia fondato sulla convinzione, smentita dall'art. 7 del Codice, che non vi fosse una normativa ponente in capo all'editore un onere di aggiornamento degli articoli in archivio.

3. Il diritto all'oblio: il "battesimo" nella sentenza n. 3679/1998 della Corte di Cassazione

Come anticipato, la sentenza in questione ha ad oggetto la tutela, ma prima ancora la configurazione e la delimitazione, del diritto all'oblio. Il diritto all'oblio è un diritto di creazione

331 D. lgs. 30 giugno 2003 n. 196, pubblicato nella *GU* n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123.

332 Corte di Cassazione, sentenza 5 aprile 2012, cit., pp. 4 e 5.

333 Sent. ult. cit., pp. 21, 22 e 23.

334 Articolo modificato dall'art. 34, comma 9 del decreto legislativo 1 settembre 2011, n. 150, con i limiti di applicabilità previsti dall'art. 36 dello stesso decreto legislativo 1 settembre 2011, n. 150. Il comma 13 è stato abrogato e la disciplina delle controversie di competenza dell'autorità giudiziaria ordinaria sono oggi disciplinate dall'articolo 10 del decreto legislativo 1 settembre 2011, n. 150.

giurisprudenziale, non disciplinato (ancora) dal legislatore. Per dirla con i giudici della Corte di Cassazione, che per la prima volta diedero cittadinanza al diritto all'oblio nel nostro ordinamento, esso è da intendere come il «giusto interesse di ogni persona a non restare indebitamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata»[335].

Nello specifico, il caso trattato dalla sentenza del 1998 riguardava - come è possibile desumere dal passo riportato - la (ri)pubblicazione di fatti avvenuti in passato e già oggetto di (una precedente) pubblicazione alcuni anni prima, di fronte alla quale la Corte ha potuto sancire il principio in base al quale il soggetto interessato può opporsi alla (ri)pubblicazione, eccependo proprio il diritto all'oblio, se non vi è più un interesse pubblico all'informazione. E' possibile osservare che la Cassazione nella sentenza in questione si limitò a fornire una definizione essenziale, che avrebbe inevitabilmente richiesto una specificazione da parte della giurisprudenza successiva al fine di un inquadramento del diritto all'oblio all'interno della normativa relativa alla protezione dei dati personali (v. par. 4).

Specificazione che, probabilmente, ha raggiunto il massimo grado di organicità proprio nella sentenza della Cassazione n. 5525/2012.

4. La controversa configurazione del diritto all'oblio nel caso di specie

Dovendo pronunciarsi su un caso inerente alla protezione dei dati personali, la Suprema Corte ha colto l'occasione, innanzitutto, per segnalare l'evoluzione della normativa in materia di *privacy*, compiutasi attraverso il passaggio dalla legge n. 675 del 1996 (legge di attuazione della direttiva 95/46) al decreto legislativo n. 196 del 2003 ("Codice in materia di protezione di dati personali"), evidenziando altresì che a una tale evoluzione ne sia corrisposta un'altra, riconosciuta anche dalla dottrina[336], relativamente al contenuto e alla concezione del diritto alla riservatezza. Con riguardo al primo aspetto, tale diritto «ha visto ampliarsi il proprio contenuto venendo a compendiarsi anche del diritto alla protezione dei dati personali»; mentre, per quanto concerne il secondo, «il decreto legislativo n. 196 del 2003 ha […] sancito il passaggio da una concezione statica a una concezione dinamica della tutela alla riservatezza, tesa al controllo dell'utilizzo e del destino dei dati»[337]. In questo quadro, il Codice della *Privacy* viene a configurarsi come un sistema di tutela non soltanto del diritto alla riservatezza *strictu sensu*, ma anche del diritto alla protezione dei dati personali nonché del diritto all'identità personale o morale.

Ad ogni modo, seppure tali diritti astrattamente siano distinguibili, nelle fattispecie concrete essi si ritrovano a essere spesso inscindibilmente connessi tra loro. Ne è una dimostrazione la fattispecie, esaminata dalla Cassazione, in cui il diritto all'oblio viene in rilievo come un'esigenza di tutela non solo del diritto alla riservatezza ma anche, principalmente, del diritto all'identità personale e morale. In generale, pertanto, ci si può facilmente rendere conto di come il diritto all'oblio si inserisca in un crocevia di altri diritti che necessitano di un bilanciamento.

Nello specifico, si può costatare che il diritto alla riservatezza (la cui rilevanza costituzionale è ricondotta dalla Corte di Cassazione non solo all'art. 2 Cost. ma anche all'art. 21 Cost., suscitando qualche perplessità in dottrina[338]) dev'essere contemperato con il diritto di informazione e alla informazione (tradizionalmente ricavato dall'art. 21 Cost.), mentre il diritto di cronaca trova un limite nel diritto all'identità personale o morale. A una tale esigenza di bilanciamento risponde l'art. 11 del decreto legislativo n. 196/2003 che stabilisce i criteri di liceità del trattamento di dati personali, correlativamente ai quali l'art. 7 definisce i diritti dell'interessato. Proprio sulla base delle suddette indicazioni normative, la Cassazione ha sancito la massima secondo la quale il titolare dell'organo di

335 Cass. civ., III sez., sentenza 9 aprile 1998, n. 3679.

336 L. FEROLA, *Riservatezza, oblio, contestualizzazione: come è mutata l'identità personale nell'era di* Internet, in F. PIZZETTI, *Il caso del diritto all'oblio,* Torino, 2013, p. 173 ss.

337 Cass. civ., sentenza 5 aprile 2012, cit., pp. 6 e 7.

338 Così F. DI CIOMMO, R. PARDOLESI, *Dal diritto all'oblio in* Internet *alla tutela dell'identità dinamica. E' la Rete, bellezza!*, in *DR,* 2012, p. 701 ss.

informazione è tenuto ad osservare i criteri di proporzionalità, pertinenza e non eccedenza dell'informazione, avuto riguardo alla finalità che ne consente il lecito trattamento.

La Corte, tuttavia, non si è limitata a richiamare le specifiche fonti normative del decreto legislativo n. 196/2003, e cioè i c.d. principi di proporzionalità, pertinenza e non eccedenza, sottolineando altresì che «è in ogni caso il principio di correttezza [...] a fondare in termini generali l'esigenza del bilanciamento in concreto degli interessi, e, conseguentemente, il diritto dell'interessato ad opporsi al trattamento, quand'anche lecito, dei propri dati»[339]. Il medesimo principio è stato peraltro richiamato dalla Suprema Corte, «in relazione ad una fattispecie diversa ma sotto certi aspetti assimilabile», anche in una recente sentenza[340], con la quale si è specificato ulteriormente che «proprio il rispetto di tale basilare regola dei rapporti privati impone di riconoscere che il diritto dell'interessato ad essere dimenticato intanto può cedere il passo rispetto al diritto di cronaca in quanto sussista un interesse effettivo ed attuale alla diffusione della notizia»[341].

Chiariti quindi i principi generali in base ai quali compiere il bilanciamento, è possibile prendere in considerazione la configurazione del diritto all'oblio operata dalla Cassazione. Essa, definendo meglio i contorni di un diritto ancora giovane e di conseguenza in via di modellazione, ha affermato che «il diritto all'oblio salvaguarda in realtà la proiezione sociale dell'identità personale, l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita (stante il lasso di tempo intercorso dall'accadimento del fatto che costituisce l'oggetto) di attualità delle stesse, sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della propria personalità»[342]. Tuttavia - come evidenziato già dalla sentenza n. 3679/1998 – se, da una parte, si pone l'interesse del soggetto a non vedere ulteriormente pubblicate o divulgate notizie che lo riguardano; dall'altra, potrebbe sussistere ancora un interesse pubblico all'informazione che giustifichi una nuova pubblicazione oppure, come nella fattispecie in questione in cui le informazioni erano conservate in un archivio *web*, un interesse pubblico alla relativa conoscenza o divulgazione per particolari esigenze di carattere storico, didattico, culturale. Da questa ricostruzione ricaviamo che l'esigenza di tutela del diritto all'oblio sorge non solo in seguito alla (ri)pubblicazione dell'informazione, ma anche in seguito alla permanenza della medesima nella memoria della rete *internet* e, a monte, nell'archivio del titolare del sito *web* (c.d. sito sorgente). La Corte, infatti, ha precisato che «con riguardo alla rete *internet* non si pone - diversamente da quanto affermato nell'impugnata sentenza - un problema di pubblicazione o di (ri)pubblicazione dell'informazione»[343]. Piuttosto, nel caso in questione, la conservazione dell'articolo, concernente una vicenda giudiziaria del ricorrente, nell'archivio *on-line* era da ritenere ammissibile per la finalità storica del trattamento, considerata compatibile con i diversi scopi per i quali i dati erano stati in precedenza trattati, rendendo pertanto lecito il trattamento pur in assenza di espresso consenso dell'interessato (art. 11, co. 1, lett. b) e art. 99 del d.lgs. 196/2003). Peraltro l'interesse pubblico alla persistente conoscenza di un fatto avvenuto in epoca di molto anteriore trovava giustificazione nell'attività (politica) svolta dal soggetto titolare dei dati. La Cassazione, giunta a tal punto, ha riconosciuto che «a fronte dell'esigenza di garantire e mantenere la memoria dell'informazione si pone […] il diritto all'oblio del soggetto cui l'informazione si riferisce»[344]. Diritto che la Corte ha voluto considerare come un «diritto di controllo a tutela della proiezione dinamica dei propri dati e della propria immagine sociale, che può tradursi, anche quando trattasi di notizia vera – e *a fortiori* se di cronaca – nella pretesa alla contestualizzazione e all'aggiornamento della notizia, e se del caso, avuto riguardo alla finalità della conservazione nell'archivio e all'interesse che la sottende, financo alla relativa cancellazione»[345]. Tale configurazione tuttavia non è stata esente da critiche, essendosi rivelato che «nella fattispecie non emerge tecnicamente

339 Cass. civ., sentenza 5 aprile 2012, cit., p. 8.

340 Cass. civ., III sez., sentenza 26 giugno 2013, n. 16111.

341 Sent. ult. cit., pp. 14 e 15.

342 Cass. civ., sentenza 5 aprile 2012, cit., p. 9.

343 Sent. ult. cit., p. 15.

344 Sent. ult. cit., p. 14.

345 Sent. ult. cit., p. 14 e 15.

l'esigenza di tutelare il diritto all'oblio [...] bensì la differente esigenza dell'interessato a che la notizia in questione non sia resa disponibile *on-line* in quanto, non essendo completa ed aggiornata, giacché non fa espresso riferimento al successivo proscioglimento, getta un intollerabile alone di discredito sulla persona del ricorrente, vittima di una vera e propria gogna mediatica»[346]. Gli stessi commentatori inoltre, considerato il sussistente interesse pubblico alla permanenza dell'informazione, hanno avvalorato la critica argomentando che nella fattispecie «non c'è qualcuno che propone, *rectius* ripropone, la vecchia notizia ad una comunità indistinta di possibili fruitori, incurante del fatto che nella comunità in questione l'interesse pubblico alla conoscenza della notizia non è più sussistente»[347]. Siffatte critiche sembrano essere dettate dall'assenza nella sentenza di un passaggio logico necessario ai fini della suddetta configurazione del diritto all'oblio, la cui portata è stata estesa dalla Cassazione fino a configurarlo come il "diritto ad essere dimenticati" (potremmo dire meglio "non più identificati") da un'immagine sociale frutto di vicende passate, vere al momento del loro trattamento quali notizie di cronaca ma non più rispondenti a verità ed esattezza in un momento successivo. Intendendo così il diritto all'oblio, la Cassazione è passata a trarre le conclusioni del caso in questione.

5. Le Conclusioni della Suprema Corte

Dopo aver configurato il diritto all'oblio nel caso di specie, la Cassazione ha focalizzato l'attenzione sulla necessità di integrazione e di aggiornamento dell'informazione, e cioè sulla necessità di un «collegamento della notizia ad altre informazioni successivamente pubblicate concernenti l'evoluzione della vicenda, che possano completare o financo radicalmente mutare il quadro evincentesi della notizia originaria»[348]. Pertanto, poiché solo in seguito a queste operazioni il trattamento dei dati personali sarebbe risultato lecito e corretto nel rispetto «sia del diritto all'identità personale o morale del titolare, nella sua proiezione sociale, del dato oggetto di informazione, sia dello stesso diritto del cittadino utente a ricevere una completa e corretta informazione»[349], è stato riconosciuto al ricorrente il diritto di ottenere l'integrazione e l'aggiornamento della notizia in argomento a lui relativa sulla base dell'art. 7, co. 3, lett. a), d.lgs. n. 196/2003.

Sancita l'esigenza di aggiornamento e di integrazione, si è posto il problema di delineare il *quomodo* della tutela, le modalità di relativa attuazione nonché, prima ancora, di individuare il soggetto sul quale grava l'obbligo di aggiornamento o di integrazione.

Riguardo al primo aspetto, ad avviso della Corte, è apparsa necessaria una misura che consentisse «l'effettiva fruizione della notizia aggiornata, non potendo (diversamente da quanto affermato dal Garante nella memoria) considerarsi in proposito sufficiente la mera generica possibilità di rinvenire all'interno del "mare di internet" ulteriori notizie concernenti il caso di specie, ma richiedendosi la predisposizione di sistema idoneo a segnalare (nel corpo o a margine) la sussistenza nel caso di un seguito e di uno sviluppo della notizia, e quale esso sia, consentendone il rapido ed agevole accesso ai fini del relativo adeguato approfondimento»[350]. Tale disposto è stato interpretato da alcuni esponenti della dottrina come un obbligo di aggiornamento che scatti non solo a seguito della formale richiesta dell'interessato secondo l'analoga procedura di rimozione meglio nota come procedura di "notice and take down", ma anche «a prescindere da qualsiasi iniziativa di chicchessia»[351]. In effetti la Corte non è stata chiara sul punto, ma avendo riconosciuto l'azionabilità dell'art. 7, co. 3 del d.lgs. n. 196/2003 si potrebbe comunque desumere che essa volesse prevedere un sistema basato sulla presentazione di un'istanza dell'interessato all'aggiornamento/integrazione dei propri dati con conseguente obbligo (successivo) di soddisfare la richiesta.

346 F. DI CIOMMO, R. PARDOLESI, *Dal diritto all'oblio in* Internet, cit., p. 703.
347 F. DI CIOMMO, R. PARDOLESI, *Dal diritto all'oblio in* Internet, cit., p.706.
348 Cass. civ., sentenza 5 aprile 2012, cit., p. 11.
349 Sent. ult. cit., p. 17.
350 Sent. ult. cit., p. 20.
351 F. DI CIOMMO, R. PARDOLESI, *Dal diritto all'oblio in* Internet, cit., p. 704.

Riguardo invece al secondo aspetto (o meglio, quesito), e cioè l'individuazione del soggetto sul quale grava l'obbligo, la Corte si è soffermata sui caratteri dei siti sorgente e dei motori di ricerca, operando le dovute differenziazioni, al fine di rispondere al quesito. Essa, in realtà, non ha proceduto con ordine: dopo aver compiuto inizialmente una distinzione tra "archivio" e "memoria della rete internet" («mentre l'archivio si caratterizza per essere ordinato secondo criteri determinati, con informazioni intercorrelate volte ad agevolarne l'accesso e a consentirne la consultazione, la rete *internet* costituisce in realtà un ente ove le informazioni non archiviate ma solo memorizzate», essa quindi «non è un archivio, ma un deposito di archivi»[352]), è giunta a concludere che «gli archivi sono quelli dei singoli utenti che accedono alla rete, dei titolari dei siti, che costituiscono invero la fonte dell'informazione (c.d. siti sorgente)», di contro il motore di ricerca è «un mero fornitore del servizio di fruizione della rete, limitandosi a rendere sul sito *web* i dati dei c.d. siti sorgente, assolvendo ad un'attività di mero trasporto delle informazioni»[353]. Tuttavia, solo dopo parecchi paragrafi, la Cassazione, applicando la distinzione operata, ha stabilito che «è il titolare del sito [...] e non già il motore di ricerca (nel caso, *Google*), a dover provvedere al raggiungimento del suindicato obiettivo»[354], prendendo in tal modo una posizione su un tema sicuramente controverso e di grande attualità, come dimostra il parere dell'Avvocato generale nella causa C-131/12[355].

6. Il "peso" della Cassazione sulle decisioni del Garante della protezione dei dati personali

La decisione di porre a carico del titolare del sito sorgente un obbligo di aggiornamento/integrazione ha segnato una svolta nel panorama giurisprudenziale del nostro ordinamento. In particolare, la suddetta decisione ha avuto rilevanti ripercussioni sugli orientamenti del Garante della protezione dei dati personali. Infatti, la posizione del Garante, che nel processo in questione costituiva una delle parti resistenti, era contraria all'integrazione e all'aggiornamento della notizia avendo rigettato a monte l'istanza di blocco dei dati personali del ricorrente. D'altronde il Garante, in precedenti provvedimenti, aveva ritenuto infondate le richieste di aggiornamento delle notizie «non potendosi disporre un intervento modificativo e/o integrativo del contenuto di un articolo che, nato come espressione di libera manifestazione del pensiero, ad oggi è legittimamente conservato, per finalità di documentazione, all'interno di un archivio che, benché informatizzato, svolge pur sempre la medesima funzione degli archivi cartacei»[356].

Il Garante, tuttavia, com'era facile prevedere, non è stato insensibile alle prese di posizione della Suprema Corte e pertanto, con soluzione di continuità, in un recente provvedimento ha stabilito - richiamando la sentenza n. 5525/2012 - che «come indispensabile corollario della riconosciuta liceità della conservazione degli articoli di cronaca a suo tempo pubblicati nella sezione del sito *internet* [...] denominato archivio storico, va garantito il diritto (pienamente compreso fra le posizioni giuridiche azionabili ai sensi dell'art. 7 del Codice) dell'interessato ad ottenere l'aggiornamento/integrazione dei dati personali che lo riguardano quando eventi e sviluppi successivi abbiano modificato le situazioni oggetto di cronaca giornalistica (seppure a suo tempo corretta) incidendo significativamente sul profilo e sull'immagine dell'interessato che da tali rappresentazioni può emergere»[357].

