
# Towards a Global Data Protection Framework in the Field of Law Enforcement:

## An EU Perspective

Cristina Blasi Casagran

Thesis submitted for assessment with a view to obtaining
the degree of Doctor of Laws of the European University Institute

Florence, 8 June 2015

European University Institute
**Department of Law**
This thesis has been submitted for language correction

# Towards a Global Data Protection Framework in the Field of Law Enforcement: An EU Perspective

Cristina Blasi Casagran

Thesis submitted for assessment with a view to obtaining the degree of Doctor of Laws of the European University Institute

**Examining Board:**
Professor Marise Cremona, European University Institute (Supervisor)
Professor Gregorio Garzón Clariana, Autonomous University of Barcelona
Dr. Maria O'Neill, University of Abertay Dundee
Professor Martin Scheinin, European University Institute

## Summary

This thesis seeks to examine the existing EU frameworks for data-sharing for law enforcement purposes, both within the EU and between the EU and third countries, the data protection challenges to which these give rise, and the possible responses to those challenges at both EU and global levels. The analysis follows a bottom-up approach, starting with an examination of the EU internal data-sharing instruments. After that, it studies the data transfers conducted under the scope of an international agreement; and finally, it concludes by discussing the current international initiatives for creating universal data protection standards.

As for the EU data-sharing instruments, this thesis demonstrates that these systems present shortcomings with regard to their implementation and usage. Moreover, each instrument has its own provisions on data protection and, despite the adoption of a Framework Decision in 2008, this has not brought about a convergence of data protection rules in the JHA field. A similar multiplicity of instruments is also found when the EU transfers data to third countries for the purpose of preventing and combating crimes. This is evident from examining the existing data-sharing agreements between the EU and the US. Each agreement has a section on data protection and data security rules, which again differ from the general clauses of the 2008 Framework Decision. This study demonstrates the influence of US interests on such agreements, as well as on the ongoing negotiations for an umbrella EU-US Data Protection Agreement.

One possible way to ensure a high level of EU data protection standards in the field of law enforcement in the face of US pressure is by enhancing the role of Europol. This EU Agency shares information with EU member states and third countries. This thesis demonstrates that Europol has a full-fledged data protection framework, which is stronger than most of the member states' privacy laws. However, taking Europol rules as a reference for global standards would only partially achieve the desired result. The exchange of data for security purposes does not only involve law enforcement authorities, but also intelligence services. The recent NSA revelations have shown that the programmes used by these bodies to collect and process data can be far more intrusive and secretive than any current law enforcement system.

In view of the above, this thesis explores the potential of CoE Convention 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and

the Cybercrime Convention as the basis for a global regime for data protection in law enforcement. This thesis concludes that an optimum global data protection framework would entail a combination of the 108 CoE Data Protection Convention and the Cybercrime Convention. The cumulative effect of these two legal instruments would bind both law enforcement and intelligence services in the processing of data. In sum, by promoting the Europol approach to data protection and existing Council of Europe rules, the EU could play a crucial role in the creation of global data protection standards.

## Contents

## Abbreviations

| | |
|---|---|
| AFIS | Automated Fingerprint Identification System |
| AFSJ | Area of Freedom, Security and Justice |
| APEC | Asia-Pacific Economic Cooperation |
| API | Advance Passenger Information |
| APIS | Advance Passenger Information System |
| Art. 29 WP | Article 29 Data Protection Working Party |
| ATFUS | Bureau of Alcohol, Tobacco, Firearms and Explosives |
| ATS | Automated Targeting System |
| AWF | Analysis work files |
| BCR | Binding Corporate Rules |
| BfV | Bundesamt für Verfassungsschutz |
| BND | Bundesnachrichtendienst |
| BNDD | Bureau of Narcotics and Dangerous Drugs |
| CAHDATA | Ad-Hoc Committee on Data Protection |
| CATS | Article 36 Committee |
| CBP | Bureau of Customs and Border Protection |
| CBPR | Cross-Border Privacy Rules |
| CBSA | Canada Border Services Agency |
| CEPOL | European Police College |
| CERTs | Computer Emergency Response Teams |
| CFSP | Common Foreign and Security Policy |
| CICA | Canadian Generally Accepted Privacy Principles |
| CIS | Customs Information System |
| CJEU | Court of Justice of the European Union |
| CNI | Centro Nacional de Inteligencia |
| CoE | Council of Europe |
| CODIS | Combined DNA Index System |
| COMINT | Communications Intelligence |
| CONTAIN | Container Security Advanced Information Networking |
| COREPER | Permanent Representatives Committee |
| COSI | Standing Committee on Internal Security |

| | |
|---|---|
| COTER | Counter-terrorism Working Group |
| CPEA | Cross-Border Privacy Enforcement Arrangement |
| CSDP | Common Security and Defence Policy |
| CSE | Canadian Communications Security Establishment |
| CSI | Container Security Initiative |
| CS-SIS II | Central Second Generation Schengen Information System |
| CS-VIS | Central Visa Information System |
| CT | Counter-terrorism |
| CTC | Counter-Terrorism Coordinator |
| CTTF | Counter-terrorism Task Force |
| CTG | Counter-terrorism Group |
| DEA | US Drug Enforcement Administration |
| DE-CIX | Deutscher Commercial Internet Exchange |
| DGSE | Direction générale de la sécurité extérieure |
| DHS | US Department of Homeland Security |
| DNA | Deoxyribonucleic acid |
| DPA | Data Protection Authority |
| DPO | Data Protection Office |
| DPPA | EU-US Data Privacy and Protection Agreement |
| DPR | Délégation parlementaire au renseignement |
| DSD | Australian Defence Signals Directorate |
| EAS | Europol Analysis System |
| EC | European Communities |
| EC3 | European Cybercrime Centre |
| ECD | Europol Council Decision |
| ECHR | European Convention of Human Rights |
| ECtHR | European Court of Human Rights |
| ECRIS | European Criminal Records Information System |
| EDPS | European Data Protection Supervisor |
| EDU | Europol Drugs Unit |
| EEA | European Economic Area |
| EEAS | European External Action Service |
| EIO | European Investigation Order |
| EIS | Europol Information System |

| | |
|---|---|
| EJN | European Judicial Network |
| ENISA | European Network and Information Security Agency |
| ENUs | Europol National Units |
| ELINT | Electronic intelligence |
| EP | European Parliament |
| ESTA | Electronic System for Travel Authorisation |
| EU | European Union |
| EUCARIS | European Car and Driving License Information System |
| eu-LISA | EU Agency for large-scale IT systems |
| EUMS | European Union Military Staff |
| FBI | US Federal Bureau of Investigation |
| FD | Framework decision |
| FIDE | Customs Files Identification Database |
| FIDT | International Federation for Human Rights |
| FIPPs | Fair Information Practice Principles |
| FISA | US Foreign Intelligence Surveillance Act |
| FISAA | US Foreign Intelligence Surveillance Act Amendment |
| FISC | FISA Intelligence Surveillance Court |
| FISCR | FISA Intelligence Surveillance Court of Review |
| FIUs | Financial Intelligence Units |
| FOIA | Freedom of Information Act |
| FP | Fingerprints |
| FRONTEX | European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union |
| GAPP | Generally Accepted Privacy Principles |
| GCHQ | UK Government Communications Headquarters |
| GCSB | New Zealand Government Communications Security Bureau |
| GG | German Constitution |
| HF | High Frequency |
| HLCG | High Level Contact Group |
| HQ | Headquarters |
| HUMINT | Human intelligence |