352 Cass. civ., sentenza 5 aprile 2012, cit., p. 12.

353 Sent. ult. cit., p. 13.

354 Sent. ult. cit., p. 17.

355 Vedi par. 7, causa *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*.

356 Decisione del Garante n. 196 del 19 maggio 2011, doc. *web* n. 1821331.

357 Decisione del Garante n. 31 del 24 gennaio 2013, doc. *web* n. 2286820.

7. Uno sguardo europeo: la qualificazione di fornitore di servizi di motore di ricerca e la configurabilità di un diritto all'oblio nella causa C-131/12

La decisione della Cassazione di porre l'obbligo di aggiornamento e integrazione in capo al titolare del sito sorgente e non anche al gestore del motore di ricerca lambisce - come accennato - il delicato tema, di grande attualità, riguardante gli obblighi del fornitore di servizi di motori di ricerca su *internet*. A tal proposito è possibile menzionare un recente rinvio pregiudiziale, proposto dall'Audiencia Nacional spagnola innanzi alla Corte di giustizia, avente ad oggetto il rapporto tra la disciplina affidata alla direttiva 95/46/CE e gli *Internet Service Providers* che gestiscono un motore di ricerca, *Google* nel caso di specie. Per quanto riguarda il fatto in causa, si possono rilevare delle somiglianze con il fatto esaminato dalla Corte di Cassazione nella sentenza n. 5525/2012: anche in questo caso, infatti, un soggetto ha presentato reclamo all'Autorità nazionale per la protezione dei dati personali chiedendo di ordinare all'editore la rimozione o la modifica dell'informazione pubblicata che lo riguardava. Tuttavia, a dispetto del caso giunto innanzi alla Corte di Cassazione italiana, il ricorrente ha chiesto altresì di ordinare a *Google* di eliminare o occultare i suoi dati, in modo che non comparissero più tra i risultati della ricerca né mostrassero più *links* al quotidiano. In seguito all'accoglimento del reclamo contro *Google*, quest'ultimo ha adito l'Audiencia Nacional (Alta Corte nazionale in Spagna), la quale a sua volta ha proposto una domanda di pronuncia pregiudiziale alla Corte di giustizia. La Corte lussemburghese si deve ancora pronunciare mentre sono state già rese le considerazioni dell'Avvocato generale[358].

Quest'ultimo, dopo aver ritenuto applicabile la normativa in materia di protezione dei dati personali anche al gestore di un motore di ricerca che crea in uno Stato membro un ufficio svolgente attività indirizzate agli abitanti dello stesso Stato ai fini della promozione e della vendita di spazi pubblicitari nel motore di ricerca, si è potuto soffermare sulle restanti due questioni riguardanti rispettivamente l'applicabilità della direttiva 95/46 al fornitore di servizi di motore di ricerca e la possibilità di configurare un diritto all'oblio generalizzato sulla base delle norme contenute nella direttiva stessa. Sul primo dei due quesiti appena illustrati, l'Avvocato generale riconosce che «un fornitore di servizi di motore di ricerca su *internet* "tratta" dati personali ai sensi dell'articolo 2, lettera b), della direttiva, tuttavia […] non può essere considerato "responsabile del trattamento" di tali dati personali ai sensi dell'articolo 2, lettera d), della direttiva»[359], considerato che se «offre semplicemente uno strumento di localizzazione delle informazioni, non esercita alcun controllo sui dati personali contenuti in pagine web di terzi»[360]: il controllo è escluso in quanto «il motore di ricerca lavora sulla base di copie di pagine web source che il crawler ha estratto e copiato»[361] e che pertanto il fornitore di servizi non è in grado di cambiare. Dopo tali considerazioni, l'Avvocato generale avverte che la risposta all'ultimo quesito sollevato, riguardante – come detto sopra – il diritto all'oblio, sarà rilevante solo nell'ipotesi in cui la Corte ritenesse di non condividere le soluzioni prospettate in merito alla questione precedente.

Premesso ciò, l'Avvocato Jääskinen verifica se sulla base dell'art. 12, lett. b) della direttiva - diritto dell'interessato di ottenere la cancellazione e il congelamento dei dati personali - e dell'art. 14, lett. a) della medesima - diritto dell'interessato di opporsi al trattamento - si possa riconoscere un diritto all'oblio assoluto. La risposta che viene data è negativa. Sotto il primo profilo, il diritto alla rettifica, alla cancellazione e al congelamento dei dati sorge solo nel caso in cui il trattamento non è conforme alle disposizioni della direttiva, in particolare a causa della loro incompletezza o inesattezza. Sotto il secondo profilo, va rilevato che il diritto di opporsi al trattamento di dati non può considerarsi il diritto di limitare o di porre fine alla diffusione di tutti i dati personali che l'interessato consideri nocivi o contrari ai propri interessi; piuttosto «sono lo scopo del trattamento e gli interessi da esso tutelati, confrontati con quelli della persona interessata, e non le preferenze di quest'ultima, i criteri da applicare

358 Conclusioni dell'Avvocato generale Niilo Jääskinen presentate il 25 giugno 2013, causa C-131/12, *Google Spain SL, Google Inc. c. Agencia Espanõla de Protección de Datos (AEPD), Mario Costeja González*.

359 Conclusioni ult. cit., punto 100.

360 Conclusioni ult. cit., punto 84.

361 Conclusioni ult. cit., punto 86.

allorché i dati vengono trattati senza il consenso della stessa»[362]. Infine, l'Avvocato generale esclude altresì la possibilità di riconoscere un diritto all'oblio sulla base della Carta dei diritti fondamentali dell'Unione europea. Infatti, nemmeno un'interpretazione della direttiva alla luce della Carta (in particolare dell'art. 7 che riconosce il diritto al rispetto della vita privata e familiare) permette di ricavare un diritto all'oblio generalizzato dal momento che occorre bilanciare questo diritto con diritti fondamentali, come la libertà di espressione e di informazione (art. 11) e la libertà di impresa (art. 16), che fanno capo ai vari soggetti coinvolti nel trattamento. Indubbiamente sarebbe necessario operare un bilanciamento ma l'Avvocato Jääskinen invita esplicitamente la Corte a «non concludere che questi interessi concorrenti possono essere ponderati in modo soddisfacente in situazioni individuali sulla base di una valutazione caso per caso, lasciando la decisione ai fornitori di servizi di motore di ricerca su internet in quanto simili "procedure di notifica e rimozione", se la Corte le richiedesse, porterebbero probabilmente o al ritiro automatico dei link verso qualsiasi contenuto oggetto di un'opposizione oppure ad un numero ingestibile di richieste ai fornitori di servizi di motori di ricerca su internet più popolari e importanti»[363].

A fronte quindi delle suddette posizioni assunte dall'Avvocato generale, non resta che attendere la pronuncia della Corte che sembra essere destinata a influire in maniera rilevante in una prospettiva di *de iure condendo*, come evidenziato nei primi commenti dalla dottrina[364].

7.1. La sentenza n. 5525/2012 al "vaglio" delle Conclusioni dell'Avvocato generale: un confronto proficuo

Dopo aver analizzato le Conclusioni dell'Avvocato generale si può notare che sussistono sia dei punti di contatto che dei punti di contrasto con quanto affermato dalla nostra Cassazione nella sentenza oggetto di commento. Per quanto riguarda i primi, va evidenziato che la tesi, sostenuta dall'Avvocato generale, secondo cui i gestori di un motore di ricerca non sono qualificabili come responsabili del trattamento (quanto meno con riguardo all'attività di localizzazione delle informazioni) è una conclusione ricavabile, seppur in maniera implicita, anche nella sentenza n. 5525/2012 nel passaggio in cui la Corte di Cassazione ha constatato che «il motore di ricerca è un mero intermediario telematico, che offre un sistema di reperimento di dati e informazioni attraverso parole chiave, un mero database che indicizza i testi sulla rete e offre agli utenti un accesso per la relativa consultazione». Se la qualifica dei fornitori di servizi di motore di ricerca, quindi, è un punto di contatto, non altrettanto si può dire sulla configurabilità del diritto all'oblio. La Cassazione, infatti, contrariamente all'Avvocato generale, giunge a riconoscere un diritto all'oblio sulla base dell'art. 7 del Codice sulla protezione dei dati personali: disposizione attuativa dei principi sanciti negli artt. 12 e 14 della direttiva 95/46. Diritto all'oblio che peraltro sembra prevalere anche sulla legittima finalità del trattamento: la Suprema Corte chiarisce che «[s]e il passaggio dei dati all'archivio storico è senz'altro ammissibile, ai fini della liceità e correttezza del relativo trattamento e della relativa diffusione a mezzo della rete internet è indefettibilmente necessario che l'informazione e il dato trattato risultino debitamente integrati e aggiornati». A parere dell'Avvocato generale, invece, «la libertà di informazione dell'editore di un giornale tutela il suo diritto di ripubblicare su internet in via digitale le proprie copie cartacee» e pertanto «nulla può giustificare la richiesta di una nuova pubblicazione, in formato digitale, del numero di un giornale con un contenuto diverso da quello della versione cartacea originariamente edita. Ciò equivarrebbe ad un falso storico».

Le convergenze/divergenze che intercorrono tra la sentenza della Cassazione e le Conclusioni dell'Avvocato generale Jääskinen in merito alla causa C-131/12 dimostrano che la configurazione del diritto all'oblio è un'operazione ancora in *fieri*: saranno necessarie senza dubbio altre pronunce giurisprudenziali (in *primis* quella della Corte di giustizia nel caso trattato) ma è auspicabile, al tempo stesso, un intervento del legislatore europeo.

362 Conclusioni ult. cit., punto 108.

363 Conclusioni ult. cit., punto 133.

364 O. POLLICINO, M. BASSINI, *Il diritto all'oblio a Lussemburgo,* in *Diritto 24*, 27 giugno 2013.

8. Prospettive di regolamentazione del diritto all'oblio: l'art. 17 della proposta di regolamento in materia di protezione di dati personali

Vista l'incertezza degli orientamenti giurisprudenziali circa il riconoscimento e, anche quando riconosciuto, circa i confini di un possibile diritto all'oblio, il legislatore europeo - come auspicato - sta pensando di intervenire sul tema. E' l'art. 17 della proposta di regolamento del Parlamento europeo e del Consiglio[365] ad avere ad oggetto, per il momento, la disciplina del diritto all'oblio. Il suddetto articolo sancirebbe al par. 1 che «l'interessato ha il diritto di ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati» in presenza di determinate condizioni e al par. 2 che «il responsabile del trattamento di cui al par. 1 prende tutte le misure ragionevoli, anche tecniche, in relazione ai dati della cui pubblicazione è responsabile per informare i terzi che stanno trattando tali dati sulla richiesta dell'interessato di cancellare link, copia o riproduzione dei suoi dati personali». Tuttavia, non mancano le esenzioni tra cui rientra – in base al par. 3, lett. a) - la conservazione dei dati personali per l'esercizio del diritto alla libertà di espressione.

Esenzione che rappresenta uno dei principali nodi dell'attuale proposta, come evidenziato dal Gruppo di lavoro per la tutela dei dati *ex* art. 29 nel parere 01/2012[366], nel quale dopo aver riconosciuto «il bisogno di mantenere un equilibrio tra i diritti alla vita privata e il diritto alla libertà di espressione», ha ammonito che «il regolamento dovrebbe chiarire il rapporto tra l'articolo 17, paragrafo 3, e l'obbligo previsto all'articolo 17, paragrafo 2».

9. Qualche motivo di riflessione

Pensare che l'oblio sia un problema strettamente giuridico è assolutamente fuorviante. Piuttosto è bene segnalare che il diritto si inserisce solo di recente in una questione che impegna la filosofia e la letteratura da tempi immemori. Si deve riconoscere quindi che sono stati proprio i filosofi a porre l'accento, per primi, sull'importanza dell'oblio: citando Gadamer «solo attraverso il dimenticare lo spirito conserva la possibilità del rinnovamento totale, la capacità di vedere tutto con occhi nuovi, in maniera da fondare in una articolata unità ciò che è familiare con ciò che nuovamente gli appare»[367].

Più in generale, inoltre, si può dire che il tema dell'oblio è strettamente connesso a quello della memoria e in quest'ultimo ambito rilevanti sono i contributi di Avishai Margalit nei suoi studi dedicati all'etica della memoria[368]. Studi che, tuttavia, ad avviso della dottrina[369], non sembrano adattarsi ai nuovi caratteri della società dell'informazione e al suo prodotto, una memoria informatizzata.

Ci si avvicina così al nocciolo della questione: è possibile porre dei limiti alla memoria informatizzata, tendenzialmente imperitura? La sentenza della Cassazione, in fondo, tenta di rispondere, naturalmente sulla base dei dati normativi vigenti, a quest'interrogativo. D'altronde, le critiche che le sono state rivolte, oltre che fondarsi su argomentazioni prettamente giuridiche[370], vertono proprio sulla risposta fornita al suddetto interrogativo. Così, in merito al riconoscimento del diritto all'oblio operato dalla Cassazione, si è sostenuto che «la pretesa dell'interessato sembra violare, in qualche modo, la riservatezza, o comunque le potenzialità della memoria di ognuno degli altri consociati, nonché della memoria collettiva, la quale, peraltro, nell'era digitale non conosce limiti, ed in definitiva il diritto dell'uomo alla conoscenza, cui la memoria è da sempre finalizzata»[371]. Inoltre, se a questi problemi di principio - ai quali, come visto, non è semplice dare una soluzione - si aggiungono i problemi tecnico-fattuali legati alla gestione dei siti *web*, si arriva a comprendere maggiormente quanto complicato sia il

365 Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), COM(2012) 11 def.
366 Parere 01/2012 – WP 191 sulle proposte di riforma in materia di protezione dei dati adottato il 23 marzo 2012.
367 H.G. GADAMER, *Verità e metodo*, Milano, 2000, p. 55.
368 A. MARGALIT, *L'etica della memoria*, Bologna, 2006, p. 15.
369 S. AMATO, *Il diritto all'oblio*, in S. AMATO, F. CRISTOFARI, S. RACITI, *Biometria, i codici a barre del corpo*, Torino, 2013, p. 115.
370 Vedi note 345 e 346.
371 F. DI CIOMMO, R. PARDOLESI, *Dal diritto all'oblio in* Internet*,* cit., p. 707.

tema. Nello specifico, si fa riferimento alle oggettive difficoltà tecniche di realizzazione, da parte dei *content providers*, di un sistema sullo schema di quello indicato dalla Cassazione per l'aggiornamento e l'integrazione dei dati. Secondo i critici, sarebbe in gioco la stessa natura della Rete in quanto è possibile preservare l'attuale ricchezza di *internet* solo riconoscendo ad ogni *provider* «il diritto a realizzare o implementare un archivio online in una certa occasione o per un certo periodo, senza poi essere, per ciò solo, costretto a rielaborarlo costantemente nel tempo a venire, peraltro con informazioni che potrebbero essere anche difficili da rinvenire»[372].

Di fronte alla complessità della questione, è evidente che sarebbe eccessivamente ambizioso assumere una posizione in merito. Ci si può limitare, piuttosto, a mettere in rilievo che il processo di configurazione del diritto all'oblio è controverso e ancora *in fieri* e, in questo quadro, la sentenza della Corte di Cassazione italiana rappresenta senza dubbio una tappa rilevante, a prescindere dalle tracce che lascerà nel percorso ad ostacoli che è attualmente il tentativo di regolazione giuridica del "mare di internet".

372 F. DI CIOMMO, R. PARDOLESI, *Dal diritto all'oblio in* Internet*,* cit., p.715.

V. IL CASO *GOOGLE-VIVIDOWN*: L'INTRICATO PROBLEMA DEL GOVERNO DI *INTERNET*

di Elisa Gulizzi

Sommario: 1. Premessa. - 2. Il fatto. - . Profili giuridici. - *3.1 Il concorso nel reato di diffamazione*. - *3.2 Illecito trattamento dei dati personali*. - *3.2.1 Il requisito del nocumento*. - *3.2.2. Il presupposto elemento oggettivo*. - *3.2.3 Il requisito del dolo specifico*. - 4. La responsabilità degli IPS in precedenti casi giurisprudenziali. - 5. Alcune poche considerazioni conclusive.

1. Premessa

Con sentenza 21 dicembre 2012[373], la Corte d'Appello di Milano prende posizione sulla complessa e annosa questione della responsabilità dei fornitori di servizi *internet*. La Corte ribalta le conclusioni della sentenza di primo grado[374] ed esclude la responsabilità penale dell'*internet service provider* (d'ora in poi ISP) per violazione dell'art. 167 d.lgs. 196/2003. Anzitutto infatti non è rinvenibile alcun nesso tra l'obbligo di tutelare informazioni sensibili e il dovere di impedirne la diffamazione. Ed inoltre sull'ISP, quale che sia la sua natura, non grava alcun obbligo di informativa, penalmente sanzionato, destinato all'*uploader* che carica contenuti sullo spazio messo a disposizione dal *provider* stesso. La Corte dunque riforma la sentenza di primo grado limitatamente al capo d'imputazione relativo alla violazione della normativa sulla *privacy*: nessuna disposizione del d.lgs. 196/2003 impone all' ISP di «rendere edotto l'utente circa l'esistenza e i contenuti della legge della privacy».

Il caso, lungi dall'aver provocato "molto rumore per nulla"[375] è tristemente noto: ha scosso l'opinione pubblica, indignata dalla vicenda, attirato l'attenzione dei *media*, considerato che il processo è pressoché un *unicum* nel panorama mondiale; e ha sollecitato la riflessione dei giuristi sulla gestione e il governo di *internet*.

2. Il fatto

L'analisi della sentenza d'Appello non può prescindere da riferimenti puntuali alla sentenza[376] resa dal giudice di prime cure, anzitutto per la precisione con la quale vengono ricostruiti i fatti.

In un istituto tecnico torinese alcuni ragazzi aggrediscono un compagno di classe affetto da sindrome di *Down*, lo offendono ripetutamente e lo colpiscono con oggetti, mentre gli altri compagni di classe e persino l'insegnante assistono inerti alla condotta abietta dei giovani. Questi ultimi filmano il proprio comportamento vessatorio e caricano il video su *Google Video*; il video diviene popolare per il numero di visualizzazioni ottenute, tanto che risulta essere il primo della classifica dei "video più divertenti" e addirittura compare anche nella classifica dei video più scaricati in assoluto.

L'associazione *Vividown*, citata nel video, deposita una denuncia di querela e lo stesso farà poco dopo il padre del ragazzo vessato dai compagni. Il video viene eliminato tempestivamente a seguito di due richieste di rimozione dello stesso.

Le ipotesi di reato addebitate ai dirigenti di *Google* sono concorso in diffamazione aggravata e trattamento illecito dei dati personali *ex* art. 167 legge sulla *Privacy*[377].

---

373 C. App. Milano, sent. n. 8611/2012.

374 Trib. Milano, sez. IV, 24 febbraio 2010, n. 1972, Est. Magi.

375 Così scriveva il giudice O. Magi nelle conclusioni della sentenza di primo grado del 24 febbraio 2010 n.1972, parafrasando il titolo di una famosa commedia di Shakespeare "much ado about nothing".

376 Tribunale di Milano, 24 febbraio 2010, n. 1972.

377 Decreto legislativo 30 giugno 2003, n. 196.

3. Profili giuridici

3.1. Il concorso nel reato di diffamazione

La Corte d'Appello non si discosta dalle conclusioni cui era giunto il giudice monocratico e assolve gli imputati dal reato di diffamazione.

Nella sentenza di primo grado, infatti, non si condivideva l'assunto dell'accusa, che costruiva una posizione di garanzia a carico degli imputati in termini di controllo preventivo dei contenuti del video: la permanenza del video sulla piattaforma *Google Video*, fino alla rimozione avvenuta a fronte di una doppia segnalazione, «costituirebbe una evidente compartecipazione omissiva al reato di diffamazione».

Tuttavia, sottolinea la Corte d'Appello, perché sorga responsabilità in capo all'ISP occorre ravvisare un obbligo giuridico di impedire l'evento e nello specifico verificare la sussistenza di una posizione di garanzia e «la concreta possibilità di effettuare un controllo preventivo».

Il diritto vigente non delinea alcuna posizione di garanzia in capo agli ISP; riecheggiando la tradizionale teoria del trifoglio, la posizione di garanzia può sorgere oltre che per legge, penale o extrapenale anche per contratto o precedente azione pericolosa: escludendo l'ipotesi del contratto e visto che la diffusione di informazioni non può essere considerata un'attività pericolosa *ex* art. 2050 cc, la posizione di garanzia non potrebbe che scaturire da una norma. Tuttavia la legislazione attualmente vigente non prevede una posizione di garanzia siffatta e dunque non è riscontrabile alcun nesso tra l'obbligo di tutelare le informazioni sensibili e il dovere di impedirne la diffamazione.

La Corte d'Appello esclude poi l'applicabilità degli artt. 57 e 57 *bis* cp in materia di stampa, tesi condivisa dalla dottrina dominante[378] e accolta in diverse sentenze di merito[379] e di legittimità[380]. L'art. 57 cp sancisce la responsabilità del direttore o vice-direttore responsabile per omesso controllo, necessario per impedire la commissione di reati attraverso la pubblicazione del periodico.

L'impossibilità di estendere la responsabilità dell'art. 57 cp al direttore di un periodico *online* muove dalla definizione di stampa dell'art. 1 della l. 8 febbraio 1948, n. 47 (Disposizioni sulla stampa), in forza del quale «sono considerate stampe o stampati, ai fini di questa legge, tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione». Da questa definizione si ricava una sostanziale differenza tra il prodotto stampato e il prodotto di *internet* considerato che quest'ultimo non soddisfa le due condizioni richieste dall'art. 1: un *prius,* cioè che vi sia una riproduzione tipografica, e un *posterius,* ovvero sia che il prodotto di quest'attività sia distribuito tra il pubblico in quanto destinato alla pubblicazione. Infatti, la diffusione del contenuto di un periodico *online* avviene attraverso la visualizzazione del suo contenuto da parte dei destinatari e la stampa del prodotto è da considerarsi una mera eventualità. Esistono, poi, delle ragioni di ordine sistematico che concorrono ad escludere l'applicabilità dell'art. 57 cp insieme alla suddetta impossibilità di ricorrere a un meccanismo analogico in *malam partem*: dottrina e giurisprudenza hanno segnalato infatti la difficoltà di individuare una condotta concretamente esigibile da parte del direttore del periodico *online*. Questa tesi non è stata scalfita dall'introduzione della l. 7 marzo 2001, n. 62[381] con la quale sono state applicate anche all'editoria elettronica alcune disposizioni concernenti l'obbligo di registrazione e indicazioni obbligatorie: si tratta di rinvii settoriali che non consentono di affermare l'assimilazione tra prodotto stampato e prodotto di *internet*.

---

378 S. SEMINARA, *La pirateria su* Internet *e il diritto penale*, in *RTDPE*,1997, p. 94; L. PICOTTI, *I profili penali delle comunicazioni illecite via* Internet*,* in *DII*, 1999, p. 299.

379 In particolare, Trib. Milano, 18 marzo 2004, Pres. Della Chiara, Est. Simi, in *Gmer*, 2004, n. 2523 con nota di G. CORRIAS LUCENTE, *Ma i* network providers*, i* service providers *e gli* access providers *rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che loro gestiscono?*.

380 Si veda Cass. pen., sez. V, 16 luglio 2010, n. 35511 in *DPC*, con nota di S. TURCHETTI, *L'art. 57 c.p. non è applicabile al direttore del periodico* online; e più di recente Cass. pen., sez. V, 28 ottobre 2010, n. 44126 in *DPC*, con nota di S. TURCHETTI, *Un secondo* "alt" *della Cassazione all'applicazione dell'art. 57 c.p. al direttore del periodico online*.

381 Nuove norme sull'editoria e sui prodotti editoriali e modifiche alla l. 5 agosto 1981, n. 416.

Argomentando *ad abundantiam*, si può segnalare che il reato di diffamazione viene considerato pacificamente un reato di evento[382], dunque, nel caso di specie, per impedire la commissione del fatto, il *provider* avrebbe dovuto impedire l'evento tramite un controllo preventivo.

In altre parole il gestore del sito dovrebbe sottoporre a un sistema di filtraggio precauzionale tutti i contenuti in esso caricati, il che si rivela estremamente complesso dal punto di vista tecnico e fattuale[383] ed è inoltre difficilmente concepibile già a livello teorico: sulla base di quale sistema normativo e valoriale si dovrebbe effettuare questo controllo? Il servizio sarebbe così destinato ad essere snaturato nelle sue finalità.

Nella sentenza d'appello dunque si ribadisce che non esiste né un sostegno fattuale né tantomeno normativo all'impianto accusatorio del processo di primo grado.

3.2. L'illecito trattamento dei dati personali

La sentenza di primo grado riconosce gli imputati responsabili del reato contestato al capo (b) d'imputazione per violazione dell'art. 167 commi, 1 e 2[384], del d.lgs. 196/2003 ("Codice della privacy") facendo discendere la responsabilità non già dalla sussistenza di una posizione di garanzia, non configurabile alla luce del diritto vigente, ma dalla violazione dell'obbligo di informativa sancito dall'art.13 "codice privacy".

Bisogna procedere anzitutto all'analisi delle suddette norme; chiarito il quadro normativo di riferimento si potranno comprendere le ragioni del "dietrofront" della Corte d'Appello che assolve gli imputati anche relativamente a questo secondo capo di imputazione perché il fatto non sussiste.

Anzitutto dunque, perché si configuri il reato prospettato dal richiamato art. 167 è necessaria la compresenza dei seguenti elementi: il trattamento dei dati sensibili, la mancanza del consenso da parte del soggetto, il nocumento della persona offesa ed infine il dolo specifico del soggetto agente.

3.2.1. Il requisito del nocumento

Mentre a proposito dei primi due elementi è indubbio che nel caso di specie siano rispettivamente l'uno assente e l'altro presente, e che non occorrano ulteriori approfondimenti, diversamente occorre dire del nocumento. Esso è infatti ugualmente presente; ma si richiedono alcune importanti considerazioni.

Il concetto di nocumento è stato al centro di una vivace *querelle* in dottrina, ed è stato infine oggetto di una pronuncia della Corte di Cassazione[385]. Nel caso di specie l'imputato era stato condannato in appello, sulla base dell'art. 35 l. 675/1996[386], per illecito trattamento dei dati personali, svolto senza il consenso degli interessati, iscritti ad un'associazione alla quale lo stesso imputato apparteneva, per fini di propaganda elettorale. In considerazione della disciplina sopravvenuta con il

---

382 Così Cass. pen., sez. I, sentenza 26 aprile 2011, n. 16307 che recepisce la soluzione teorica prospettata in dottrina, tra gli altri, da V. SPAGNOLETTI, *Profili problematici del reato di diffamazione a mezzo* internet, in *Gmer*, 2003, 7-8, p. 1616.

383 In questo senso E. ARPA, O. POLLICINO, *Modeling the liability of Internet Service Providers: Google vs. Vividown. A constitutional perspective*, Milano 2013, p. 59.

384Per chiarezza espositiva si riporta per esteso il testo dell'art.167 codice *privacy*, rubricato "trattamento illecito dei dati" che sancisce: «1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.».

385 Cass. pen., sez. III, sentenza 9 luglio 2004, n. 30134.

386 Legge n. 675 del 31 dicembre 1996**,** *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* (testo consolidato con il dl. 28 dicembre 2001, n. 467); legge abrogata ai sensi dell'articolo 183, comma 1, lettera a), del Codice in materia dei dati personali.

Codice della *Privacy*, la Corte di Cassazione accoglie il ricorso proposto avverso la suddetta sentenza affermando che la norma non sanziona le semplici violazioni formali e le irregolarità procedimentali né le inosservanze che producano un *vulnus* minimo all'identità personale del soggetto ed alla sua *privacy* che non determinano alcun danno patrimoniale apprezzabile. Dunque in questa sentenza la Corte esclude la sussistenza del nocumento ma si sofferma sulla natura giuridica da attribuire a questa locuzione, oggetto di un annoso dibattito dottrinale: parte della dottrina, infatti, definiva il nocumento un elemento costitutivo della fattispecie, altri lo prospettano invece come condizione obiettiva di punibilità. La Corte di Cassazione propende per quest'ultima ricostruzione considerando il nocumento quel *quid pluris* che il legislatore richiede perché il reato, seppur completo di tutti i suoi elementi, diventi punibile. Non sarebbe logico infatti considerare il nocumento elemento costitutivo visto che il danno è già individuato come oggetto del dolo specifico. Questa conclusione è a chiare lettere ribadita anche in una più recente pronuncia[387] della Suprema Corte.

Il *punctum dolens* della sentenza è rappresentato dalla condanna dell'ISP per illecito trattamento dei dati, argomentazione costruita su «un'interpretazione doppiamente analogica»[388] dell'art 167 d.lgs. n. 196/2003.

Escluso l'obbligo di filtrare preventivamente i contenuti immessi in rete, il giudice monocratico afferma che sull'ISP grava un obbligo di informativa nei confronti dell'*uploader* scaturente dall'art. 13 d. lgs. 196/2007. In altre parole, nel momento in cui viene effettuato l'*upload* di un video, l'ISP sarebbe tenuto a segnalare, tramite un *alert* all'*uploader*, l'esistenza e i contenuti della legge sulla *privacy* ed in particolar modo il fatto che il trattamento dei dati personali è subordinato al consenso dei soggetti interessati. Tuttavia tra le comunicazioni obbligatorie prescritte dall'art. 13 d.lgs. citato non figura quella prospettata dal giudice di prime cure.

Analizzando poi la struttura dell'art. 167 d.lgs. 196/2003, emerge il ricorso alla tecnica dei rinvii plurimi ad altre norme attraverso i quali si definiscono i comportamenti incriminati (si rinvia agli artt. 18, 23, 123 etc.). Si tratta di uno strumento che viene spesso utilizzato nel Codice della *Privacy* che suscita non lievi perplessità: la tecnica del rinvio o addirittura del doppio rinvio (ad esempio a provvedimenti del garante o dell'autorità amministrativa) può rendere il precetto difficilmente intellegibile, con l'evidente rischio di violazione dei principi di legalità e tassatività della norma penale.

La Corte d'Appello precisa infatti che «la norma di cui all'art. 167 appare caratterizzata dalla tipicizzazione della condotta penalmente rilevante in quanto richiede esplicitamente che l'autore del reato abbia agito non rispettando le disposizioni indicate» e tra le disposizioni richiamate non compare l'art. 13. Si è scritto che l'*iter* seguito dal giudice monocratico, sotto l'egida del "buon senso", abbia trasformato la condotta penalmente rilevante ai sensi dell'art. 167 del Codice da "trattamento di dati personali senza consenso" in "trattamento di dati personali senza informativa", condotta, quest'ultima, che però è prevista come illecito amministrativo»[389].

3.2.2. Il presupposto elemento oggettivo

L'analisi dell'elemento soggettivo del reato richiede una preventiva specificazione fondata sulle argomentazioni con le quali la Corte d'Appello dimostra della carenza dell'elemento oggettivo.

Uno degli aspetti più complessi emerso durante il processo di primo grado è la qualificazione da attribuire a *Google Video*: se si tratti in particolare di un *content provider* o di un *host provider*. Anzitutto bisogna precisare che per *provider* si intende «un intermediario che stabilisce un collegamento tra chi intende comunicare un'informazione e i destinatari della stessa»[390].

---

387 Cass. pen., sez. III, sentenza 15 giugno 2012, n. 23798.

388 In questo senso A. INGRASSIA, *La decisione d'Appello nel caso* Google vs ViviDown, in *CM*, 7, 2013, pp. 771-772.

389 Trib. Milano, 12 aprile 2010, n. 1972, Est. Magi, in *CM*, 2010, pp. 960 e ss., con nota di L. BEDUSCHI, *Caso* Google: *libertà d'espressione in* internet *e tutela penale dell'onore e della riservatezza*.

390 Per le definizioni dei *providers* si consulti *http://brunosaetta.it/responsabilita-provider/la-responsabilita-dei-provider.html*.

I servizi offerti dai *providers* sono molteplici e dunque si possono distinguere varie tipologie: anzitutto l'*access provider* che fornisce il servizio di accesso ad *internet* attraverso *modem* o connessioni dedicate; il *content provider* ovvero sia il fornitore di contenuti; il *network provider*, fornitore di accesso alla rete attraverso la dorsale *internet*; l'*host provider* che fornisce ospitalità a siti *internet*; il *service provider* che fornisce servizi per *internet*, come accessi o telefonia mobile; ed infine il *cache provider* che immagazzina dati provenienti dall'esterno in un'area di allocazione temporanea, la *cache*, al fine di accelerare la navigazione in rete.

La Corte d'Appello riconosce la natura di *host provider* cd. attivo a *Google Video*, poiché esso svolge un'attività «non neutra rispetto all'organizzazione ed alla gestione dei contenuti degli utenti, caratterizzata anche dalla possibilità di un finanziamento economico attraverso l'inserimento di inserzioni». La pubblica accusa faceva discendere dalla suddetta qualificazione l'esclusione delle limitazioni di responsabilità prevista dal d.lgs. 70/2003 che recepisce la direttiva CE sul commercio elettronico 2000/31[391]. È la sezione quarta della direttiva che si occupa della delicata questione della responsabilità dei *providers*, graduando gli obblighi cui sono tenuti a seconda che siano riconducibili in una delle seguenti categorie[392]: all'art. 12 il *mere conduit* ovvero il semplice trasporto; l'art. 13 si riferisce al *caching*, intendendosi per tale la memorizzazione temporanea; ed infine l'art. 14 che prevede l'*hosting*, cioè la memorizzazione di informazioni fornite dall'utente su un *server* di proprietà del fornitore.

Sia che si riconduca il servizio offerto da *Google Video* alla tipologia del *mere conduit* o dell'*hosting* non vi è dubbio che le condizioni di esclusione della responsabilità possano trovare applicazione: il *provider* infatti non ha né modificato le informazioni né era al corrente del contenuto illecito delle stesse.

Per completezza, è opportuno analizzare anche l'art. 15 della direttiva, che consta di due commi.

---

391 Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 *relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»)* pubblicata in *GUCE* L 178, 17 luglio 2000, p. 1.

392 Anche in questo caso, si riporta il testo degli artt. citati: Articolo 12 - Semplice trasporto ("mere conduit"): «1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione, il prestatore non sia responsabile delle informazioni trasmesse a condizione che egli: a) non dia origine alla trasmissione; b) non selezioni il destinatario della trasmissione; e c) non selezioni né modifichi le informazioni trasmesse. 2. Le attività di trasmissione e di fornitura di accesso di cui al paragrafo 1 includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo. 3. Il presente articolo lascia impregiudicata la possibilità, secondo gli ordinamenti degli Stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine ad una violazione.». Articolo 13 - Memorizzazione temporanea detta "caching": «1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che egli: a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore, d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni, e e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso. 2. Il presente articolo lascia impregiudicata la possibilità, secondo gli ordinamenti degli Stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine ad una violazione.». Articolo 14 – "Hosting": «1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. 2. Il paragrafo 1 non si applica se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore. 3. Il presente articolo lascia impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca nonché la possibilità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime.».

Al *provider* non è imposto alcun obbligo di sorveglianza né è prescritto un comportamento attivo finalizzato alla ricerca di contenuti dai quali si possano desumere attività illecite. Questa norma è dunque un'ulteriore conferma della impossibilità di configurare in capo al *provider* una forma di responsabilità omissiva *ex* art. 40 cp per concorso nel reato altrui. Tuttavia il secondo comma prevede che: «Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati». Sul *provider* grava dunque un obbligo di comunicazione e collaborazione con le autorità più che un obbligo di impedimento e controllo: in questo modo si tenta di raggiungere un equilibrio tra l'esigenza di celerità che caratterizza la fruizione di questo tipo di servizi e la necessità di tutelare il destinatario degli stessi.

3.2.3. Il requisito del dolo specifico

Si può così pervenire ad affrontare l'ultimo profilo analizzato dai giudici della Corte d'Appello di Milano, quello che concerne l'elemento soggettivo del reato. Tra i presupposti che devono realizzarsi contestualmente perché si configuri il reato descritto dall'art. 167 d.lgs. 196/2003, si richiede, infatti, anche il dolo specifico dell'agente: una precipua finalità perseguita dall'agente.

Due sono le argomentazioni addotte dalla Corte per dimostrare la mancanza, nel caso di specie, dell'elemento soggettivo del reato. Anzitutto la Corte non condivide l'assimilazione operata dal giudice di primo grado tra dolo specifico e «il fine di profitto costituito dalla palese vocazione economica dell'azienda»: non vi è dubbio infatti, che l'attività dell'azienda di *Mountain View* sia lecita. Gli imputati non hanno dunque ricevuto alcun vantaggio diretto dall'immissione del video: il servizio *Google Video* è gratuito e al video caricato sulla piattaforma non era stato specificatamente associato alcun *link* pubblicitario.

In secondo luogo gli imputati non erano «preventivamente a conoscenza del contenuto del filmato e del dato non lecitamente trattato».

Non pare possibile, infine, ritenere compatibili l'elemento psicologico individuato in capo agli imputati nella forma del dolo eventuale per avere «serbato una voluta disattenzione nelle politiche societarie relative al trattamento della privacy»[393] o il dolo specifico richiesto dall'art. 167 in termini di «partecipazione psichica intenzionale e diretta del soggetto al raggiungimento di un profitto».