| | |
|---|---|
| ICC | Interception of Communications Commissioner |
| ICCPR | International Covenant on Civil and Political Rights |
| ICEUS | Immigration and Customs Enforcement |
| IMINT | Imaginary intelligence |
| InfoEx | Information Exchange System |
| INS | Immigration and Naturalisation Service |
| IntCen | EU Intelligence Analysis Centre |
| IPAHRCS | International Principles on the Application of Human Rights to Communications Surveillance |
| IRSUS | Internal Revenue Service |
| ISA | UK Intelligence Services Act |
| ISC | UK Security Committee of Parliament |
| ISS | Internal Security Strategy |
| JHA | Justice and Home Affairs |
| JIT | Joint Investigation Teams |
| JSB | Joint Supervisory Body |
| LDH | French Human Rights League |
| LIBE | European Parliament Civil Liberties Committee |
| LPM | Loi de Programmation Militaire |
| MAD | Militärischer Abschirmdienst |
| MB | Europol Management Board |
| MCT | Mobile Competence Team |
| MEP | Member of the European Parliament |
| MLA | Mutual Legal Assistance |
| MLAT | Mutual Legal Assistance Treaty |
| NATO | North Atlantic Treaty Organisation |
| NI-SIS II | National Interface Second Generation Schengen Information System |
| NI-VIS | National Interface Visa Information System |
| NCB | National Central Bureau |
| NGO | Non-governmental organisation |
| NPs | National Parliaments |
| NSA | US National Security Agency |
| NSS | National Security Strategy |

| | |
|---|---|
| NTA | New Transatlantic Agenda |
| OECD | Organisation for Economic Co-operation and Development |
| OIA | Office of International Affairs |
| OPT | Occupied Palestinian Territory |
| OSINT | Open Sources Intelligence |
| PDBTS | EU-US Policy Dialogue on Border and Transport Security |
| PEAs | Privacy Enforcement Authorities |
| PIUs | Passenger Information Units |
| PNR | Passenger Name Records |
| PKG | Parlamentarisches Kontrollgremium |
| PKGrG | German Law on the Parliamentarian Control of Intelligence Services of 2009 |
| PPPs | Public-private partnerships |
| QMV | Qualified-majority voting |
| PWGT | Police Working Group on Terrorism |
| RELEX | External relations |
| RIPA | UK Regulation of Investigatory Powers Act |
| SAAC | Schengen Agreement Application Convention |
| SIENA | Secure Information Exchange Network |
| SIGINT | Signals intelligence |
| SIRENE | Supplementary Information Request at the National Entry Bureaux |
| SIS | Schengen Information System |
| SIS II | Second Generation Schengen Information System |
| SitCen | Joint Situation Centre |
| SOC | Serious and organised crime |
| SPOC | Single Point of Contact |
| s-TESTA | Secured Trans European Services for Telematics between Administrations |
| SWIFT | Society for the Worldwide Interbank Financial Telecommunication |
| TEK | Hungarian Anti-Terrorist Centre |
| TEU | Treaty of the European Union |

| | |
|---|---|
| TFEU | Treaty on the Functioning of the European Union |
| TFTP | Terrorist Finance Tracking Program |
| TFTS | European Terrorist Finance Tracking System |
| TIDE | Terrorist Identities Datamart Environment |
| TLD | Transatlantic Legislators' Dialogue |
| TSP | Telecommunication Service Provider |
| TREVI | Terrorism, Radicalism, Extremism, and political Violence |
| TSDB | Terrorist Screening Database |
| TWG | Terrorism Working Group |
| UDHR | Universal Declaration of Human Rights |
| UK | United Kingdom |
| UKIPT | UK's Investigatory Powers Tribunal |
| UMF | Universal Message Format |
| UNSC | Security Council of the United Nations |
| US | United States |
| Patriot Act | Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act |
| USPIS | United States Postal Inspection Service |
| USSS | Secret Service |
| VIS | Visa Information System |
| VRD | Vehicle Registration Data |
| VwGO | Code of Administrative Court Proceedings |
| VWP | US Visa Waiver Program |
| WLS | DHS Watchlist Service |

# Acknowledgments

My decision to pursue a Ph.D. came in 2007 when I was finishing my law degree at the Autonomous University of Barcelona (UAB). At that time I was collaborating with the Department of EU law and I knew that I wanted to begin an academic career. I was sure that my Ph.D. topic would be related to EU law, but I needed more expertise in the area before I could settle on a specific topic. During the following four years, I continued my studies in EU law in Spain and Saarbrücken (Germany), and I also carried out an internship at the Legal Service of the European Commission. In 2011, I felt ready to start my adventure at the EUI.

Many persons have contributed in different ways to this Ph.D. project over the last four years. Therefore, I would like to say a word of thanks to each of them.

First, I would like to thank my Ph.D. supervisor at the EUI, Marise Cremona for believing in me and my project from the very beginning. She has given me unwavering support throughout all these years but, above all, she taught me all that I needed to write a Ph.D. Thanks to her I learned how to structure my ideas, and to develop my own arguments and reasoning. She always gave me valuable comments to improve my work, and I received her complete support in all the internships, workshops and conferences I decided to participate in. In sum, she has been my main source of inspiration during the four years of my Ph.D.

I would also like to thank Martin Scheinin, Steven Peers and Maria O'Neill for their helpful suggestions about parts of this thesis. They have all helped shaped the final version of this thesis. Likewise, I am very grateful to Montserrat Pi, Claudia Jiménez, Esther Zapater and Susana Beltran for facilitating my teaching experience at the UAB.

This thesis would never have been conceivable without the constant encouragement and advice of Dr. Gregorio Garzón Clariana. Dr. Garzón has been my mentor since 2007, when I decided to initiate my academic career. His valuable advice to conclude an LL.M. in Saarbrücken and to apply for a traineeship in the European Commission were essential in order to be awarded with a Ph.D. scholarship at the EUI.

During the years of my Ph.D., I had the opportunity to work as an intern at the European Data Protection Supervisor (EDPS) and at Europol. I am very grateful to Hielke Hijmans, Alba Bosch Moliné, Daniel Drewer, Jan Ellermann, Nayra Pérez Gutiérrez and Pelopidas Donos for their regular help and kindness throughout my

internships. Some of the conversations I had with them have certainly influenced the argument and content of this thesis.

I am indebted to Mike for his permanent support and help since the moment I met him in 2006. He believed in me and lent me a helping hand with every possible question related to my thesis. From him I have learned that with patience and commitment I can achieve anything I set my mind to.