4. La responsabilità degli ISP in precedenti casi giurisprudenziali

In occasione di un convegno organizzato dall'Università degli studi di Roma Tre, il giudice Magi, estensore della sentenza di primo grado, rispondeva ad un'intervista affermando: «Il problema di queste norme è che sono poco frequentate: se si cerca negli archivi e nelle banche dati non si trova niente. A livello giuridico questa è stata una foresta da disboscare col machete, nella quale non c'erano strade».[394]

Effettivamente, il caso *Google vs Vividown* si presenta come un *unicum* nel panorama giuridico internazionale; tuttavia prima di giungere alle conclusioni, si ritiene opportuno soffermarsi su alcuni casi giurisprudenziali che si sono occupati della complessa tematica della responsabilità degli IPS seppur in termini (e con eco mediatica) diversi da quelli della sentenza qui analizzata.

---

393 In primo grado l'Accusa perveniva alla conclusione che il servizio era stato volutamente lanciato senza che fosse stato messo a punto un efficace sistema di controlli perché potesse sfondare sul mercato. Successivamente, a fronte del successo che il servizio riscuoteva, si definiva un sistema di controlli che permetteva agli utenti di segnalare i contenuti inappropriati dei video caricati per provvedere eventualmente alla rimozione degli stessi.

394 Per il testo integrale dell'intervista resa dal giudice Magi: *http://www.blogstudiolegalefinocchiaro.it/privacy-e-protezione-dei-dati-personali/intervista-a-oscar-magi-giudice-del-caso-googlevividown/*.

La vicenda *Fapav-Telecom*[395] trae origine da un'indagine disposta dalla Federazione Anti Pirateria Audiovisiva (appunto Fapav) dalla quale emerge l'elevatissimo numero di visite, in gran parte effettuate da clienti Telecom Italia s.p.a. (d'ora in poi Telecom), totalizzate dai siti di condivisione illegale di audiovisivi. A questo risultato si è giunti monitorando il comportamento di ignari utenti e per questo accanto a Telecom si schiera il Garante della *privacy*. Anche questo caso, come la sentenza d'Appello del caso *Google vs. Vividown*, si conclude con l'affermazione della non responsabilità dell'ISP che non è dunque perseguibile per il *download* illegale di contenuti da parte degli utenti e non è tenuto né ad inibire l'accesso ai siti di *sharing* illegale né a fornire a terzi i dati (in particolare gli indirizzi IP) degli utenti.

Nella sentenza si richiama tuttavia l'IPS alla collaborazione con le autorità, in linea con l'art. 15 della direttiva sul commercio elettronico, per scongiurare il dilagante fenomeno della violazione del diritto d'autore.

Un secondo caso riguarda la responsabilità del sito svedese "The pirate bay" per favoreggiamento della violazione del diritto d'autore. Il GIP di Bergamo, investito del caso, ha ordinato agli ISP di bloccare l'accesso al sito. Il Tribunale di Bergamo, tuttavia ha sospeso il provvedimento giudicando il sequestro illegittimo: il provvedimento del GIP si risolve, a parere del Tribunale del riesame, in una inibitoria atipica poiché il sequestro avrebbe una natura non reale (finalizzata cioè ad apporre un vincolo di indisponibilità alla *res*), ma obbligatoria: esso è infatti indirizzato a soggetti indeterminati, gli ISP, che devono impedire l'accesso al sito. La Corte di Cassazione ha annullato l'ordinanza di dissequestro[396]: in capo ai *provider* grava «un obbligo generale di sorveglianza sui flussi telematici in transito sui propri sistemi». L'ISP deve dunque predisporre dei filtri per impedire l'accesso al sito ostacolando quindi la circolazione illegale di contenuti coperti da diritto d'autore.

5. Alcune poche considerazioni conclusive

Nei due casi ai quali ho fatto riferimento il tema della responsabilità dell'ISP è subordinato e per certi aspetti oscurato dal problema della tutela della proprietà intellettuale[397]. La carenza di questo profilo nel caso *Google vs Vividown* ha costretto la giurisprudenza a confrontarsi per la prima volta in maniera non mediata con il problema del ruolo da attribuire all'ISP nel caso di commissione di illeciti su o per mezzo di *internet*.

La sentenza d'appello, confermata dalla recentissima pronuncia della Corte di Cassazione[398], sembra aver accolto le critiche sollevate dalla dottrina[399] contro la sentenza di primo grado e si presenta più conforme ai dettami generali del diritto penale, al contesto normativo sovranazionale e alle norme contenute nel Codice della *Privacy*. L'impossibilità di riscontrare nel diritto vigente una posizione di garanzia in capo all'ISP è un dato di fatto che prescinde dalle valutazioni circa l'opportunità di colmare questo *deficit* normativo.

È evidente che la sentenza di primo grado ha scoperchiato il "vaso di Pandora" del "governo di internet": il caso ha drammaticamente messo in luce la complessità della materia e dovere del giurista è, prima ancora di chiedersi se e come colmare il *deficit* normativo, interrogarsi su come il diritto possa tenere il passo rispetto all'ineluttabile progresso tecnologico e agli influssi di esso sulla comunicazione.

E ancora come si possa giungere, nell'epoca in cui comunicazione significa anzitutto interattività, ad un soddisfacente bilanciamento di valori primari.

---

395 Tribunale di Roma, sez. specializzata per la proprietà industriale ed intellettuale, ordinanza 14 aprile 2010.

396 Cass. Pen., sez. III, 23 dicembre 2009, n. 49437.

397 Motivo per cui non sono stati riferiti casi molto interessanti che hanno visto coinvolto il *leader* delle aste *online* Ebay, ad esempio la sentenza della Corte di giustizia del 12 luglio 2011, in causa C-324/09.

398 Cass. Pen., sez. III, 3 febbraio 2014 n. 5107.

399 La consapevolezza del difficile compito del Tribunale di Milano precede i rilievi sulle soluzioni da questi adottate in R. LOTIERZO, *Il caso Google – Vividown quale emblema del difficile rapporto con il Codice della privacy*, in *CP*, 2010, pp. 1288 ss.

Bisogna tener presente infatti che la commissione di illeciti nel cyberspazio consente all'agente di celarsi dietro il più completo anonimato: come la dottrina[400] più attenta ha sottolineato, l'indirizzo IP (*Internet protocol address*) consente di identificare il dispositivo ma non l'agente; e proprio queste difficoltà probatorie sono alla base dei tentativi di costruire una forma di responsabilità automatica degli ISP, fornitori a vario titolo dello "spazio virtuale di commissione dell'illecito"[401].

L'esigenza di depurare da contenuti illeciti la "sconfinata prateria di internet dove tutto è permesso e niente può essere vietato" non può tradursi in un obbligo di controllo preventivo in capo agli ISP che, alla luce del diritto vigente, non potrebbe non presentare le sembianze di una responsabilità oggettiva.

D'altra parte una responsabilità siffatta potrebbe rivelarsi un pericoloso strumento di limitazione della libertà di manifestazione del pensiero[402], in un contesto, quello di *internet*, che ha dato prova, specie negli ultimi anni, di sconfinate opportunità di partecipazione e interazione.

---

400 G. CORRIAS LUCENTE, Ma *i* network providers*, i* service providers *e gli* access providers *rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che loro gestiscono?*, cit., p. 2524.

401 V. SPAGNOLETTI, *La responsabilità del* provider *per i contenuti illeciti di* internet, in *Gmer*, 2004, pp. 1992 ss.

402 Evidenziano il rischio che i *providers,* pur di evitare di essere perseguiti penalmente possano procedere ad un'operazione di censura generalizzata, E. ARPA, O.POLLICINO, *Modeling the Liability etc.*, cit. p. 59.

VI. I *PERSONAL NAME RECORDS* TRA ISTANZE DI SICUREZZA GLOBALE E TUTELA DEI DATI PERSONALI

di Giovanni Antonino Cannetti

«Quando la sicurezza e l'uguaglianza sono in conflitto, non bisogna esitare un momento: è l'uguaglianza che deve cedere. L'istituto dell'eguaglianza non è che una chimera: tutto ciò che si può fare è diminuire l'eguaglianza.»
JEREMY BENTHAM

1. Come tutto ebbe inizio

Nel lontano 1996 la compagnia *Northwest Airlines* introdusse per la prima volta sui propri voli un Sistema Computerizzato per Supportare il Monitoraggio del Passeggero (*Computer Assisted Passenger Pre-Screening System,* CAPPS).

Il CAPPS è stato sviluppato attraverso una sovvenzione fornita dalla *Federal Aviation Administration* (FAA) proprio alla *Northwest Airlines*, con un sistema prototipo testato nel 1996.

Esso era conformato in modo da confrontare i dati dei passeggeri (PNR) presenti nel Sistema di Prenotazione Computerizzata (cd. *Computer Reservation System,* CRS) della compagnia aerea con quelli inseriti in una banca dati contenente una *no-fly list*, una lista di persone considerate potenzialmente pericolose, inizialmente gestita dall'FBI, con la finalità di garantire la sicurezza del volo.

Detto sistema, entrato in funzione a pieno regime nel 1999, aveva come scopo quello di elaborare i dati estrapolati dai *passenger name record* delle compagnie aeree al fine di individuare automaticamente i soggetti che potevano presentare rischi per la sicurezza e sottoporli, così, a procedure di controllo più rigorose.

I *passenger name record* o PNR consistono in un insieme di informazioni che vengono raccolte dalle compagnie in sede di prenotazione di un biglietto aereo; tra le informazioni raccolte rientrano anche quei dati non strettamente necessari alla transazione, ma il cui trattamento è comunque finalizzato a fornire un migliore servizio alla clientela.

Analogamente, i CRS conservano una cronologia relativa a ciascun passeggero che comprende tutti i dati PNR raccolti dalle compagnie aeree, le informazioni sui viaggiatori abituali e la fonte di provenienza di qualsiasi prenotazione o richiesta speciale, incluse le informazioni di contatto degli agenti di viaggio.

Nello specifico il CAPPS serviva, appunto, ad elaborare i dati estrapolabili dai PNR attraverso la loro comparazione con le informazioni contenute in liste governative di nomi di persone sospettate di terrorismo. Inoltre, tale sistema effettuava l'analisi delle caratteristiche comportamentali dei passeggeri.

Ciò serviva, in particolare, ad evidenziare eventuali casi di comportamento di viaggio sospetto a loro volta deducibili da elementi quali modalità di pagamento anomale o durata singolare del viaggio.

Il CAPPS suddivideva quindi i passeggeri in due gruppi, separando quelli per i quali era sufficiente un controllo di tipo generale da quelli che, invece, necessitavano di uno *screening* più

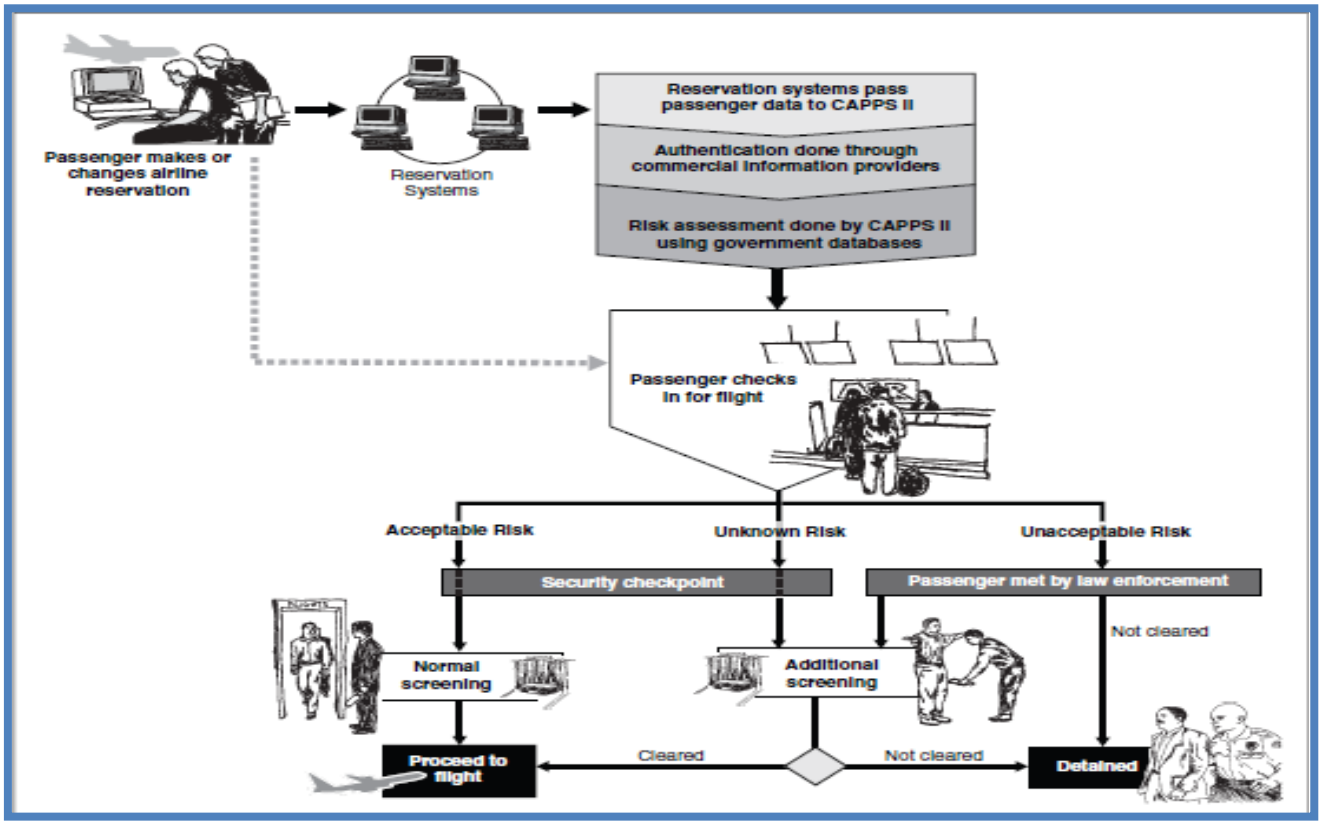
approfondito o nei cui confronti vigeva un divieto assoluto di imbarco. Il tutto era finalizzato ad aumentare la sicurezza aeroportuale ed evitare eccessivi ritardi per i passeggeri[403].

Nel 1997, altri grandi vettori iniziarono a lavorare su sistemi di *screening* e nel 1998 la maggior parte delle compagnie aeree statunitensi aveva volontariamente implementato CAPPS, mentre i pochi ritardatari si stavano muovendo verso l'attuazione.

Inoltre, durante questo periodo, la Commissione sulla sicurezza aerea della Casa Bianca (a volte indicata come la "Commissione Gore") pubblicò il proprio rapporto finale nel febbraio 1997[404].

A causa delle critiche da parte dell'opinione pubblica, in ragione dei potenziali rischi per i diritti fondamentali e per la *privacy*, un anno dopo la sua istituzione, il CAPPS venne limitato al solo controllo bagagli dei passeggeri.

Lo schema qui di seguito descrive i passaggi fondamentali del sistema CAPPS II[405]



1.1. Di necessità virtù; ovvero la reazione USA alle nuove istanze di sicurezza per il traffico aereo

Gli attentati dell'11 settembre 2001 sono stati il *casus belli* per porre in essere interventi legislativi incisivi, rivolti a rafforzare la sicurezza nazionale statunitense; esemplificazione di tale linea politica è l'approvazione, il 25 ottobre del 2001, poco più di un mese dopo l'attentato, dello *Uniting and Strengthening America by Providing Appropriate Tool Required to Intercept and Obstruct Terrorism Act of 2001*,

[403] L. FAVERO, *La dimensione esterna della tutela dei dati personali nel diritto dell'UE* – Tesi di Dottorato. *Alma Mater Studiorum* – Università di Bologna, 2013.
[404] *White House Comm'n on Aviation Safety and Security, Final Report to President Clinton*, Feb. 12, 1997.
[405] Il sistema CAPPS II è stato introdotto dopo gli attentati delle *Twin Towers* e contiene alcune innovazioni rispetto al CAPPS. Per i dettagli si veda il *Report to Congressional Committees (2004) GAO* reperibile all'indirizzo *http://www.gao.gov/new.items/d04385.pdf* e *sub.* nota 5.

meglio noto a tutti come *USA Patriot Act*, sulla cui incidenza ed importanza non è però possibile, in questa sede, soffermarsi[406].

Il 19 novembre 2001 il Congresso statunitense approvò inoltre una nuova Legge sull'Aviazione e la Sicurezza dei Trasporti (*Aviation and Transportation Security Act*, in prosieguo, ATSA).

L'ATSA emendò la sezione 44909 del titolo 49 dello *United States Code*, aggiungendo un nuovo paragrafo intitolato: "Flights in foreign air trasportation to the United States".

L'attuazione della nuova normativa ha comportato la federalizzazione della sicurezza aeroportuale, a sua volta ottenuta mediante l'istituzione della *Transportation Security Administration* (in prosieguo TSA) presso il *Department of Homeland Security* (in prosieguo DHS).

Tra gli strumenti introdotti a seguito della nascita della TSA, è il caso di accennare al sistema CAPPS II, proposto il 1° agosto 2003, per combattere il terrorismo e prevenire altri dirottamenti ai danni di compagnie aeree statunitensi. Il CAPPS II permetteva alla TSA di accedere alle informazioni personali relative ai passeggeri delle compagnie aeree e di "etichettarli" in base al grado di minaccia che costituiscono apparentemente alla sicurezza del volo.

Secondo il programma, tutti i passeggeri aerei erano tenuti a fornire molteplici informazioni, tra cui primariamente il proprio nome, cognome, indirizzo, numero telefonico di casa e data di nascita.

Se il precedente sistema utilizzava i dati PNR al solo scopo di selezionare i passeggeri onde sottoporre il loro bagaglio ad uno *screening* più approfondito, il CAPPS II avrebbe utilizzato i PNR anche al fine di individuare i soggetti da sottoporre a interrogatorio o perquisizione[407].

Nel 2004, tuttavia, anche il sistema CAPPS II venne abbandonato in ragione delle critiche da parte dell'opinione pubblica e delle forza politiche di opposizione[408].

Attualmente, dunque, ai sensi dell'*Aviation and Trasportation Security Act*, le compagnie aeree che, viaggiano verso o dagli Stati Uniti o che vi transitano sono tenute a fornire alle autorità doganali americane (*Customs and Border Protection Administration,* CBP), prima della partenza del volo: il manifesto dei passeggeri e dell'equipaggio, vale a dire le informazioni relative alle compagnie, ai voli, all'identità e all'itinerario di viaggio di tutti i passeggeri nonché i dati dei PNR.

2. Nemici comuni, accordi comuni. I Primi negoziati USA–UE

La nuova normativa americana poneva di fronte alle compagnie aeree mondiali un inequivocabile *aut-aut*: o iniziavano a fornire i PNR alla CBP oppure le autorità statunitensi minacciavano di privarle dei loro diritti di atterraggio nel territorio USA.

E' superfluo specificare come la maggior parte delle compagnie ottemperarono quasi subito al nuovo dettato normativo.

Anche le compagnie aeree europee, ovviamente, desiderose di evitare le multe e di conservare remunerativi privilegi di atterraggio, si erano venute a trovare tra due fuochi: quello della nuova normativa statunitense, la quale imponeva il trasferimento dei dati alle autorità doganali statunitensi, e quello della legislazione degli Stati membri dell'Unione europea in materia di protezione dei dati personali, che invece lo vietava.

Quest'ultima legislazione, di derivazione comunitaria, trova la propria genesi nella direttiva 95/46/CE[409] in materia di protezione dei dati personali, la quale vieta il trasferimento di essi verso Paesi terzi qualora questi ultimi non garantiscano un livello adeguato di protezione. Il sistema della direttiva è stato definito di *mixed administration*[410] e attribuisce un ruolo centrale alle autorità garanti nazionali.

---

406 L.T. LEE, *The USA patriot Act and telecommunications: privacy under attack*, in *RC&TLJ*, vol. 29, n. 2, June, 2003.

407 V. ALBERTO, D. BOGATZ, *Computer Assisted Passenger Prescreening System: National security V. civil liberties*, Maxwell School of Syracuse University, in *http://www.maxwell.syr.edu/uploadedFiles/campbell/events/AlbertoBogatz.pdf*.

408 J. FISHER, *What price does society have to pay for security? A look at the aviation watch list,* in *WillLR*, 2008.

409 Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla Libera Circolazione dei Dati*, in *GUCE* L-281, 23 novembre 1995, p. 31.

410 F. BIGNAMI, *Mixed Administration in the European Data Protection Directive: The Regulation of International Data Transfers*, in *RTDP*, 2004, pp. 31-57.

In particolare, la direttiva si presenta come una "evoluzione" della Convenzione del Consiglio d'Europa del 1981, la quale presentava come principale elemento critico la discrezionalità, attribuita agli Stati aderenti, nel decidere quali trasferimenti potevano reputarsi legittimi.

La Commissione europea, pur riconoscendo la legittimità degli interessi di sicurezza in gioco, informava le autorità statunitensi del fatto che le nuove disposizioni in materia di trasferimento dei dati PNR rischiavano di entrare in contrasto con la legislazione comunitaria e con quella degli Stati membri in materia di tutela dei dati, nonché con talune disposizioni del regolamento (CEE) del Consiglio 24 luglio 1989, n. 2299.

Gli elementi principali della direttiva sono invece sintetizzabili anzitutto nel principio della libera circolazione dei dati personali all'interno del mercato comune europeo. A questo si aggiunge lo scopo del mantenimento del sistema preventivo di accertamento del livello di protezione dei dati personali solo per i Paesi *extra*-comunitari; infine si afferma la competenza della Comunità nel valutare l'adeguatezza della protezione dei dati personali nei Paesi esterni all'Unione europea.

In particolare, in base all'articolo 25 della direttiva 95/46, entrata in vigore il 13 dicembre 1995 e pubblicata in GUCE L 281 del 23 novembre 1995, qualora una singola autorità garante nazionale ritenga che un trasferimento di dati all'esterno dello spazio comunitario non sia conforme ai principi della direttiva, può interromperlo, ma è tenuto ad informare di ciò la Commissione. A questo punto il caso deve essere dibattuto all'interno del Comitato dei rappresentanti dei Paesi membri, introdotto dall'articolo 31 della direttiva[411]. Quest'ultimo potrà decidere di fermare il trasferimento dei dati personali a partire da tutti i Paesi membri dell'Unione europea, oppure incaricare la Commissione di intraprendere negoziazioni con il Paese terzo per raggiungere una soluzione mediata.

Se lo Stato *extra*-comunitario s'impegna a garantire un livello di tutela adeguato ai dati personali dei cittadini europei, l'esecutivo di Bruxelles adotta di conseguenza una decisione di "adequacy finding", riconoscendo che è stata raggiunta la protezione adeguata. La decisione della Commissione europea dovrà successivamente essere approvata dal Comitato, diventando così vincolante per tutti i Garanti nazionali. E' proprio questo l'*iter* affrontato anche con gli USA.

2.1. Il controverso progetto di decisione sull'adeguatezza

Nel febbraio 2003 la Commissione europea e la CBP conclusero finalmente una dichiarazione congiunta (*joint statement*)[412] in base alla quale la Commissione avrebbe autorizzato le compagnie aeree europee, solo provvisoriamente e al fine di superare la condizione di *impasse* giuridico in cui si erano trovate, a trasferire i PNR alla CBP; alla dichiarazione veniva allegato un documento contenente determinati impegni (*undertakings*) assunti dal CBP in vista dell'avvio delle future negoziazioni per la stipula della decisione sull'adeguatezza.

A livello di normativa europea, il compito di pronunciarsi in merito all'adeguatezza del livello di tutela offerto da parte dello Stato *extra*-europeo ai dati personali trasmessi spetta, ai sensi dell'art. 25 della direttiva 95/46, ad un particolare comitato, il "Gruppo di lavoro 29", composto dai rappresentanti delle autorità Garanti nazionali ed investito del compito di fornire pareri non vincolanti alla Commissione.

In una delle prime opinioni consultive[413] il Gruppo di lavoro ha individuato una serie di principi che le legislazioni dei Paesi *extra*-europei dovrebbero rispettare al fine di poter essere considerate

411 Il "Comitato 31" è uno dei comitati che fanno parte della cosiddetta "comitologia" comunitaria. In base all'articolo 202 del TCE, il Consiglio delega alla Commissione l'autorità di adottare decisioni applicative delle legislazioni comunitarie. Tuttavia, gli Stati membri hanno voluto mantenere un certo controllo su tali decisioni, attraverso l'istituzione dei Comitati, che devono approvare a unanimità o a maggioranza qualificata le decisioni della Commissione.

412 *Joint statement* approvato al termine della riunione tenutasi a Bruxelles il 17 e il 18 febbraio 2003 tra rappresentanti della Commissione europea e del CBP.

413 Gruppo di lavoro 29, *First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*, documento di consultazione adottato il 26 giugno 1997, p. 6.

adeguate; questi possono essere sintetizzati nel fatto che la legislazione nazionale preveda sanzioni abbastanza severe per i *controllers* (ad esempio, una Compagnia con sede legale all'estero) che non tutelino i dati, che i *data subjects* (ossia i diretti titolari dei dati) possono far valere i loro diritti in modo rapido ed effettivo, senza dover affrontare costi eccessivi; l'attenzione particolare nel trasferimento di "dati sensibili"[414] attraverso decisioni automatiche individuali (ad esempio quelli trasmessi attraverso *internet* e a finalità di *marketing*) ed infine il divieto di ri-esportazione dei dati, in particolare verso Paesi terzi che non garantiscano un livello di tutela adeguato.

E' bene evidenziare come, a detta del "Gruppo 29", anche i Paesi che non dispongono di un meccanismo di *enforcement* basato su Garanti nazionali possono comunque essere considerati adeguati e trovare un giusto equilibrio tra la necessità di tutelare i diritti dei *data subjects* europei, anche al di fuori dello spazio comunitario, e il permettere il trasferimento dei dati verso Paesi terzi che utilizzano sistemi di *enforcement* diversi da quello comunitario.

A fronte di tali considerazioni, le condizioni poste specificamente dal CBP nel corso dei negoziati apparvero in aperto contrasto con i principi della direttiva 95/46/CE ed il Gruppo 29 non mancò di far valere le proprie osservazioni attraverso un parere emesso il 13 giugno 2003[415].

In particolare, le autorità statunitensi chiedevano l'applicazione del cosiddetto sistema *pull,* in base al quale la CBP otteneva i PNR attraverso l'accesso diretto ai CRS delle compagnie aeree fino a 72 ore prima della partenza del volo. L'altro sistema possibile, quello di tipo *push*, era invece più rispettoso della *privacy* dei cittadini europei poiché i dati sensibili venivano filtrati automaticamente dalle compagnie aeree prima di essere inviati alla CBP.

I dati trasmessi sarebbero stati inoltrati ad una banca dati centralizzata che veniva gestita sia dalla *US Customs and Border Protection* che dalla *US Immigration and Naturalization Service* le quali potevano poi condividere i medesimi dati con altre agenzie federali di *intelligence* nello scopo di "proteggere la sicurezza nazionale" ed identificare agevolmente chi si era macchiato di *serious criminal offences (*gravi crimini penali). In altre parole, tali informazioni potevano essere utilizzate da praticamente tutte le agenzie federali USA e ciò risultava in contrasto con il principio di divieto di trasferimento ulteriore.

Inoltre, la quantità di dati richiesti dalla CBP (inizialmente trentotto) e la durata del trattamento e archiviazione degli stessi (7-8 anni) non rispettavano il principio di proporzionalità né quello della limitazione del tempo di ritenzione dei dati al periodo di sola elaborazione di questi[416].

Infine, il passeggero europeo non godeva di alcun diritto di accesso, rettifica o cancellazione dei suoi dati né di alcun strumento di ricorso giudiziale contro potenziali abusi da parte del CBP.

2.2. A strong political pressure

L'attività di negoziazione, avviata per il raggiungimento di un necessario compromesso, aveva intanto permesso al CBP di incassare un buon vantaggio; attraverso il *joint statement* e le *undertakings*, sostanzialmente, seppur provvisoriamente, il Governo USA otteneva l'accesso richiesto ai dati PNR senza dover fare alcuna concessione in cambio, mentre la Commissione si trovava, al contrario, nella situazione di dover invitare gli Stati membri a disapplicare la normativa di derivazione comunitaria[417], riconoscendo in capo alle autorità doganali degli USA un diritto implicante comunque l'attribuzione di una potestà sovrana straniera sul territorio dell'Unione. Un trattato internazionale diveniva allora

---

414 Secondo l'articolo 8(1) della direttiva 95/46/CE l'elaborazione di dati personali che rilevano l'origine etnica, razziale, le convinzioni politiche o religiose, o le condizioni di salute dell'individuo è vietata. Tali dati sono considerati "sensibili" in quanto possono causare una discriminazione dell'individuo se tali dati vengono a conoscenza di soggetti terzi.

415 *Opinion* 4/2003 *on the Level of Protection ensured in the US for the Transfer of Passengers' Data*, reperibile su *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp78_en.pdf.*

416 Basti pensare, come ha a suo tempo evidenziato anche il Gruppo 29, che l'accordo con l'Australia richiedeva un numero inferiore di dati (18, invece dei 34 richiesti dalla CBP). Inoltre, i dati erano mantenuti nei *database* delle autorità di dogana australiane solo fino all'arrivo a destinazione del volo. Eventualmente, le dogane di questo paese immagazzinano dati su un passeggero solo se quest'ultimo ha commesso un atto illegale o se i dati sono necessari per le esigenze di un'inchiesta riguardante un presunto delitto.

417 Vedi *supra* nota10.

necessario per esprimere il consenso dell'Unione all'esercizio di una potestà sovrana straniera sul proprio territorio.

Nonostante le difficoltà incontrate nel riconciliare posizioni tanto differenti, nel dicembre 2003 la Commissione europea annunciò l'intenzione di voler adottare una decisione di *adequacy finding* nei confronti delle richieste americane[418], accompagnata da un "light international agreement" (accordo internazionale leggero), finalizzato vincolare gli Stati Uniti a rispettare le condizioni di trattamento dei PNR pattuite durante le negoziazioni.

In dottrina è stato osservato come all'adozione di una decisione sull'adeguatezza (la cui natura è già stata precedentemente evidenziata[419]) non aveva mai fatto seguito un accordo internazionale.

Durante i mesi del negoziato, il CBP venne incontro ad alcune richieste della Commissione europea; i dati sensibili che potevano permettere l'identificazione di un passeggero sulla base della sua razza o religione, ad esempio, vennero esclusi dalla lista dei PNR trasmessi alla CBP. Inoltre, i *data subject* avrebbero avuto diritto di rettifica dei loro dati.

Eppure, le concessioni americane restavano comunque insufficienti sotto molti aspetti[420]; tra queste, il numero dei dati raccolti, pur ridotto dalle precedenti 38 voci alle 34, costituiva ancora una quantità di dati esorbitante.

Altri punti su cui i negoziati ebbero una qualche incidenza furono il periodo di trattamento e ritenzione dei dati (portato a 3 anni e sei mesi) e la garanzia del mantenimento della "confidenzialità" delle informazioni trasmesse (ma pur sempre inoltrabili a tutte le altre autorità statunitensi e straniere competenti in materia di terrorismo e crimine organizzato). Infine, il CAPPS continuava a funzionare sulla base di un sistema *pull*, invece di un sistema *push*. Si può sin da ora anticipare come, nel maggio del 2004, la Commissione europea approvò una decisione di *adequacy finding* nei confronti delle richieste della CBP nonostante il parere contrario del comitato che rappresentava le Autorità Garanti nazionali.

L'accordo internazionale fu successivamente ratificato dal Consiglio[421]. Come può immaginarsi, il Governo americano aveva esercitato tutta la sua forza politica per ottenere tale risultato; non a caso, nella conferenza stampa successiva all'approvazione della decisione di adeguatezza, il Commissario Bolkestein fece accenno al fatto che le autorità americane avevano applicato «a strong political pressure» sulla Commissione, al fine di ricevere l'*adequacy finding*, pur specificando di ritenere il risultato dei negoziati, complessivamente, bilanciato[422].

3. La partita nel Parlamento europeo

Come già accennato precedentemente, il Parlamento, nonostante la rilevanza della decisione sull'*adequacy finding*, è l'unica istituzione totalmente esclusa da tale processo decisionale, malgrado la stessa direttiva 95/46/CE sia stata approvata anche dal Parlamento europeo per mezzo della procedura di co-decisione.

A causa di tale condizione deteriore nel livello procedimentale, anche le osservazioni compiute dal Parlamento europeo restarono in quel contesto per lo più prive di incidenza, inasprendo così il conflitto *inter*-istituzionale.

Già poco dopo la conclusione dell'accordo *ad interim,* Stefano Rodotà, Presidente del Gruppo art. 29, inviava una lettera pubblica[423] al Presidente della Commissione su i Diritti e le Libertà dei Cittadini, Giustizia ed Affari Interni del Parlamento europeo (in seguito "LIBE") nella quale criticava

418 Comunicazione dalla Commissione a Consiglio e Parlamento adottata il 16 dicembre 2003; documento COM(2003) 826 final, in *http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/apis-communication/apis_en.pdf*.

419 Vedi nota *sub*. 9.

420 Gruppo di lavoro art. 29: Parere 2/ 2004, adottato il 29 gennaio 2004. Documento n. 2/2004. Il testo del parere è disponibile in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_it.pdf*.

421 Decisione del Consiglio del 17 Maggio 2004. Il testo della Decisione del Consiglio è disponibile in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0496:IT:HTML*.

422 Redazione, *Europe Bows to U.S. on Air Passenger Data. International Herald Tribune*, 18 maggio 2004.

423 Consultabile su *http://www.statewatch.org/news/2003/mar/art29ch.pdf*.

l'accordo per essere stato concluso senza tenere in considerazione il parere 6/2002 reso dal Gruppo di lavoro e senza consultare quest'ultimo.

Nel marzo 2003 il Parlamento europeo adottava dunque una risoluzione[424] con la quale manifestava la propria contrarietà all'accordo *ad interim*. In particolare il Parlamento nutriva dubbi sul fatto che i dati comunicati alle autorità di frontiera USA fossero adeguatamente protetti una volta trasferiti nel *database* americano, posta l'assenza di una decisione della Commissione che constatasse l'adeguatezza del livello di protezione offerto dalla legislazione americana.

Il Parlamento europeo fu inoltre escluso dall'approvazione dell'accordo internazionale "light" stipulato dalla Comunità europea con gli USA nel maggio 2004 come corollario alla decisione di *adequacy finding* della Commissione; infatti, si fece ricorso alla base dell'articolo 300(3) del Trattato della Comunità europea. In base ad esso, i trattati internazionali approvati in settori in cui a livello interno si applichi la procedura di co-decisione prevista dall'articolo 251 del Trattato erano ratificati dal Consiglio su proposta della Commissione. Il Parlamento svolgeva esclusivamente una funzione "consultiva" con parere non vincolante. Tuttavia, il secondo comma dell'articolo 300(2) del Trattato della Comunità europea stabiliva che, nel caso in cui il trattato internazionale emendasse una norma comunitaria precedentemente approvata per mezzo della procedura di co-decisione, il Parlamento doveva fornire il suo assenso (con valore vincolante) alla ratifica del Consiglio.

3.1. La scelta politica della Commissione mette all'angolo il Parlamento

Dunque, secondo il Parlamento europeo, l'accordo internazionale *light* che la Commissione intendeva concludere con gli USA rappresentava una deroga ai principi della direttiva 95/46/CE e necessitava pertanto del parere favorevole dell'istituzione, oltre che dell'approvazione del Consiglio. La scelta della Commissione di optare per una procedura di approvazione dell'accordo internazionale che non coinvolgesse significativamente il Parlamento europeo non fu certo casuale: ovvie ragioni politiche facevano temere che il Parlamento europeo, sotto l'influenza della LIBE, non avrebbe mai approvato un simile trattato internazionale con gli USA per permettere il trasferimento dei PNR. E' per tale ragione che, il 1° marzo 2004, la Commissione sottoponeva al Parlamento il progetto di decisione sull'adeguatezza in virtù dell'art. 25, n. 6, della direttiva, accompagnato dal progetto di impegno del CBP. A strettissimo giro, il 17 marzo 2004 la Commissione trasmetteva al Parlamento, nell'ottica della consultazione di tale organo, come già detto, ai sensi dell'art. 300, n. 3, primo comma CE anche una proposta di decisione del Consiglio avente ad oggetto la conclusione di un accordo con gli Stati Uniti in materia di trasferimento dei dati PNR.

Infine, con lettera datata 25 marzo 2004 il Consiglio, riferendosi alla procedura d'urgenza e giustificandola con l'esigenza di immediata risposta al fenomeno terroristico e di abbattimento della condizione di incertezza in cui versavano i vettori aerei, ha chiesto al Parlamento di esprimere un parere su tale proposta entro il 22 aprile 2004.

Il 31 marzo 2004, in attuazione dell'art. 8 della decisione del Consiglio 28 giugno 1999, 1999/468/CE, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione (GU L 184, p. 23), il Parlamento ha adottato una risoluzione in cui esprimeva un certo numero di riserve di carattere giuridico sulla proposta presentatagli. In tale risoluzione ha considerato, in particolare, che il progetto di decisione sull'adeguatezza eccedeva le competenze conferite alla Commissione dall'art. 25 della direttiva 95/46, ha invocato la conclusione di un accordo internazionale appropriato che rispettasse i diritti fondamentali su un certo numero di punti specificati nella risoluzione stessa e ha chiesto alla Commissione di sottoporgli un nuovo progetto di decisione.