My greatest thanks go to my mother Loles and to my brother Eduard for their loving encouragement and for being a great pillar of support throughout my life. In 2008 I made the decision to continue my studies abroad. Despite the distance, I have always felt them by my side, every single day, ready to hear my problems, but also to make me laugh. I have never thanked them enough for all they have done for me. Without them my dream could have never become a reality. Therefore, I would like to dedicate this thesis to them, as the smallest sign of my gratitude.

# Introduction

*Given the unique power of the state, it is not enough for leaders to say: Trust us, we won't abuse the data we collect. For history has too many examples when that trust has been breached. Our system of government is built on the premise that our liberty cannot depend on the good intentions of those in power; it depends on the law to constrain those in power.*[1]

US President Obama

## 1.1. Subject Matter and Aims

We are in the midst of a war against terrorism. This is the message that governments around the world repeat to society every time they launch a new security measure. Travellers' details, financial information, facial recognition programmes and users' activity on the Internet are just some of the data that are being increasingly accessed and processed by law enforcement authorities for security purposes. The main objective of such governmental surveillance is to prevent, detect, investigate, and prosecute terrorism and other serious criminal offences.

Although the world has recently been subjected to several acts of terrorism, the wave of terror in which we are currently immersed has its origin in the attacks of 9/11, carried out by the terrorist group Al-Qaeda. One week after the attack, the UN Security Council issued a Resolution calling for global cooperation between the UN contracting parties to criminalise all forms of terrorism.[2] Governments, therefore, deemed it necessary to establish a coordinated worldwide security system. After that event, they intensified their mutual cooperation to prevent and combat terrorism. Unfortunately, new attacks ocurred, and this time they took place within the European borders. On the morning of 11 March 2004, coordinated bombings of commuter train in Madrid (Spain) killed 191 people and wounded 1,800. Similarly, on 7 July 2005 a series of coordinated suicide-bomb attacks took place on London's public transport system, killing fifty-six people and injuring over 700. Both attacks were led by Al-Qaeda. Most recently, on 7 January 2015, two French nationals linked to Al-Qaeda killed 12 people in the offices of the satirical newspaper Charlie Hebdo in Paris.

[1] Press release 'Remarks by the President on Review of Signals Intelligence', Department of Justice, Washington D.C., 17.01.2014.
[2] UN Resolution 1373(2001), 28.09.2001.

All of these events have triggered the European Union (EU) to enhance its counter-terrorism policy, increasing police cooperation within and beyond the European territory. In 2009, the Treaty of Lisbon brought significant developments with regard to the Area of Freedom, Security and Justice (AFSJ). The new treaty also permitted the adoption of the Stockholm Programme,[3] as well as the EU Internal Security Strategy.[4] Both documents emphasised the importance of achieving greater coherence between external and internal elements of the work in the AFSJ.

Many of the measures the EU has adopted consist of the processing and sharing of data among law enforcement authorities. The main bone of contention for each of these instruments is their potential clash with the EU fundamental right to data protection. Data protection is a rather new issue due to the astounding advances in computer science and technology of the latter half of the 20th century. It primarily prevents data from being misused or lost by private and public entities.

The Universal Declaration of Human Rights (UDHR) foresees in Article 12 that 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence'. The rights to privacy and data protection are thus universal rights and, accordingly, the principles and scope of that right should be understood in the same way around the world. However, in practice, this is not the case. For instance, many security agreements regarding the collection, processing, storage and transfer of personal data for law enforcement purposes have been concluded between the US and the EU. One of the key tensions during the negotiations of each of these agreements has been related to data protection. This is because the EU and the US have numerous legal differences they had to face with respect to data protection and privacy matters, and these differences have not always been easy to reconcile in the agreements.

However, this divergence is not only found between the EU and the US systems. The EU itself has fragmented laws regarding the processing and protection of personal data for law enforcement purposes. This internal fragmentation within the EU causes legal insecurity for the EU citizens who seek to protect their personal data. Although Article 8 of the EU Charter of Fundamental Rights enshrines the right to data protection, this has been further developed by specific EU and national laws. Yet, such sectoral laws are not consistent with each other, and it ultimately causes a lack of legal protection for the individual.

[3] OJ C 115, 04.05.2010, pp. 1-38.
[4] COM(2010) 673 final, 22.11.2010.

The purpose of this research lies in examining the challenges and feasibility for a global data protection framework in the field of law enforcement, through looking at the EU and its network of external relations as regards data sharing for law enforcement purposes and data protection. Global standards for privacy and data protection are crucial because the sharing of data no longer has any physical borders. In the age of the Internet anyone can learn about and search for just about anything using computers that can save, store, and transmit data, as well as by using smart phones, which can do all of the above. These inventions have changed the way we live exponentially. Since any piece of information can be communicated and shared rapidly from almost anywhere in the world, global standards that pose limits to the processing of personal data are more necessary now than ever before.

Many studies have focused on the right to data protection in the area of security. For instance, De Busser,[5] Boehm,[6] Hillebrand,[7] O'Neill[8] and Tzanou[9] have recently published studies on data protection in the area of EU counter-terrorism and criminal law. All of these studies analyse the internal/external dichotomy of the AFSJ, as well as some data-sharing agreements between the EU and the US. Yet, the existing literature is fragmented and does not offer a full overview of the current EU data-sharing instruments and their data protection rules.

This thesis aims to achieve a full-fledged analysis of the existing EU frameworks for data-sharing for law enforcement purposes within the EU and between the EU and third countries, the data protection challenges to which these give rise, and possible responses to those challenges at both the EU and global levels. In order to do so, I will first analyse and expand the current literature and laws on data-sharing activities among law enforcement authorities within and beyond the EU. After that, I will suggest mechanisms at the EU and the international levels that could offer adequate data

---

[5] De Busser E 2009, *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities*, Maklu Publishers, Antwerpen.

[6] Boehm F 2012a, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Springer, Berlin.

[7] Hillebrand C 2012, *Networks in the European Union. Maintaining democratic legitimacy after 9/11*, Oxford University Press, Oxford.

[8] O'Neill M 2012, *The Evolving Counter-Terrorism Legal Framework,* Routledge Research in EU Law, New York.

[9] Tzanou M 2012, *The added value of data protection as a fundamental right in the EU legal order in the context of law enforcement*, Ph.D thesis, European University Institute, Florence.

protection standards when the information is processed for the prevention and combat of terrorism and other serious crimes.

### 1.2. Limitations of the Research

The scope of this research has certain limitations. First, it is important to highlight that it is conducted solely from an EU perspective. The US legal framework is only scrutinized to the extent that it is relevant for an EU-US comparison. An analysis of the US security measures based on the processing of data is beyond the scope of the present study.

Second, this research focuses on EU law but there are some matters that are not looked at. For example, it does not include a full analysis of the existing EU legislation and CJEU case law on data protection, but only specific data-sharing rules and cases that fall within the area of law enforcement. Moreover, it contains no details about the history of EU data protection law. The study is contemporary and the instruments under consideration have been mostly adopted in the last decade.