---

424 *European Parliament Resolution on transfer of personal data by airlines in the case of transatlantic Flights,* consultabile su *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P5-TA-2003-0097+0+DOC+XML+V0//EN.*

3.2. La reazione della LIBE: la "carta" CGUE

A causa del rifiuto della Commissione di coinvolgere il Parlamento nella negoziazione di un vero trattato internazionale, la Commissione LIBE propose inoltre al plenario del Parlamento di riservarsi di portare il caso davanti alla Corte di giustizia al fine di verificare la legalità dell'accordo internazionale progettato ed, in particolare, di verificare la compatibilità di tale accordo con la protezione dei diritti fondamentali dei cittadini europei.

La proposta della LIBE di ricorrere al parere della Corte di giustizia fu approvata a stretta maggioranza dalla seduta plenaria del Parlamento del 21 aprile 2004[425]. In quella stessa data, su richiesta del suo Presidente, il Parlamento ha approvato una raccomandazione della commissione giuridica e del mercato interno volta ad ottenere, ai sensi dell'art. 300, n. 6, CE, un parere della Corte sulla compatibilità dell'accordo previsto con le disposizioni del Trattato. Il Parlamento ha inoltre deciso in pari data di rinviare a tale commissione il rapporto sulla proposta di decisione del Consiglio, respingendo così implicitamente, in questa fase, la domanda di esame urgente della detta proposta presentata dal Consiglio il 25 marzo.

Senza considerare quanto avvenuto nella seduta parlamentare del 21 aprile, il 14 maggio 2004 la Commissione adottò, la propria decisione di *adequacy* e alcuni giorni dopo, il 17 maggio, il Consiglio adottò la decisione 2004/496/CE, la quale approvava l'accordo di trasferimento dei PNR agli USA.

Poiché la Commissione aveva proceduto alla conclusione dell'accordo senza l'approvazione del Parlamento europeo e senza attendere che la Corte di giustizia si esprimesse sulla questione, il Parlamento ritirava le richieste di parere e presentava due ricorsi alla Corte di giustizia in data 27 luglio 2004.

4. La "resa dei conti" (parte I)

La decisione sull'adeguatezza relativa al livello di protezione dei dati personali contenuti nei *dossier* passeggeri trasferiti all'Ufficio delle Dogane e della Protezione delle Frontiere USA diventava dunque oggetto della causa C-318/04, mentre la causa iscritta al numero C-317/04 concerneva l'annullamento della decisione n. 2004/496/CE in merito alla conclusione dell'accordo.

E' dunque possibile evincere da subito la stretta *inter*-dipendenza tra le due cause; in considerazione di tale condizione, confermata nella fase orale, i procedimenti in esame venivano riuniti ai fini della decisione a norma dell'art. 43 del regolamento di procedura della Corte.

4.1. La causa C-318: Commissione c. Parlamento

La risoluzione della causa C-318 si rivelerà determinante anche per il giudizio di legittimità dell'accordo internazionale con gli Stati Uniti. Preliminarmente, due elementi processuali vanno evidenziati: per la prima volta nella sua storia, il Garante Europeo per la Protezione dei dati, con ordinanza del presidente della Corte 17 marzo 2004, veniva ammesso a sostegno delle conclusioni del Parlamento.

Malgrado ciò, così come per la causa C-317, il Presidente della Corte, con ordinanza del 21 settembre 2004 pubblicata solamente in ottobre, respingeva la richiesta del Parlamento di sottoporre entrambe le controversie alla procedura d'urgenza *ex* art. 62; ciò non deponeva a favore dell'accoglimento dei ricorsi, comportando per di più una probabile attesa della sentenza della Corte con procedura ordinaria di almeno 3 anni, equivalenti al termine di validità fissato per l'accordo[426].

---

425 276 voti a favore; 260 i contrari e 13 astensioni. Redazione, *Parliament Takes Commission to Court over Passenger Data*, *EurActive.com*, 22 aprile, 2004.

426 M. A. LEDIEU, *Accord PNR - Pas d'urgence pour la CJCE,* in *Communication Commerce électronique,* n. 1, Janvier 2005, Alerte 22.

Precedentemente, con ordinanza del presidente della Corte 17 dicembre 2004, era stato ammesso l'intervento del Regno Unito a sostegno delle conclusioni della Commissione.

Sebbene il Parlamento avesse dedotto ben quattro motivi di ricorso, la pronuncia di annullamento da parte della Corte venne determinata solo in funzione della "corretta base legale".

4.2. I motivi di ricorso

L'eccesso di potere, la violazione della Convenzione europea dei diritti fondamentali e della direttiva nelle sue disposizioni a tutela della *privacy*, ed infine il mancato rispetto del principio di proporzionalità, non sono motivi presi in considerazione nella succinta decisione della Corte di giustizia. Di ciò non v'è da stupirsi, in quanto il motivo di ricorso relativo alla presunta adozione *ultra vires* della decisione della Commissione, in contrasto con l'art. 3, n. 2, primo trattino, della direttiva 94/46/CE, relativo all'esclusione delle attività non rientranti nell'ambito di applicazione del diritto comunitario, poteva agevolmente riconoscersi come assorbente tutti gli altri motivi ed appariva inoltre di più facile accertamento.

In particolare, appariva indubbio che il trattamento dei PNR dopo il trasferimento all'autorità americana, di cui alla decisione sulla adeguatezza, è e sarà effettuato per l'esercizio di attività proprie degli Stati come intese ai sensi del punto 43 della sentenza 6 novembre 2003, nel caso *Lindqvist*[427], in cui, da una parte, era stato chiarito il carattere meramente esemplificativo dell'elencazione dell'articolo e, per altro verso, che i trattamenti dei dati esclusi dal campo di applicazione della direttiva erano quelli correlati allo svolgimento di "attività proprie degli Stati o delle autorità statali estranee ai settori di attività dei singoli".

4.3. "Scacco matto" *alla decisione di* adequacy finding

L'argomentazione difensiva di Commissione e Regno Unito, secondo cui il trasferimento dei dati PNR alla *Customs and Border Protection* statunitense doveva intendersi finalizzato a fornire dei servizi di tipo commerciale, ossia un trattamento dati effettuato dai vettori privati interessati all'interno della Comunità e al fine del loro trasferimento a Stati terzi, viene rapidamente ad infrangersi.

Attraverso un rapido esame del 6°, 7°, 8°, 15° considerando, la Corte rilevava che: la decisione sull'adeguatezza della Commissione era basata sulla legge americana del 2001 e i suoi conseguenti regolamenti di attuazione adottati dal CBP, che la legislazione aveva ad oggetto «il rafforzamento della sicurezza, nonché le condizioni di ingresso negli Stati Uniti e di uscita dal paese», e che gli stessi considerando prevedevano il sostegno della Comunità agli Stati Uniti «nella loro lotta contro il terrorismo nei limiti imposti dal diritto comunitario», oltre che l'utilizzo dei dati PNR allo scopo di prevenire e combattere il terrorismo e gli altri gravi reati transnazionali, ivi compresa la criminalità organizzata.

Pur se raccolti inizialmente dalle compagnie aeree nell'ambito di attività di tipo commerciale, pienamente rientranti nel diritto comunitario, ossia la vendita di titoli di viaggio, il trattamento dei dati considerato nella decisione sull'adeguatezza ha come oggetto la pubblica sicurezza e le attività dello Stato in materia di diritto penale.

La Corte di giustizia si conformava dunque alla raccomandazione, contenuta nelle conclusioni un po' più precise rassegnate dall'Avvocato generale Philippe Léger, secondo cui: «La Commissione non dispone, sulla base dell'articolo 25 della direttiva n. 95/46, del potere di adottare una decisione relativa

[427] Sentenza della Corte di giustizia del 6 novembre 2003, causa del procedimento C-101/01, *Bodil Lindqvist*..

al livello di protezione adeguata dei dati personali trasferiti nel quadro ed in virtù di un trattato escluso espressamente dal campo di applicazione della direttiva».

La Corte concludeva, il 30 maggio 2006, che la direttiva 95/46/CE non poteva fondare la competenza della Comunità per la decisione di adeguatezza, la quale doveva pertanto essere annullata.

5. La "resa dei conti" (parte II): un esito scontato

Seppur nella nostra esposizione vengano trattate come momenti separati, le cause C-317 e C-318, è bene ribadirlo, sono cause che la Corte riunisce *ex* art. 43 del regolamento di procedura, in considerazione della loro connessione.

Tale condizione si traduce nel far assumere alla pronunzia di annullamento della *adequacy finding* il valore di elemento quasi "pregiudiziale" per valutare la legittimità della decisione n. 2004/496/CE del Consiglio del 17 maggio 2004.

Non a caso la Corte di giustizia, pur investita dal Parlamento di ben sei motivi a sostegno del proprio ricorso, con una pronuncia che per la sua sinteticità è stata ritenuta una tra le più rapide e condensate di tutta la storia del contenzioso vertente sulla scelta della base giuridica, si limitava a constatare che l'art. 95 CE, letto in combinazione con l'art. 25 della direttiva, non era suscettibile di fondare la competenza della Comunità per concludere l'Accordo[428] e tralasciava invece di analizzare l'adeguatezza del trasferimento dei PNR con i diritti dei soggetti dei dati personali garantiti dalla direttiva 95/46/CE o dalla Convenzione 108 del Consiglio d'Europa.

5.1. Causa C-317: Consiglio c. Parlamento

Dunque, nella causa C-317 vengono ammessi, con ordinanze del presidente della Corte 18 novembre 2004 e 18 gennaio 2005, gli interventi della Commissione e del Regno Unito di Gran Bretagna ed Irlanda del Nord a sostegno delle conclusioni del Consiglio mentre, come già è stato detto, con ordinanza della Corte del 17 marzo 2005 veniva ammesso il Garante europeo della protezione dei dati a sostegno delle conclusioni del Parlamento.

5.2. I motivi di annullamento

Il Parlamento deduce sei motivi di annullamento, relativi alla scelta erronea dell'art. 95 CE come fondamento giuridico della decisione 2004/496 e alla violazione, rispettivamente, dell'art. 300, n. 3, secondo comma, CE, dell'art. 8 della CEDU, del principio di proporzionalità, dell'obbligo di motivazione e del principio di leale cooperazione.

Nel primo motivo veniva affermata l'erroneo ricorso all'art. 95 CE per fondare la competenza della Comunità a concludere l'accordo, in quanto quest'ultimo riguardava il trattamento di dati esclusi dall'ambito di applicazione della direttiva 95/46/CE sulla tutela dei dati personali. In particolare, la decisione non avrebbe avuto, né per oggetto né per contenuto, il miglioramento dell'efficienza del mercato interno attraverso l'eliminazione di ostacoli per la libera prestazione dei servizi, ma la *ratio* sarebbe stata ravvisabile bensì nella volontà di legittimare il trattamento di dati personali così come imposto dalla legislazione statunitense.

Nel secondo e terzo motivo il Parlamento sottolineava come l'accordo implicasse una modifica di una direttiva adottata con la procedura di co-decisione di cui all'art. 251 CE e che, pertanto, si sarebbe

[428] Cfr. punto 68 della sentenza, 30 maggio 2006, cit.

dovuto concludere solo previo parere conforme del Parlamento[429]; inoltre il Parlamento sosteneva che l'accordo era stato concluso in violazione in particolare del diritto alla tutela dei dati personali, e che esso costituiva altresì un'ingerenza ingiustificata nella vita privata, come tale incompatibile con l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

Gli altri motivi sono riassumibili nel fatto che l'accordo prevedesse il trasferimento di una quantità eccessiva di dati dei passeggeri e che tali dati venissero conservati troppo a lungo dalle autorità americane, così violando il principio di proporzionalità. Si asseriva violato anche il principio di leale cooperazione previsto all'art. 10 CE, in quanto il Consiglio aveva, con evidente *nonchalance,* adottato la decisione 2004/496/CE, a dispetto dell'esito della seduta parlamentare del 21 aprile, la quale si era conclusa con voto a maggioranza favorevole all'avvio della procedura di domanda di parere 1/04 dinanzi alla Corte di giustizia[430].

Last but not least, il Parlamento faceva constatare la assoluta mancanza di una motivazione avvallante le caratteristiche tanto anormali dell'atto, in difetto pertanto di un elementare obbligo di motivazione.

5.3. Le tesi difensive di Consiglio e Commissione

Il Consiglio, nel proprio controricorso, sosteneva che l'Accordo avrebbe inteso imporre obblighi uniformi a tutte le compagnie interessate riguardo alla libera circolazione dei dati PNR tra la Comunità e gli Stati Uniti, garantendo altresì condizioni di adeguata tutela delle libertà e dei diritti fondamentali delle persone, tra cui la loro vita privata. In particolare, l'Accordo sarebbe stato diretto a porre rimedio alle distorsioni della concorrenza venute a crearsi tra le compagnie aeree degli Stati membri e fra queste ultime e le compagnie degli Stati terzi, eventualmente derivanti dalle condizioni imposte dagli Stati Uniti. Come affermato dal Consiglio, le condizioni della concorrenza «avrebbero potuto essere falsate per il fatto che solo alcune di asse avrebbero accordato alle autorità statunitensi un accesso alle loro banche dati»[431].

Di conseguenza la direttiva, validamente adottata su fondamento dell'art. 100 A del Trattato, avrebbe contemplato la possibilità di trasferire dati personali verso uno Stato terzo in grado di garantirne un livello adeguato di protezione, anche attraverso l'avvio, in condizioni di necessità, di negoziati finalizzati alla conclusione di un accordo tra la Comunità e tale Paese.

La Commissione evidenziava altri profili: essa sottolineava *in primis* l'esistenza di un «conflitto di leggi», dal punto di vista del diritto internazionale pubblico, tra norme statunitensi e la disciplina comunitaria, con la conseguente necessità di conciliarle; e rilevava come l'art. 95 costituisse «fondamento normativo naturale» della decisione, in quanto l'accordo avrebbe riguardato la dimensione esterna della protezione dei dati personali nel momento del loro trasferimento all'interno della Comunità. Gli artt. 25 e 26 della direttiva avrebbero, dunque, fondato una competenza esclusiva esterna a favore della Comunità. Inoltre, la Commissione sosteneva che il trattamento iniziale di quei dati da parte delle compagnie aeree avesse finalità commerciali. L'uso che ne avrebbero fatto in seguito le autorità statunitensi non li avrebbe sottratti alla sfera di operatività della direttiva.

6. La CGUE trae le proprie conclusioni

Finalmente si giunse a dirimere la controversia. La pronuncia, seppur all'apparenza rivolta a perseguire istanze garantistiche, in realtà ha sollevato più di un profilo problematico, che la dottrina non

[429] Riguardo a questa scelta, giuridicamente dubbia, e al non troppo velato tentativo di affermazione di *intelligencija* da parte della Commissione sul Parlamento, si è detto *supra*, par 4.1.
[430] Vedi *supra* nota n. 417.
[431] Cfr. punto 64 decisione.

ha mancato di evidenziare[432]. Nella sostanza, in relazione alla decisione del Consiglio, che si riferiva ad un tema legato alla pubblica sicurezza, l'articolo 95 CE non costituiva per la Corte una base legale adeguata e, pertanto, la decisione doveva essere anch'essa annullata.

Eppure la decisione in esame, censurando la scelta di un fondamento normativo nell'ambito del primo "pilastro" ai fini dell'annullamento per un atto adottato *ultra vires,* rappresenta un caso unico nell'ambito di una giurisprudenza che, tendenzialmente, ha sempre teso ad affermare la preferibilità della base normativa comunitaria rispetto a quelle radicate nel secondo o terzo "pilastro", come nei casi relativi alle sanzioni penali in tema di illeciti ambientali nel 2005 e 2007[433].

Un altro interessante aspetto da sottolineare è che nella propria sentenza la Corte si è limitata ad annullare l'accordo internazionale e la decisione di *adequacy* sulla base di una inesatta base legale, senza invece analizzare l'adeguatezza del trasferimento dei PNR con i diritti dei soggetti titolari dei dati personali garantiti dalla direttiva 95/46/CE o dalla Convenzione 108 del Consiglio d'Europa[434].

6.1. Decisione e conseguenze a breve termine

Pur annullando la decisione di *adequacy* e del Consiglio, la Corte preservò in via transitoria gli effetti della prima per un periodo di 90 giorni (30 settembre 2006) per permettere alla Commissione di negoziare un nuovo accordo con le autorità americane sulla base di una base giuridica appropriata. Tale decisione è frutto dell'interpretazione dei punti 1, 2 e 7 dell'Accordo tra Unione europea e Stati Uniti; poiché la Comunità europea non poteva addurre il proprio diritto a giustificazione della mancata esecuzione dell'Accordo, questo rimase applicabile per i 90 giorni successivi alla sua denuncia. Visto il collegamento tra l'Accordo e la decisione sull'adeguatezza, quest'ultima deve mantenere i propri effetti lungo tale periodo, fermi i tempi ulteriori necessari per adottare le misure che l'esecuzione della sentenza stessa comporta.

7. L'accordo del 2007

La sentenza della Corte di giustizia non chiarì completamente quale dovesse essere la base legale per il trasferimento dei dati, in quanto il semplice fatto che un'attività non ricadesse nell'ambito di applicazione della direttiva 95/46/CE non implicava necessariamente che tale attività fosse regolata all'interno del terzo pilastro[435]. Ad ogni modo, il successivo accordo sul PNR del 2007 venne approvato da una decisione del Consiglio sulla base del terzo pilastro, articoli 24 e 38 del TUE, senza alcun coinvolgimento del Parlamento europeo[436] né una possibilità di sindacato da parte della Corte di giustizia.

Tale sentenza obbligò inoltre gli USA e l'Unione europea di adottare intanto una misura "provvisoria" che permettesse la continuazione del trasferimento dei dati PNR da parte delle compagnie aeree agli USA, poi concretizzatasi nella conclusione di un accordo temporaneo (*interim*

---

432 V. MICHEL, La *dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration* , note sous l'arrêt su 30 mai 2006, *Parlement européen c. Conseil*, aff. jtes C-317 et 318/04, in *RTDE*, 2006, p. 535.