In addition, it does not examine data processing activities of all EU agencies within the AFSJ. Particularly, the study of Frontex and Eurojust is omitted because, even if they may process information for law enforcement purposes, they are fundamentally composed of custom and judicial authorities respectively. Therefore, the only EU agency that is an object of study is Europol.

CFSP measures are only considered to the extent that they are adjacent to law enforcement. Furthermore, the 'smart borders package' consisting of the Entry and Exit System (EES) and the Registered Traveller Programme (RTP) is excluded from this thesis since the Commission proposals note that data is not going to be used for law enforcement initially. Only after two years from the entry into force of the regulations, will the necessity for data access by law enforcement authorities be assessed.

Finally, it must be mentioned that this study is fundamentally legal and political. The historical and social issues related to the causes of terrorism, criminal activities, ideologies, etc. are not tackled.[10]

[10] For an analysis on this matter, see Bures O 2011, *EU Counterterrorism Policy. A Paper Tiger?*, Ashgate, Surrey, pp. 10-27.

## 1.3. Methodology and Source Materials

My methodological approach combines both descriptive and normative perspectives. Regarding the descriptive approach, it explains in detail the main EU instruments for sharing information for law enforcement purposes, the EU-US international agreements for the exchange of data, the functioning of Europol, and the EU data protection rules. To do so, it conducts an exhaustive study of the legal documents of the EU (treaties, regulations, Council decisions, directives, etc.) as well as secondary sources such as academic articles, reports and books in the area of data protection and the AFSJ. In addition, the present work takes into consideration personal interviews that I conducted during internships at the EDPS, from July to October 2012, and at the Europol HQ, from May to July 2013. While working for these EU bodies I had the opportunity to talk to experts and officials that provided me with relevant information on data protection matters. Understanding the current EU laws on data protection for law enforcement is critical before venturing into the normative component of this thesis.

The normative approach focuses on the issues to be considered for the establishment of global data protection standards in the field of security. I am seeking to examine the current conflict between different regimes to look at what legal rules are available to resolve them. I also identify the appropriate level at which the rules should be adopted, and I discuss those parties that do manage to strike a balance between data protection and security.

## 1.4. Terminology

This thesis uses a number of concepts that need further clarification. First of all, the terms 'data protection' and 'privacy' are utilised throughout the chapters according to an accepted legal meaning of each. While data protection and privacy are closely linked, they are not identical. Privacy is the individual right of control over one's body, home, property, thoughts, feelings, secrets, and identity. In contrast, data protection relates to all information on identified or identifiable persons, but it does not protect legal persons. It relates to the most essential data that can identify a person (for instance,

name, fingerprints, ID number, or photographs).[11] Despite the differences, privacy and data protection complement each other as rights. They both encompass the obligation for public and private entities to respect the most intimate information that belong to an individual. Numerous jurisprudence of the CJEU has shown that these two rights are closely linked, although they are not identical.[12]

For the purpose of this thesis, the concept of 'law enforcement purposes' and 'counter-terrorism purposes' are not synonyms, since the former is broader than the latter. However, on some occasions, I will treat counter-terrorism as an example of law enforcement, although it may also be other things.

Regarding the concepts of 'data' and 'information', these do not differentiate in meaning. Nevertheless, in strict terms, data is the unstructured, raw collected facts and figures. When such data is structured and placed within a context, it transforms into information.

The concepts of 'field of security' or 'security actors' encompass police, intelligence, and military agents. Concepts of 'terrorism', 'law enforcement', 'organised crime' and 'serious crimes' do not differentiate among them for the purpose of this thesis. Lastly, the term 'processing of personal data' is interpreted in the sense of Article of 2(b) of the Framework Decision 2008/977/JHA. According to this provision, it includes the 'collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

### 1.5. Structure of Study

This thesis is divided into five chapters, including an introduction and a conclusion. It follows a bottom-up approach. From an EU perspective, the establishment of global data protection standards can only be conceived consistently if common laws on data protection already exist among member states of the EU (hereinafter, member states). Therefore, the first chapter of this thesis will begin by studying the EU information systems and databases that fall under the 'internal' dimension of the Area of Freedom, Security and Justice (AFSJ). It will assess both the lack of implementation and use of

[11] For a detailed discussion of the distinction between the two terms, see Kokott J & Sobotta C 2013, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law*, vol. 3, no. 4, pp. 222-228.
[12] See, for instance, C-131/12, 13.05.2014, and C-293/12, 08.04.2014.

these EU legal instruments. It will also highlight the expansion of data-sharing instruments in the EU. In the last ten years, data-sharing laws that were originally created for ensuring the border management and the internal market in the EU have been applied in the field of law enforcement. Chapter 1 will critically analyse the different data protection provisions in each of these EU instruments and explains how it brings fragmentation of the data protection rules in the AFSJ.

Furthermore, in order to set a standard for global data protection laws, the EU and the US would need to agree on the right balance between security and privacy. Chapter 2 will examine how, after 9/11, external pressures (especially from the US) have influenced the EU political and legal environment. In particular, a number of international agreements have been concluded between the EU and the US for the exchange of crime-related information. The chapter will offer a substantive assessment of the EU-US data-sharing agreements and related issues of concern. It will particularly discuss the divergent data protection clauses in each of the agreements. In order to achieve global data protection standards, the EU and US laws on privacy in the field of law enforcement first need to be aligned.

Chapter 3 deals with Europol. It discusses the possibility that Europol data protection rules may become a model to follow for law enforcement authorities' data exchanges within and beyond the EU borders. It sets out the agency's procedures for the exchange of data with member states and third countries, by focusing in particular on the use of SIENA. It also discusses the main features of the proposed Europol regulation, and it compares the data protection standards of the agency with those applied by law enforcement authorities in the member states. It then examines Europol's data exchanges beyond the EU, paying special attention to the relationship between the agency and the US.

There is a close cooperation between law enforcement authorities and intelligence services. In the prevention and investigation of crime, these bodies often exchange intelligence with each other. But what are the safeguards applicable for data collected or accessed by intelligence services? Chapter 4 will provide an analysis of the National Security Agency (NSA) programmes and its secret collaboration with the member states. It will assess whether the EU could set up data protection rules for the exchange of intelligence, despite the Treaty of Lisbon's exclusion of 'national security' matters. It will also examine the scope and relevance of Article 39 TEU, and the feasibility of using this clause as a way to clarify IntCen's data transfers.

After analysing the challenges and issues of concern for the setting up of global data protection standards in the field of security, Chapter 5 will present initiatives for establishing international data protection principles. Particularly, it will specifically look at the OECD Privacy Guidelines, the APEC Privacy Framework, the UN Guidelines for the Regulation of Computerized Personal Data Files, the Council of Europe 1981 Convention and the Cybercrime CoE Convention. These are all proposals from international forums or organisations on the establishment of global data protection rules. After a careful examination, it will suggest a combination of the two CoE Conventions as the most adequate regulatory system to create a global data protection framework. It will also explain how the EU has acquired an important role in influencing the CoE in the field of data protection.

In summary, this thesis will identify specific challenges that the EU needs to overcome in the field of law enforcement in order to achieve global rules on data protection and privacy. It will conclude that the establishment of an international data protection framework for data processed for security purposes requires the EU first to promote consistency among its own member states.

# Chapter 1: Data exchanges for law enforcement purposes within the EU

This analysis of the feasibility for the establishment of global data protection standards in the area of law enforcement will begin by examining the existing EU legislation on these matters. The first observation to be made is that member states were originally the only competent to legislate in the field of criminal law. National governments enjoyed a wide discretion in the adoption of security measures, creating significant differences between member states' criminal systems.[13] The same diversity existed for the particular rules on the collection and processing of data in the prevention, detection, investigation and prosecution of crimes. The main problem resulting from this disparity was the lack of police cross-border police cooperation in the exchange of relevant information during a criminal investigation.

Since 9/11, and especially after the Madrid and London attacks in 2004 and 2005 respectively, the EU has significantly expanded its role within the Area of Freedom, Security and Justice (AFSJ) in the area of data enchange by adopting a number of legal instruments and systems that would add value to the traditional bilateral criminal-related data exchanges between member states.

In the first chapter of this thesis, I will attempt to concisely review the tools available within the EU for exchanging information between law enforcement authorities. It will demonstrate the growth in the creation of data-sharing tools used for security purposes at the EU level. This expansion includes systems that initially fell under the scope of border management and commercial policies. This thesis seeks to find out whether these multiple systems and actors are consistent with each other or not. It will also examine if these measures are actually effective in preventing and detecting crimes, or if they are rather weak in practice.[14]

After that, the EU data protection legislation covering the use of these systems and databases will be studied. It will specifically examine whether all these instruments

[13] Luchtman M 2011 'Choice of forum in an area of freedom, security and justice', *Utrecht Law Review*, vol. 7, no. 1, pp. 44-101.
[14] Bures O & Ahern S 2007, 'The European Model of Building Regional Cooperation Against Terrorism' in *Uniting against Terror. Cooperative nonmilitary responses to the global terrorist threat*, eds. D Cortright & GA López, Massachusetts Institute of Technology Press, Massachusetts, pp. 187 and 223; Bures 2011, pp. 245-254.

operating within the EU offer the same data protection standards for the individuals whose data are processed.

For the last twenty years the EU has been adopting measures in order to approximate national data protection legislations. Yet, the field of law enforcement has always been subject to special rules and conditions due to the intergovernmental nature of criminal laws. Therefore, this chapter will explore the successes and shortcomings that the EU is encountering in the establishment of harmonised data protection rules in the field of law enforcement.

## 1. Origin, evolution and scope of the EC/EU legislation on the processing of personal data for criminal matters

In the current distribution of competences between the EU and its member states, criminal law is, to a large extent, subject to the jurisdiction of each Member State. Consequently, twenty-eight criminal codes coexist in the EU.[15] Some countries, due to their own national background, are characterised as having strong provisions on terrorism and other crimes (particularly, Spain, the United Kingdom, France, Greece, Italy and Portugal), while others do not include many criminal offences in their national laws. In the same way, some legal jurisdictions of the member states allow for certain elements of extraterritoriality when it comes to prosecuting for crimes, while others do not foresee it at all.[16]

Today, there is neither an EU institution with operational police powers, nor a unified EU criminal jurisdiction.[17] Yet, current crimes and offences are often difficult to locate in a well-defined country or territory. Often these might be committed in more than one country, or even on different continents. The cross-border dimension of crime has prompted the establishment of a system of 'multilevel governance' on security matters,[18] in which the EU has progressively adopted measures that coordinate member states' security actions.

---

[15] Yet, it is worth noting that there is no 'criminal code' in either the UK or Ireland. In those countries, criminal law operates on the basis of a mixture of common law and statutes.

[16] For instance, legal jurisdictions of England and Wales allow extraterritoriality for the prosecution of crimes, independent of the provisions in the limited number of EU framework decisions, and more recently directives, about the establishment of jurisdiction.

[17] Lööf R 2008, *Defending liberty and structural integrity: a social contractual analysis of criminal justice in the EU*, Ph.D thesis, European University Institute, Florence, p. 131.

[18] Lavenex S & Wichmann N 2009, 'The external governance of EU Internal Security', *Journal of European Integration*, vol. 31, no. 1, p. 89.

The first instruments enabling a cross-border cooperation among member states date back to before the Treaty of Lisbon. Before Lisbon, there was no legal basis in the Treaties stating that the EU was competent to set up minimum rules on criminal matters. Therefore, the existing secondary legislation on that area was quite dispersed. The EU nonetheless found a way to legislate on criminal matters by enacting either intergovernmental measures within the scope of the former third pillar or directives as part of the former first pillar (the European Communities' pillar).[19] With respect to the first-pillar legal instruments, a few instruments such as the PNR agreements, the API Directive and the now void Data Retention Directive were adopted. Also, regarding the former third pillar on Justice and Home Affairs (JHA), numerous intergovernmental measures for cooperation in law enforcement have come into force since the seventies.

The Terrorism, Radicalism, Extremism, and political Violence (TREVI) Group was established by the European Council in 1976. Its function was to coordinate effective counter-terrorism responses among European governments by organising regular meetings at the ministerial level.[20] The TREVI Group worked on the development of Europol (firstly called Europol Drugs Unit (EDU)) and on the definition of 'terrorism'.[21] In 1979, two new EU initiatives were launched in the field of terrorism: an agreement on the application of the European Convention of Terrorism between the member states, and the Police Working Group on Terrorism (PWGT). The PWGT was later absorbed by the TREVI Group,[22] and integrated in the JHA since 1992 with the Maastricht Treaty.

In 1992, the Treaty of Maastricht introduced provisions that gave new competences to the EU in the field of criminal law. On the one hand, according to the principle of subsidiarity, the EU had competence to regulate on criminal matters as long as member states were unable to do so.[23] On the other hand, Article 31(e) TEU called for the

[19] See, for instance, case C-170/96 *Commission* v. *Council* (Airport Transit Visas) [1998] ECR I-2763, case C-176/03 *Commission* v. *Council* (Environmental Penalties) [2005] ECR I-7879, joined cases C-317/04 & C-318/04, *Parliament* v. *Council* (Passenger Name Recognition) [2006] ECR I-4721, case C-440/05, *Commission* v. *Council* (Ship Source Pollution) [2007] ECR 2007 page I-09097, and case C-91/05 *ECOWAS judgment* (SALW), [2008] ECR page I-03651.

[20] Bunyan T 1993 'Trevi, Europol and the European state', *Statewatching the new Europe*, pp. 1-5.

[21] O'Neill 2012, p. 18.

[22] Kurth Cronin A & Ludes JM 2004, *Attacking terrorism: Elements of a grand strategy*, Georgetown University Press, Washington D.C., p. 154.