433 Decisione quadro 2003/80/GAI del Consiglio del 27 gennaio 2003 *relativa alla protezione dell'ambiente nel diritto penale*, in *GUUE* L 29, 5 febbraio 2003, p. 55; e Decisione quadro 2005/667/GAI del Consiglio del 12 luglio 2005 circa l'obbligo di reprimere penalmente alcune condotte pregiudizievoli per l'ambiente, tra cui l'inquinamento provocato dalle navi (in *GUUE* L 255, 30 settembre 2005, p. 164) vennero annullate da CGE 13 settembre 2005, causa C-176/03, *Commissione c. Consiglio* e C-440/05, *Commissione c. Consiglio.*

434 Commento del Commissario alla giustizia Franco Frattini in merito alla decisione della Corte di giustizia sulla vicenda PNR, in *http://www.europalex.kataweb.it/article_view.jsp?idArt=45457&idCat=545*.

435 Cfr. *EDPS opinion on the final report by the EU US High Level Contact Group on Information Sharing and Privacy and Personal Data protection*, par. 22, in *www.edps.europa.eu*.

436 Decisione del Consiglio 2007/551, in *GUUE* L 204 del 4 agosto 2007, p. 16.

agreement) tra UE e USA. L'accordo fu concluso nell'ottobre 2006, firmato il giorno 16 in Lussemburgo e il 19 a Washington[437] e destinato a scadere il 31 luglio 2007.

Quest'ultimo allargò il numero di destinatari dei dati, includendo l'ufficio federale americano per l'immigrazione (*US Immigration and Customs Enforcement Department*), il Dipartimento di Stato e altre entità direttamente legate a quest'ultimo.

E` importante sottolineare inoltre che l'*interim agreement* fu successivamente modificato in ragione di una lettera inviata dal DHS alla Presidenza del Consiglio e alla Commissione europea[438] in cui presentò una sua interpretazione di alcuni punti contenuti nelle *undertakings* del CBP del 2004 e comunicò l'adozione di alcuni nuovi strumenti normativi che avrebbero di fatto modificato il valore delle *undertakings* (condivisione dei PNR con ogni altra agenzia federale per la prevenzione e repressione del terrorismo, controllo sugli usi, tempi, utilizzo dati, livelli di sicurezza e sanzioni contro gli abusi, sistema *push* per acquisizione dei dati senza limiti temporali ecc.)[439]. La Commissione ed il Consiglio hanno prontamente risposto a tale missiva, accettando senza alcuna restrizione le richieste americane.

Nell'accordo del 2007 si possono identificare alcune alterazioni nel contenuto dell'accordo rispetto al precedente *interim agreement* e alla successiva lettera del DHS. Un mese prima della scadenza dell'accordo temporaneo, la Commissione europea e il US DHS re-intrapresero le discussioni volte a concludere l'accordo definitivo, firmato il 23 luglio 2007 a Bruxelles ed il 26 luglio 2007 a Washington con scadenza al luglio 2012.

7.1. I Progressi di tutela e le (ancora) dolenti note

Tentando di sintetizzare il contenuto dell'accordo del 2007, non può negarsi, in accordo con la maggioranza della dottrina[440], che, attraverso l'esclusione della applicazione dei principi sul trattamento dei dati contenuti della direttiva 95/46/CE alla materia del trasferimento dei PNR verso le autorità statunitensi, la Corte abbia finito col creare uno spazio in cui le istituzioni europee, in sede di negoziazione di un nuovo accordo con gli USA, hanno potuto agire sostanzialmente *legibus solutae*, in mancanza di indicazioni circa gli *standard* minimi di tutela da garantire alla luce del diritto comunitario[441].

Va tuttavia riconosciuto alla Corte il merito di aver innalzato all'attenzione delle istituzioni l'evidente vuoto normativo riguardante la tutela dei dati personali nel campo della lotta al terrorismo ed alla criminalità organizzata[442].

Secondo il nuovo accordo, i PNR potevano essere utilizzati per proteggere gli interessi vitali dei titolari dei dati o di altre persone, o in qualsiasi procedimento penale, o quando «così richiesto per legge». Riguardo alla già citata lettera del DHS, tale missiva, allegata all'accordo, prevedeva che il DHS avrebbe comunicato all'Unione europea qualunque nuova legge americana che avrebbe materialmente modificato le condizioni di uso dei PNR elencati nella missiva stessa. Pertanto, gli Stati Uniti erano di fatto nella condizione di modificare unilateralmente i termini dell'accordo sul PNR del 2007. Il DHS poteva inoltre condividere i PNR con tutte le agenzie governative americane che avevano funzioni di "applicazione della legge" (*law enforcement*) e compiti di tutela della pubblica sicurezza, *in primis* dunque la CIA e l'FBI.

---

437 *Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security* (Decisione 2006/729/PESC/GAI) firmato a Washington il 19 ottobre 2006. Il testo dell'accordo è disponibile su: *http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2006_10_accord_US_en.pdf*.

438 *Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States of America, concerning the interpretation of certain provisions of the undertakings issued by DHS on 11 May 2004 in connection with the transfer by air carriers of passenger name record (PNR) data (2006/C 259/01).*

439 L'Accordo *Interim* sul PNR conteneva essenzialmente le stesse clausole del suo predecessore del 2004; tuttavia, è la sua lettura in combinazione con la lettera inviata dal DHS (che è stata ufficialmente allegata alla decisione del Consiglio di adottare l'*Interim Agreement*, e a cui la decisione fa' riferimento nel suo testo) che ha creato le maggiori perplessità.

440 Tra i tanti, si veda M. BOTTA, M. DE AZEVEDO, *La protezione dei dati personali nelle relazioni USA-UE,* in *DII,* 2010*,* pp. 326 e 327.

441 A. TERRASI, *Trasmissione dei dati personali e tutela della Riservatezza: l'accordo tra Unione Europea e Stati Uniti del 2007* in *RDI*, 2008, p. 381; M. SPATTI, *Il trasferimento dei dati relativi al* Passenger Name Record: *gli Accordi dell'Unione europea con Australia e Stati Uniti d'America*, in *DCI,* 2013, p. 683 ss.

442 Vedi *supra* nota 393.

L'accordo del 2007 ha inoltre introdotto la possibilità che tali informazioni fossero trasmesse a Paesi terzi, in seguito alla verifica degli usi che sarebbero stati fatti dei dati da parte dei destinatari e della loro capacità di proteggere tali informazioni, senza che fosse previsto almeno una consultazione preventiva delle autorità europee.

I campi delle informazioni che dovevano essere raccolte furono ridotti a 19 rispetto ai 34 contenuti nei precedenti PNR; riduzione però più teorica che pratica in quanto essa era frutto di una semplice fusione di rubriche di dati già esistenti piuttosto che una vera e propria riduzione del numero di dati richiesti[443].

I dati sarebbero stati mantenuti nella banca dati del DHS per un periodo di 7 anni.

Successivamente, sarebbero stati trasferiti in un'ulteriore banca dati il cui accesso era maggiormente ristretto (dati dormienti) per un periodo di 8 anni. Pertanto, il DHS avrebbe conservato ogni PNR per un periodo totale di 15 anni. Tuttavia, i dati relativi ad un caso specifico sotto inchiesta, erano ritenuti nella banca dati fino al completamento dell'inchiesta o alla sua archiviazione. Tale modifica aveva valore retroattivo, in quanto si applicava anche ai dati raccolti sulla base del primo accordo del 2004.

In considerazione del punto 9 par. 2 per cui «il presente accordo non intende derogare o apportare modifiche alle leggi degli Stati Uniti d'America o dell'Unione europea o dei suoi Stati membri» si soggiunse che esso «non crea né conferisce alcun diritto o beneficio ad altre persone o enti pubblici o privati» e pertanto il Governo americano avrebbe dovuto estendere ai cittadini non americani l'applicazione del FOIA (*Freedom of Information Act*)[444], non menzionato negli accordi precedenti, eliminando così la discriminazione precedentemente esistente.

Tuttavia l'accordo sui PNR del 2007 non prevedeva alcun mezzo pratico per permettere agli interessati di poter esercitare effettivamente i loro diritti di accesso, rettifica e di rimedio giurisdizionale; pertanto, dubitando che una decisione politica e le relative garanzie contenute all'interno della lettera del DHS potessero essere realmente in grado di estendere la tutela di uno strumento normativo a beneficio degli interessati dal trattamento, tali diritti restavano privi di tutela ed eventuali violazioni avrebbero potuto essere fatte valere esclusivamente su di un piano politico, nel momento i cui le competenti autorità comunitarie avessero lamentato il mancato rispetto degli impegni assunti dalle autorità USA e quindi delle norme attributive di diritti ai singoli.

L'accordo ha facilitato, ed è questa una nota finalmente positiva, la transizione da un sistema *pull* di trasferimento dei PNR a un sistema di *push* senza però dettare tempi certi e un meccanismo di controllo per assicurare l'esecuzione dell'implementazione del sistema di trasferimento PNR da parte delle compagnie aeree. Tale mancanza limitò pertanto la rilevanza del nuovo sistema di trasferimento dei dati[445].

8. La risoluzione del Parlamento europeo del 5 maggio 2010

L'entrata in vigore del Trattato di Lisbona ha segnato una svolta in relazione alla protezione del diritto alla *privacy* e dei dati personali, anche grazie alle disposizioni che conferiscono al Parlamento europeo un maggiore potere di incisione nell'ambito della procedura volta alla conclusione degli accordi internazionali, in particolare l' attribuzione di un potere di veto in capo al Parlamento europeo (secondo quanto previsto dall'articolo 218 TFUE) per quanto riguarda gli accordi internazionali rientranti in quei campi in cui si applica la procedura legislativa ordinaria. Tra questi, con la demolizione del sistema a

443 Gruppo di lavoro art. 29, *Parere 5/2007 relativo al nuovo accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) da parte dei vettori aerei al Dipartimento per la Sicurezza interna degli Stati Uniti concluso nel luglio 2007*, p. 10. Disponibile su *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_it.pdf.*

444 Il FOIA, emendato dall'*Electronic Freedom of Information Act* del 1996, regola il diritto di accesso dei cittadini statunitensi ai documenti detenuti dalle autorità federali americane.

445 Vedi *supra,* nota 431.

pilastri operata dal Trattato di Lisbona, figura oggi anche la cooperazione di polizia e giudiziaria in materia penale.

La *privacy* e i dati personali vengono poi espressamente menzionati dagli art. 7 e 8 della Carta dei Diritti Fondamentali dell'Unione europea. Il Trattato di Lisbona, che ha sostituito la Costituzione europea dopo la sua mancata ratifica, fa' riferimento nell'art. 6 del Trattato sull'Unione europea alla Carta dei Diritti Fondamentali, secondo cui «l'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000 adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati». Pertanto, nonostante il testo della Carta non sia stato inserito nel Trattato di Lisbona, quest'ultima è diventata vincolante. Secondo l'art. 51(1) della Carta, quest'ultima garantisce una serie di diritti ai cittadini europei che devono essere rispettati dalle istituzioni europee nello svolgimento della propria attività legislativa. La protezione dei dati personali è dunque garantita da un atto giuridico primario nell'Unione europea.[446]

Il Parlamento europeo, nella risoluzione 5 maggio 2010[447] decideva di rinviare la votazione sulla richiesta di approvazione del rinnovo dell'accordo del 2007 fintantoché non venisse accertata la conformità delle modalità di utilizzo dei dati PNR col diritto dell'Unione, tenuto conto del principio essenziale per cui l'Unione europea è fondata sullo stato di diritto e che pertanto qualsiasi trasferimento di dati personali da parte dell'Unione europea e dei suoi Stati membri verso paesi terzi per finalità di pubblica sicurezza (del paese terzo), al fine di offrire le necessarie garanzie ai cittadini dell'Unione, deve basarsi su accordi internazionali aventi il rango di atti legislativi, deve rispettare le garanzie procedurali e deve ottemperare alla normativa sulla protezione dei dati.

Il Parlamento chiedeva che qualsiasi nuovo strumento legislativo sui PNR fosse preceduto da una valutazione d'impatto sulla *privacy* e da un *test* di proporzionalità al fine di dimostrare l'insufficienza degli strumenti giuridici già esistenti.

Sulla stessa linea si poneva il Gruppo di lavoro art. 29, il quale con i pareri 7/2010 e 10/2011 si esprimeva su due proposte della Commissione, sottolineando come l'esigenza primaria nell'ipotesi di trasferimento dei dati dei passeggeri europei al DHS fosse il rispetto dei principi di necessità e proporzionalità; in particolare, pur essendo la seconda proposta (di direttiva) della Commissione del febbraio 2011 accompagnata da una valutazione d'impatto, il Gruppo di lavoro 29 osservava come, pur nella condivisione della legittimità della lotta contro il terrorismo e la criminalità organizzata, fosse indispensabile perseguire il giusto equilibrio tra la tutela della sicurezza pubblica e le limitazioni del diritto al rispetto della vita privata garantito dall'articolo 8 della CEDU e dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Anche il Garante europeo Peter Hustinx, richiamando la risoluzione del Parlamento del 5 maggio, a conclusione e sintesi del parere del 9 dicembre 2011 in merito alla proposta del Consiglio di un nuovo accordo sull'uso ed il trasferimento dei PNR al DHS americano sottolinea come «necessity and proportionality are key principles without which the fight against terrorism will never be effective»[448].

Il Garante manifestò nell'occasione un evidente disappunto a seguito della disarmante presa di coscienza che l'accordo venne proposto a poche settimane dal termine previsto per l'adozione della proposta di revisione dell'intero tessuto legislativo europeo in tema di *data protection*[449].

Si rivela sintomatico del *bellum intestinum* tra istituzioni europee il fatto che, a pochi giorni di distanza, il Consiglio abbia adottato il nuovo accordo sullo scambio dei dati PNR senza affatto recepire le osservazioni del *Privacy Supervisor*.

---

446 M. BOTTA, M. DE AZEVEDO, *La protezione*, cit., p. 340.

447 Risoluzione del Parlamento europeo del 5 maggio 2010 *sull'avvio dei negoziati per la conclusione di accordi sui dati del codice di prenotazione (PNR) con gli Stati Uniti, l'Australia e il Canada* (*GUUE* C 81E del 15 marzo 2011, p. 70).

448 Reperibile al seguente *link*: *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-12 09_US_PNR_IT.pdf*.

449 M. SENOR, *Rieccoci con i PNR! Nuovo accordo UE-U.S.A., nuove schermaglie tra istituzioni europee, in MediaLaws,* in *Giornale Online di Diritto e Politica dei Media in un'ottica comparatistica,* 27 dicembre 2010, reperibile su *http://www.medialaws.eu/rieccoci-con-i-pnr-nuovo-accordo-ue-u-s-a-nuove-schermaglie-tra-istituzioni-europee/*.

9. Il nuovo Accordo USA-UE del 15 dicembre 2011

Come dicevamo, i negoziati avviati dalla Commissione con la controparte statunitense nel gennaio del 2011 si conclusero nel dicembre del 2011 e l'accordo venne firmato dai rappresentanti UE e USA il 15 dicembre 2011. La sua entrata in vigore fu stabilita per il 1° luglio 2012.

Il Parlamento europeo, chiamato a pronunciarsi nell'aprile 2012, nonostante fosse stato in precedenza critico sul contenuto dell'accordo, come lo erano stati del resto il Garante europeo ed il Gruppo di Lavoro art. 29, lo approva in Plenaria, con 409 voti a favore, 226 contrari e 33 astensioni.

Anche la dottrina più scettica dovette dunque ammettere che motivazioni politiche e diplomatiche (la c.d. "ragion di stato" di machiavelliana memoria) avevano avuto, ancora una volta, facile giogo delle preoccupazioni relative alla protezione dei diritti fondamentali, seppur col voto contrario di una consistente minoranza di deputati.

Tra gli elementi più rilevanti, l'accordo prevede che i dati siano raccolti per finalità di lotta al terrorismo ed alla grande criminalità transnazionale. Tuttavia la formulazione dell'articolo 4 dell'accordo risulta di portata alquanto estesa e vaga, dilatando così in modo inammissibile l'estensione delle finalità.

Sotto questo profilo l'accordo potrebbe astrattamente essere strumentalizzato per consentire l'utilizzo di questi dati per finalità diverse da quelle espressamente dichiarate, quali ad esempio la repressione delle violazioni delle leggi sull'immigrazione.

La durata della conservazione dei dati viene mantenuta eccessiva, non essendo stata ridotta rispetto ai precedenti accordi ma, addirittura, ulteriormente aumentata.

Nello specifico i dati vengono inizialmente conservati in una banca dati attiva per almeno cinque anni per poi essere trasferiti in una banca dati "dormiente" per dieci ulteriori anni. Dunque, dopo ben quindici anni i dati così conservati vengono convertiti in *files* completamente anonimi, ed in tale condizione il loro periodo di conservazione non conosce più alcun limite; l'accordo prevede infatti che questi dati anonimi possano, in qualsiasi momento, "riacquisire" i propri caratteri di personalità nell' interesse del proficuo svolgimento di indagini da parte delle competenti autorità americane in relazione a rischi concernenti la sicurezza nazionale ovvero in presenza di indizi relativi alla commissione di gravi reati.

Un piccolo progresso sussiste per quanto riguarda le modalità di trasferimento dei dati rispetto al precedente Accordo del 2007, in quanto il nuovo accordo prevede oramai un trasferimento secondo la modalità "push". Allo stesso modo i cittadini dell'Unione europea saranno avvisati dell'utilizzo dei loro dati PNR ed avranno ugualmente il diritto di accesso ai loro dati PNR al fine di ottenerne la rettifica o la cancellazione in caso di inesattezza.

L'accordo prevede ugualmente il diritto di ricorso amministrativo o giudiziario conformemente alla legge americana per i cittadini europei i cui dati siano stati utilizzati in maniera illecita.

Tuttavia, ad onta dei numerosi richiami alle leggi americane in materia di protezione della *privacy* contenute nel testo del nuovo accordo, non appare chiaro in quale misura i diritti ivi menzionati possano essere azionati nella pratica poiché il *Privacy Act* non pare applicabile ai dati PNR[450]. Lo stesso art. 21 dell'Accordo - precisando che quest'ultimo «non crea né conferisce in virtù del diritto degli USA alcun diritto o vantaggio su qualsiasi altra persona pubblica privata o entità» -avvalora seri dubbi circa l'effettività della tutela prevista. Si è osservato che il diritto a un ricorso efficace e all'accesso a un tribunale imparziale in conformità con la Carta dei diritti fondamentali dell'Unione europea è invece prevista espressamente nella decisione comportante l'accettazione dell'Unione dell'accordo PNR tra UE e Australia firmato a Bruxelles il 29 settembre 2011 ed entrato in vigore il 1 giugno 2012[451].

Sembra dunque inevitabile ammettere che il nuovo accordo PNR si colloca certamente al di sotto degli *standard* europei in materia di protezione dei diritti fondamentali, seppur per la necessità di venire incontro a contingenti necessità di sicurezza e prevenzione del fenomeno terroristico[452].