[23] For a deeper analysis of the principle of subsidiarity in the field of criminal law, see Baumeister P 2008, 'Das Subsdiaritätprinzip und seine Bedeutung im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen', *Alternativenentwurf Europol und europäischer Datenschutz*, eds. Jürgen Wolter, Wolf-Rüdiger Schenke, Hans Hilger, Josef Ruthig, Mark A. Zoller. C.F.Müller Wissenschaft, pp. 158-169.

establishment of minimum rules relating to the constituent elements of terrorist acts and penalties. The treaty set rules for the first time on JHA, and TREVI was officially dissolved.[24] Two other Working Groups on criminal matters were established that year: the Terrorism Working Group (TWG) and the Working Party on Cooperation in Criminal Matters. While the first was composed of member states' interior ministers and focused on law enforcement cooperation against internal security threats, the latter promoted mutual recognition of criminal acts and judgments within the EU. In essence, the idea of cooperating against terrorism and cross-border crimes became an EU priority with the Treaty of Maastricht.

Particularly relevant for this thesis is the role of Europol. Europol started functioning as the EDU within the framework of TREVI III, dealing mainly with drug-trafficking and money-laundering cases. In 1995, it extended its competences and covered also counter-terrorism investigations.[25] Rules governing this body were first enclosed in the Europol Convention, which was ratified by all member states in 1999. From that moment, Europol became the European law enforcement organisation responsible for assisting member states 24/7 in the prevention and combat of serious forms of crime. Today, Europol is the largest AFSJ agency,[26] covering any crime that affects the common interest of the EU, as well as those serious crimes affecting two or more member states.[27]

In 1997, three other initiatives were incorporated as part of the JHA. First, the Counter-Terrorism Working Group or COTER was established. It deals with current issues in the area of international cooperation against terrorism. Second, the Multidisciplinary Group on Organised Crime was created.[28] It draws up guidelines for the coordinated fight against organised crime. Lastly, the Council established the Article 36 Committee (CATS). This committee coordinates the competent Council working groups in the field of police and judicial cooperation and prepares relevant work of the Permanent Representatives Committee (COREPER).[29]

The AFSJ has its origins in the Treaty of Amsterdam of 1999. Although the policy

[24] O'Neill 2012, p. 18.
[25] O'Neill 2012, pp. 71-72.
[26] Boehm F 2012b, 'Information sharing in the Area of Freedom, Security and Justice – Towards a common standard for data exchange between agencies and EU information systems' in *European Data Protection: In Good Health?*, eds. Gutwirth S, Leenes R, de Hert P & Poullet Y, Springer, Berlin, p. 177.
[27] Europol is thoroughly examined in Chapter 3 of this thesis.
[28] Now replaced by the Working Party on General Matters.
[29] CATS has now turned into the COSI Committee, regulated in Article 71 TFEU.

has no recognised definition to date, numerous scholars have tried to make sense of this new concept in their studies. In that sense, Wolf, Wichmann & Mounier define it as:

'An attempt to provide an overall strategic orientation to punctual measures adopted in the policy area of JHA, such as border management, the fight against terrorism and the fight against organized crime.'[30]

The Treaty of Amsterdam established in Article 61(e) TEU that the Council needed to adopt measures in the area of police and judicial cooperation that would enshrine a high level of security and would conform to the TEU. The treaty amended some provisions of the JHA policy area. For instance, policies on border checks, asylum and immigration were moved from the former third pillar to the first, enhancing the Community's jurisdiction to adopt measures on criminal matters. Likewise, the Court of Justice of the European Union (CJEU) became competent to decide on the AFSJ legislation that fell under the scope of the first pillar. However, provisions on police and judicial cooperation in criminal matters remained as former third-pillar policies. Consequently, the only way for the EC to legislate on such areas was by widely interpreting criminal measures as part of the scope of either customs union or internal market policies.[31]

Thus, by the end of the nineties the EU had launched some initiatives to approximate national measures in the field of criminal matters. Among them, the Tampere Conclusions of 1999 are to be highlighted. They set up the European Police Chiefs Task Force as a forum where high-ranking national policemen could discuss cross-border security matters. Also, in the Tampere Conclusions the European Council pinpointed the need for a 'common effort […] to prevent and fight crime and criminal organisations throughout the Union'.[32] However, the ratification of some of these measures was slow, and they were only accelerated after the terrorist attacks of 11 September 2001.

[30] Wolff S, Wichmann N & Mounier G 2009, 'The external dimension of justice and home affairs: A different security agenda for the EU?', *European Integration* vol. 31, no. 1, p. 10.
[31] This is examined in section 3.2.3 of this chapter with respect to the void Directive 2006/24/EC.
[32] European Council. Tampere Conclusions, 15-16.10.1999.

The 9/11 attacks had a significant impact on the EU legislation, particularly on the adoption of new laws within the scope of the AFSJ.[33] The first EU action plan on terrorism was adopted on 16 October 2001 and it enabled intelligence services of the member states to exchange information and to increase their cooperation.[34] Likewise, the creation of the Counter-terrorism Group (CTG) and the CP 931 Working Party[35] took place right after the attacks. The EU also adopted the European Security Strategy, in which it announced its aim of contributing to the global security through external actions.[36]

The Security Council of the United Nations (UNSC) enacted many resolutions for the prevention and fight against terrorism to be implemented by its contracting parties (including all EU Members). But resolutions from the UNSC are not *self-executing* and they required a national enforcement mechanism. Therefore, the EU had to adopt measures implementing such UN resolutions before they were incorporated in the domestic laws of the member states. Especially important was the Common Position 2001/930/CFSP on countering terrorism,[37] which implemented the UNSC Resolution 1373 (2001). Similarly, Council Framework Decision 2002/475/JHA on combating terrorism provided for the first time a common definition for the crime of terrorism among the member states, and it obliged them to implement that crime in their criminal codes.[38]

The EU security measures for the exchange of information increased dramatically after 9/11. Data exchanges between member states and EU bodies became a crucial tool for the prevention of future similar attacks. Nevertheless, more terrorist attacks occurred: on 11 March 2004 when bombs were simultaneously detonated on the commuter train system in Madrid and, one year later, on 7 July 2005, similar bombings took place on three underground trains and a bus in central London.

---

[33] Hayes B & Jones C 2013, 'Catalogue of EU Counter-Terrorism Measures Adopted since 11 September 2001', *SECILE: Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness*, p. 25. Available from <secile.eu> [22 October 2014].

[34] Council of the European Union, 12800/01, 'Note from the Presidency. Co-ordination of Implementation of the Plan of Action to Combat Terrorism', 16.10.2001.

[35] OJ L 344, 28.12.2001, pp. 93-96.

[36] Council of the European Union, European Security Strategy, *A secure Europe in a better World*, 12.12.2003. http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf

[37] OJ L 344, 28.12.2001, pp. 90-92.

[38] OJ L 164, 22.06.2002, pp. 3–7.

The EU institutions launched several initiatives after the attacks in Madrid and London. The European Council issued a declaration[39] in 2004, which was reaffirmed in 2005.[40] They highlighted the need to adopt common measures on the retention of telecommunications data as soon as possible. In response to both declarations, the Commission launched a series of communications[41] suggesting ways how to improve the coordination of counter-terrorism activities inside the EU institutions and how to enhance the member states' access to information. These communications also proposed the establishment of an integrated approach in the fight against terrorism. In 2005, two other EU instruments came into force: Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences,[42] and the Hague Programme.[43] Even though this programme has been described as relatively timid by some scholars,[44] it contained several recommendations for the intensification of police cooperation within the EU, and the establishment of systems for the cross-border exchange of information.

The Madrid bombings motivated the creation of a Counter-Terrorism Coordinator (CTC) in 2004.[45] The CTC is tasked with monitoring and implementing the EU Counter-Terrorism Strategy. This strategy sought the exchange of information and cooperation concerning terrorist offences and was finally adopted in 2005.[46] The EU Counter-Terrorism Strategy was based on four main pillars: prevention, protection, pursuit and response. Although the role of the CTC has been often criticized for not having any executive powers, this figure exerts significant influence in numerous decisions in the field of counter-terrorism.[47]

One day before the Treaty of Lisbon entered into force, several EU measures related to the exchange of information in the field of law enforcement were adopted.[48] The

---

[39] Council of the European Union, *Declaration on combating terrorism*, 25.03.2004. http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/79637.pdf

[40] Council of the European Union, *Declaration on condemning the terrorist attacks on London*, 13.07.2005 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/85703.pdf

[41] COM(2004) 376 final, 18.05.2004; COM (2004) 429 final, 16.06.2004; COM(2004) 698 final, COM(2004) 702 final, COM(2004) 701 final and COM(2004) 700 final, 20.10.2004.

[42] OJ L 253, 29.09.2005, pp. 22-24.

[43] OJ C 53, 03.03.2005, pp. 1-14.

[44] For instance, Bures 2011, p. 70.

[45] The current CTC is Gilles de Kerchove.

[46] Council of the European Union, 14469/4/05 REV 4, 30.11.2005.

[47] Mackenzie A, Bures O, Kaunert C & Léonard S 2013, 'The European Union Counter-terrorism Coordinator and the External Dimension of the European Union Counter-terrorism Policy', *Perspectives on European Politics and Society*, vol. 14 no. 3, pp. 325-338.

[48] These EU measures are Framework Decision 2009/902 setting up a European Crime Prevention Network (EUCPN) and repealing Decision 2001/427; Decision 2009/917 on the use of information

main reason for this was to avoid the new EU policy-making procedure, in which the European Parliament (EP) would vote for those security measures within the scope of the AFSJ in co-decision with the Council.

When the Treaty of Lisbon came into force in December 2009, the legal paradigm changed. One of the main amendments was the removal of the pillars and the shared competence between the EU and its member states on the AFSJ,[49] including data-sharing security measures.[50] The Treaty of Lisbon also incorporates an explicit legal basis for the approximation of national criminal laws in Article 83 TFEU. According to this clause, the EU can establish:

'Minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis'.

Thanks to this provision, the EU has expanded the definition of terrorism and it has also established a common list of terrorist groups. These EU common rules seek to complement national criminal laws, without replacing them. This is explicitly underlined in Article 276 TFEU, which states that:

'The Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State or the exercise of the responsibilities incumbent upon member states with regard to the maintenance of law and order and the safeguarding of internal security.'

The EU can also create rules on how to ensure the implementation of EU measures at the national level.[51] According to Protocol 36, attached to the Treaty of Lisbon, member

technology for customs purposes; Decision 2009/934 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information; Decision 2009/936 adopting the implementing rules for Europol analysis work files; Decision 2009/968 adopting the rules on the confidentiality of Europol information.

[49] Article 3(2) TFEU and Article 4(2)(j) TFEU.

[50] Articles 82(1) and 87(2)(a) TFEU.

[51] See for instance, Directive 2013/40/EU for the harmonisation of criminal sanctions and procedures against cyber attacks, OJ L 218, 18.08.2013, pp. 8-14.

states had to implement those EU instruments consisting of the exchange of data among law enforcement (formerly adopted under the third pillar) by 1 December 2014.[52] Article 10(4) of the protocol foresaw the possibility that the UK would not implement such instruments as long as the notification was made at least six months before the expiration of the transitional period. The UK notified its intention to opt-out in 2013[53] and later opted back in again to 35 measures.[54] Today, the UK is bound by some of the current EU data-sharing systems – but not all of them.[55]

The Treaty of Lisbon also includes the participation of the EP and the CJEU in the decision and review of EU measures for the fight against terrorism and organised crime. Lastly, the solidarity clause of Article 222 TFEU binds member states to provide assistance and to mobilise all instruments and resources at their disposal in case of a terrorist attack.

After the Treaty of Lisbon entered into force, the fear of a new terrorist attack within the EU reappeared, and France and Germany were the main targets.[56] In consequence, new EU measures in the field of criminal law were enacted. The Commission released communications announcing its intentions to strengthen the EU counter-terrorism and criminal policies,[57] and the Ad Hoc Working Group on Information Exchange for an Information Management Strategy was subsequently established.[58]

Particularly relevant is the adoption of the Stockholm Programme in December 2009,[59] in an attempt to assess the evolution and achievement of policies that were part of the AFSJ. In it, the Commission highlighted the primary concerns, and it introduced

---

[52] List of the former third pillar acquis: Council of the European Union, 9930/14, 19.05.2014.

[53] Letter from the European Parliament President to the Commission on UK JHA OPT-OUT, 02.08.2013; and letter from the Commission President to the European Parliament, 5.9.2013. See also UK House of Commons Home Affairs Committee, 'Pre-Lisbon Treaty EU police and criminal justice measures: the UK's opt-in decision', Ninth Report of Session 2013–14, 29.10.2013. On the consequences of this exception, see the Proposal for a Council Decision determining certain consequential and transitional arrangements concerning the cessation of participation of the United Kingdom of Great Britain and Northern Ireland in certain acts of the Union in the field of police cooperation and judicial cooperation in criminal matters adopted before the entry into force of the Treaty of Lisbon, COM(2014) 596 final, 26.09.2014.

[54] Miller V 2014 'The UK block opt-out in police and judicial cooperation in criminal matters: recent developments', *House of Commons, International Affairs and Defence Section, Standard Note: SN/IA/6930,* 10.11.2014.

[55] For instance, the UK has decided to rejoin SIS II, CIS, ECRIS, Eurojust, Europol and the Swedish initiative, to name but a few. See 'Protocol 36 to the Treaty of Lisbon on transitional provision: the position of the United Kingdom', European Parliament, Committee on Civil Liberties, Justice and Home Affairs 2014 – 2019, November 2014.

[56] Kaunert C 2012 'Conclusion: assessing the external dimension of EU counter-terrorism –ten years on', *European Security*, vol. 21 no. 4, p. 578.

[57] COM(2010)386 final, 20.07.2010 and COM(2011) 573 final, 20.09.2011.