---

450 Vedi *supra*, in riferimento alla stessa problematica per l'Accordo del 2007, il paragrafo 7.1.

451 *GUUE* L 186, 14 luglio 2012, p. 1.

452 S. PEYROU, *Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer: réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne,* in *EADUE*, n. 7, Juillet 2012, étude 8.

10. Considerazioni conclusive

Il rischio che sempre si corre nel voler trattare in modo sintetico una tematica come quella della circolazione e tutela dei dati personali nell'epoca dell'informatizzazione in cui viviamo, è di trovarsi costantemente un passo indietro rispetto agli eventi; come nel paradosso enunciato dal filosofo Zenone di Elea, Achille non riesce mai a prendere la tartaruga. Basti pensare al recente scandalo *NSAgate*[453]*,* noto in Italia come D*ataGate,* le cui ripercussioni sulle politiche e le disposizioni normative ancora *de jure condendo,* relative al trasferimento dati al di fuori dell'Europa, saranno forse comprensibili solo ai posteri.

Dunque, limitandosi ad accennare alla direzione intrapresa in materia di PNR, questa dovrebbe condurre ad un vero e proprio "pacchetto di riforme sulla protezione dati per lo spazio europeo"; la Commissione europea ha infatti proposto all'inizio del 2012 una riforma globale delle norme sulla protezione dei dati dell'Unione europea, costituita da un regolamento generale e da una direttiva, che però il Garante europeo per la protezione dei dati non ha mancato di criticare. Le proposte intendono sostituire, rispettivamente, la decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale e la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995.

Il Consiglio dell'Unione, riunitosi a Lussemburgo il 26 e 27 aprile 2012 in occasione della sua 3162ª sessione nella formazione Giustizia e affari interni, oltre ad adottare la già esaminata decisione relativa alla conclusione del nuovo accordo UE-USA sui PNR in sostituzione di quello preesistente, applicato in via provvisoria dal 2007, ha concordato altresì un orientamento generale sul progetto di direttiva sull'uso dei dati contenuti nel codice di prenotazione a fini di protezione dai reati di terrorismo e dai reati gravi; ciò ha permesso alla presidenza danese di avviare i negoziati con il Parlamento europeo nel quadro della procedura legislativa ordinaria ai sensi dell'art. 294 del TFUE. La discussione in sede di Consiglio ha riguardato, in particolare, due questioni principali: la prima consiste nel determinare se le nuove norme proposte debbano essere circoscritte alla raccolta dei dati del *passenger name record* per i voli da e verso i paesi terzi o se debbano disciplinare anche i voli interni all'UE. Il compromesso proposto permetterebbe agli Stati membri, senza obbligarli, di raccogliere i dati PNR anche per i voli *intra* UE selezionati. La seconda questione principale discussa riguarda il periodo di conservazione. La proposta iniziale della Commissione, presentata nel febbraio 2010, prevede un periodo globale di conservazione di 5 anni. Dopo trenta giorni, tuttavia, i dati PNR dovrebbero essere mascherati; di modo che gli elementi del PNR relativi alla persona non siano più accessibili all'ufficiale dello sportello del servizio di contrasto, e possano essere visionati soltanto dopo aver ottenuto un'autorizzazione specifica. Alcuni Stati membri considerano troppo breve, sotto il profilo operativo, questo periodo iniziale di conservazione di 30 giorni, dal momento che è spesso necessario controllare molto rapidamente - entro poche ore - gli spostamenti di una persona automaticamente selezionata per accertamenti supplementari. La posizione attuale del Consiglio è di mantenere il periodo globale di conservazione di cinque anni, estendendo però di due anni il periodo iniziale durante il quale i dati sono pienamente accessibili. L'obiettivo generale della direttiva proposta è istituire un sistema coerente su scala europea dei dati del codice di prenotazione, creando un modello UE unico per tutti gli Stati membri che adotteranno le nuove norme e assicurando la cooperazione tra le autorità competenti all'interno dell'Unione. Di conseguenza, tutti i vettori aerei che operano sulle rotte disciplinate dalle nuove norme dovranno fornire i dati PNR alle autorità degli Stati membri incaricate dell'applicazione della legge.

Autorità che, tuttavia, sarebbero autorizzate a usare i dati, che già sono raccolti dai vettori aerei, ai soli fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati (transnazionali) gravi.

Attualmente, in seno al Parlamento europeo, la commissione competente è la Commissione per le Libertà civili, giustizia e affari sociali (LIBE). Il relatore per la proposta di Regolamento è l'On. Jan

[453] *http://www.theguardian.com/world/2013/jun/11/edward-snowden-nsa-whistleblower-profile.*

Philipp Albrecht (Gruppo Verdi, Germania), per la proposta di direttiva è l'On. Droutsas (S&D, Grecia). L'*iter* legislativo è tutt'ora in corso.

In conclusione, appare opportuno richiamare gli accordi intervenuti tra l' Unione europea e alcuni Paesi (in particolare Australia e Canada) a cui si è peraltro fatto accenno più volte nella trattazione[454], con una funzione comparativa dei livelli di tutela offerti rispetto all'accordo USA - UE, al fine di esaminarne i più recenti sviluppi.

Nella GUUE L 186 del 14 luglio 2012 è stato pubblicato l'accordo tra l'Unione europea e l'Australia sul trattamento e sul trasferimento dei dati del codice di prenotazione da parte dei vettori aerei all'Agenzia australiana delle dogane e della protezione di frontiera, firmato a Bruxelles il 29 settembre 2011 ed entrato in vigore il 1° giugno 2012, conformemente all'articolo 29, paragrafo 1 dell'accordo.

Anche in questo caso, la solerzia del Garante europeo per la protezione dei dati si è concretizzata in un parere[455]; quest'ultimo accoglie con favore le misure di salvaguardia previste nelle proposte, soprattutto per quanto riguarda l'attuazione concreta dell'accordo e gli aspetti relativi alla sicurezza dei dati, nonché le soddisfacenti disposizioni di supervisione e di contrasto. Il GEPD sottolinea che ogni individuo ha accesso all'autorità australiana per la protezione dei dati, come pure alle autorità giudiziarie australiane, una tra le garanzie fornite dalle proposte e ritenuta essenziale.

Tuttavia, il GEPD ha anche individuato un significativo margine di miglioramento, soprattutto per quanto riguarda il campo di applicazione dell'accordo, la definizione del terrorismo, l'inclusione di alcune finalità eccezionali e il periodo di conservazione dei dati PNR, sproporzionato rispetto al precedente accordo del 2008.

Inoltre, il Garante evidenzia quello che è forse un problema generale della disciplina sui PNR adottata fino ad ora in Europa: egli rammenta che «gli elementi oggettivi da prendere in considerazione per la scelta della base giuridica comprendono in particolare lo scopo e il contenuto dell'atto. Se l'esame di un atto dell'UE rivela che esso persegue una doppia finalità o ha una duplice componente e se una di queste è identificabile come principale o preponderante, mentre l'altra è solo accessoria, l'atto deve essere fondato su un'unica base giuridica, ossia quella richiesta dalla componente fondamentale o preponderante».

In breve, il GEPD affermava che lo scopo dell'accordo, piuttosto che il miglioramento della cooperazione di polizia, avesse quello di autorizzare il trasferimento di dati personali da parte di operatori privati in considerazione della richiesta di un paese terzo, mettendo al contempo in dubbio l'equilibrio tra il trattamento di dati personali su larga scala e lo scopo perseguito, soprattutto in considerazione della varietà di reati inclusi nel campo di applicazione del progetto di accordo, ritenendo che per la lotta al terrorismo e ad altri gravi reati si possa disporre di ben altri efficaci strumenti. Se un tale trasferimento verso un paese terzo non sarebbe in linea di massima possibile in base alle norme dell'UE, l'accordo PNR è dunque da intendersi nel senso di rendere possibile tale trasferimento di dati personali in modo conforme ai requisiti dell'UE in materia di protezione dei dati, attraverso l'adozione di particolari salvaguardie. Per queste ragioni, il GEPD prendeva posizione sul fatto che l'accordo dovesse - almeno principalmente - essere fondato sull'articolo 16 del TFUE e non sugli articoli 82, paragrafo 1, lettera d), e 87, paragrafo 2, lettera a) in linea con la dichiarazione 21 allegata al trattato di Lisbona e nel contesto più ampio della legittimità di qualsiasi sistema PNR, visto come la raccolta sistematica dei dati dei passeggeri per finalità di valutazione del rischio.

Tutte queste considerazioni sono state, tuttavia, in massima parte disattese.

Più critico si è mostrato il Garante europeo in merito alle proposte di decisione di Commissione e Consiglio sull'accordo tra Canada e Unione europeo in materia di trattamento e trasferimento dei PNR[456], precedentemente discusse il 19 luglio 2013 nella 3279 ª sessione del Consiglio dell'Unione e che contengono il testo della proposta di Accordo.

---

454 Vedi *supra* note 408, 438, 442.

455 Pubblicato in *GUUE* C 322, 5 novembre 2011.

456 La sintesi in italiano del parere è pubblicata in *GUUE* C 51, 22 febbraio 2014.

Anche in questo caso il GEPD mette in dubbio la necessità e la proporzionalità dei sistemi PNR e dei trasferimenti in massa di dati PNR a paesi terzi. Conformemente a quanto stabilito sia dalla Carta dei diritti fondamentali dell'Unione europea che dalla Convenzione europea dei diritti dell'uomo, devono essere soddisfatti entrambi i requisiti per eventuali limitazioni all'esercizio dei diritti fondamentali, tra cui il diritto al rispetto della vita privata e alla protezione dei dati di carattere personale; le ragioni addotte dall'autorità pubblica per giustificare tale limitazione devono essere pertinenti e sufficienti, ma occorre altresì dimostrare che non è possibile utilizzare metodi meno invasivi; viene dunque raccomandato che le proposte si basino sull'articolo 16 del TFUE, in combinato disposto con gli articoli 218, paragrafo 5, e 218, paragrafo 6, lettera a), del TFUE.

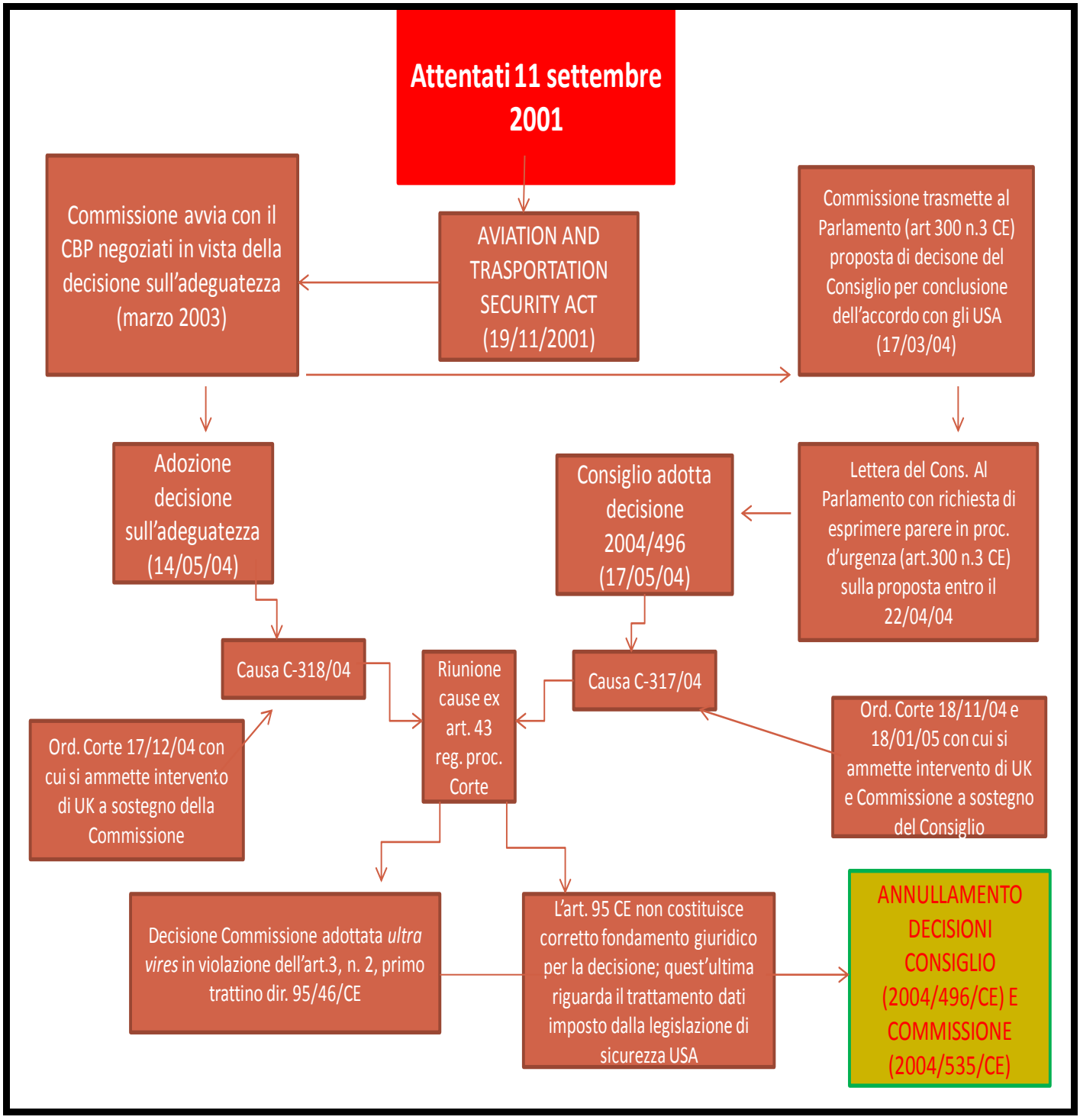
Il Garante ha espresso inoltre perplessità in merito alla limitata disponibilità del ricorso amministrativo indipendente e del pieno ricorso giudiziario per i cittadini dell'UE non presenti in Canada e mette in dubbio che un accordo esecutivo sia idoneo a garantire tali diritti. Il GEPD raccomanda altresì di esigere la conferma che nessun'altra autorità canadese al di fuori di quella competente possa accedere direttamente ai dati PNR o farne richiesta ai vettori contemplati dall'accordo.

In sostanza, a fronte della minaccia rappresentata dal terrorismo globale, si rende oggi necessaria l'adozione di misure per tutelare la sicurezza pubblica, tra le quali il controllo dei PNR. Tuttavia, la gestione in massa di tali informazioni, senza nessuna stretta o nemmeno presunta correlazione tra l'individuo e il fenomeno criminoso, rischia di alterare a svantaggio dei singoli i rapporti con la pubblica autorità, investita così della potestà di godere di una totale discrezione in relazione all'utilizzo dei dati dei propri cittadini (e non) in nome della sicurezza nazionale; discrezione che può inevitabilmente condurre ad un numero di abusi e discriminazioni nella moderna società dell'informazione, dove gli individui sono veri e propri "portatori di dati". Il cammino per raggiungere un migliore equilibrio tra i due opposti interessi della protezione della sicurezza pubblica con la protezione dei dati personali resta ancora lungo.

Cronologia breve:

- 1996: introduzione del sistema CAPPS
- Febbraio 1997: pubblicazione relazione sulla sicurezza aerea della Commissione "Gore"
- 11 Settembre 2001: attentati alle *Twin Towers*
- 25 Ottobre 2001: approvazione *Usa Patriot Act*
- 19 Novembre 2001: approvazione Aviation and Trasportation Security Act (ATSA)
- 1 Agosto 2003: introduzione sistema CAPPS II
- 17 Febbraio 2003: conclusione del *joint statement* tra Commissione e la CBP
- 13 Marzo 2003: risoluzione del Parlamento europeo con parere contrario *all'accordo ad interim*
- 16 Dicembre 2003: comunicazione della Commissione per la futura adozione della decisione di *adeguacy finding*
- 17 Marzo 2004: Commissione trasmette al Parlamento proposta di decisione del Consiglio per la conclusione dell'accordo con gli USA
- 31 Marzo 2004: risoluzione del Parlamento europeo in cui sono espresse un certo numero di riserve di carattere giuridico sulla proposta del Consiglio
- 21 Aprile 2004: approvazione proposta LIBE per il ricorso al parere della Corte di Giustizia
- 14 Maggio 2004: adozione decisione di *adeguacy finding* da parte della Commissione
- 17 Maggio 2004: adozione decisione 2004/496 del Consiglio
- 27 Luglio 2004: presentazione ricorsi alla CGUE
- 17 Dicembre 2004: ordinanza della CGUE di riunione delle cause C-317 e C-318

- 30 Maggio 2006: sentenza della CGUE
- 16 Ottobre 2006: firma nuovo accordo provvisorio USA - UE
- 27 Luglio 2007: firma accordo definitivo USA – UE
- 5 Maggio 2010: risoluzione con cui il Parlamento europeo rinvia il voto per il rinnovo dell'accordo del 2007
- 9 Dicembre 2011: parere del Garante europeo protezione dati
- 15 Dicembre 2011: firma nuovo accordo USA – UE
- 25 Gennaio 2012: comunicazione della Commissione sul nuovo pacchetto di riforme sulla protezione dei dati nello spazio europeo
- Aprile 2012: approvazione accordo USA – UE da parte del Parlamento europeo


Attentati 11 settembre 2001
AVIATION AND TRASPORTATION SECURITY ACT (19/11/2001)
Commissione avvia con il CBP negoziati in vista della decisione sull'adeguatezza (marzo 2003)
Commissione trasmette al Parlamento (art 300 n.3 CE) proposta di decisone del Consiglio per conclusione dell'accordo con gli USA (17/03/04)
Adozione decisione sull'adeguatezza (14/05/04)
Consiglio adotta decisione 2004/496 (17/05/04)
Lettera del Cons. Al Parlamento con richiesta di esprimere parere in proc. d'urgenza (art.300 n.3 CE) sulla proposta entro il 22/04/04
Causa C-318/04
Riunione cause ex art. 43 reg. proc. Corte
Causa C-317/04
Ord. Corte 17/12/04 con cui si ammette intervento di UK a sostegno della Commissione
Ord. Corte 18/11/04 e 18/01/05 con cui si ammette intervento di UK e Commissione a sostegno del Consiglio
Decisione Commissione adottata *ultra vires* in violazione dell'art.3, n. 2, primo trattino dir. 95/46/CE
L'art. 95 CE non costituisce corretto fondamento giuridico per la decisione; quest'ultima riguarda il trattamento dati imposto dalla legislazione di sicurezza USA
ANNULLAMENTO DECISIONI CONSIGLIO (2004/496/CE) E COMMISSIONE (2004/535/CE)