[58] Council of the European Union, 16637/09, 25.11.2009.

[59] OJ C 115, 04.05.2010, pp. 1-38

broad recommendations within the AFSJ. Likewise, the programme identified the increasing amount of data exchanged among member states during criminal proceedings, and it referred to the current data-processing instruments.

The Stockholm Programme was put into action by the Council and the Commission. In February 2010 the Council released a 'Draft Internal Security Strategy for the European Union: Towards a European Security Model',[60] while in November that year the Commission issued a detailed communication on 'The EU Internal Security Strategy in Action: five steps towards a more secure Europe'.[61] At the same time, the Council adopted Decision 2010/131/EU,[62] which set up the Standing Committee on Internal Security (COSI). According to Article 3(1) of that decision, the COSI's purpose is to facilitate and ensure effective operational cooperation and coordination between police and customs authorities. COSI is also responsible for helping ensure consistency in the activities of Eurojust, Europol, Frontex and other relevant bodies that may be invited to attend the Committee's meetings as observers.[63] Yet, its meetings have often been criticised because they gather only national law enforcement officials from member states, but not bodies in charge of fundamental freedoms and rights (e.g. privacy rights).[64]

Regarding the data-sharing measures for law enforcement purposes, the Commission released communications in 2010 and 2012.[65] In them, it underlined that 'no new EU-level law enforcement databases or information exchange instruments are […] needed at this stage'.[66] However, the paradigm changed after the terrorist attacks occurred in Paris on 7 January 2015. After this tragedy, Ministers of Home Affairs of the member states met in Paris to decide on the adoption of new counter-terrorism measures within the EU. These will reinforce the police and intelligence cooperation in the exchange of crime-related information. However, at the time of writing this thesis, there is no certainty as to the exact measures that will be proposed. Therefore, this thesis will only

[60] Council of the European Union, 5842/2/10, 23.02.2010.
[61] COM(2010)673 final, 22.11.2010; Council of the European Union, 16797/10, 23.11.2010.
[62] OJ L 52, 03.03.2010, p. 50.
[63] Article 5 of Decision 2010/131/EU.
[64] Scherrer A, Jeandesboz J & Guittet EM 2011, 'Developing an EU internal security strategy, fighting terrorism and organised crime'. *European Parliament, Directorate General for Internal Policies. Policy Department C: Citizens' rights and Constitutional Affairs. Civil Liberties, Justice and Home Affaires*, Brussels, p. 45.
[65] COM(2010)385 final, 20.07.2010 and COM(2012)735 final, 07.12.2012.
[66] COM(2012)735 final, 07.12.2012, p. 2.

analyse the data-sharing instruments and databases that are functioning today within the field of security.

## 2. EU data-sharing instruments for law enforcement purposes

Two methods for the exchange of crime-related information within the EU can be distinguished. The first one refers to the traditional mutual legal assistance (MLA) procedure between member states. It is a pure bilateral contract that allows member state 'A' to request specific information from member state 'B', and the latter has the obligation to transfer it. This system has been commonly used within the EU to gather evidence, information about previous convictions, fingerprints and many other relevant data during a criminal investigation.

However, after 9/11 and especially after the Madrid and London terrorist attacks, the EU has been seeking a stronger integration of its member states within the AFSJ. Therefore, a number of EU instruments have been adopted to centralise and coordinate the exchange of information. These serve as an alternative to the traditional MLA procedures and deepen the EU integration in the field of criminal matters. The sections below will analyse whether these systems work in a consistent manner, and whether they offer sufficient data protection safeguards.

### 2.1. The use of traditional mutual legal assistance procedures within the EU

In order to understand the *raison d'être* of the European information systems, a few words about the functioning of the traditional mutual legal assistance (MLA) procedures are needed. The MLA procedures could be defined as the first step to reach a full mutual recognition among member states. Mutual recognition is regulated in Article 82(2)(a) TFEU and it was first created as part of the EU economic policy. Resulting from the establishment of the single market, member states had to find the way to recognise goods and products from other EU countries as equivalent in quality as their own domestic products. Today mutual recognition applies to other legal areas that are not harmonised at the EU level, such as criminal law. The new European Investigation

Order (EIO), examined below, is one example of a measure applying mutual recognition in criminal matters.[67]

As noted above, member states differ in their criminal procedural systems. Thus, when a criminal investigation is carried out in one member state by a particular national judicial authority, the procedures and laws enforced do not coincide in other EU countries.[68] This hinders the efficient cooperation between member states in the exchange of criminal information. Therefore, both the Tampere and the Hague Programmes defined mutual recognition as the cornerstone of the EU judicial cooperation.[69]

In cases where mutual recognition is not possible, the traditional mutual legal assistance (MLA) procedures can still apply. The Commission defines the MLA procedure as:

'The cooperation between different countries for the purpose of gathering and exchanging information, and requesting and providing assistance in obtaining evidence located in one country to assist in criminal investigations or proceedings in another.'[70]

---

[67] Some other examples are Framework Decision 2005/214 on the application of the principle of mutual recognition to financial penalties, 24 February 2005; Framework Decision 2006/783 on the application of the principle of mutual recognition to confiscation orders, 6 October 2006; Framework Decision 2008/909 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union, 27 November 2008; Framework Decision 2008/947 on the application of the principle of mutual recognition to judgments and probation decisions with the view to the supervision of probation measures and alternative sanctions, 27 November 2008; Framework Decision 2009/299 amending Framework Decision 2002/584, 2005/214, 2006/783, 2008/947, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition in the absence of the person concerned at the trial, 26 February 2009; and Framework Decision 2009/829 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention, 23 October 2009.

[68] Jones C 2011, 'Implementing the "principle of availability": The European Criminal Records Information System, The European Police Records Index System, The Information Exchange Platform for Law Enforcement Authorities', *Statewatch Analysis*, p. 5. Available from <www.statewatch.com> [22 October 2014]; Sayers D 2011, 'The European Investigation Order Travelling without a "roadmap"', *CEPS Paper in Liberty and Security in Europe*, p. 3; Vernimmen-Van Tiggelen G & Surano L 2008, 'Analysis of the future of mutual recognition in criminal matters in the European Union', *Institute for European Studies*, *Université Libre de Bruxelle, ECLAN Report,* p. 23. Available from http://ec.europa.eu/justice/criminal/files/mutual_recognition_en.pdf [23 October 2014].

[69] Tampere European Council Conclusions, 15-16.10.1999; Council of the European Union, 14898/13, 16.10.2013, p. 3.

[70] European Commission, 'Mutual Legal Assistance and Extradition', Available from <http://ec.europa.eu/justice/criminal/judicial-cooperation/legal-assistance/index_en.htm> [23 October 2014].

The main distinction between the mutual recognition and the MLA regimes is the power of the executing authority: under the mutual recognition system, the national judicial authority directly orders the foreign authority to recognise and execute a decision. The grounds for refusal by the foreign authorities are very limited here. In contrast, the MLA regime gives the foreign Member State the discretion to refuse the execution of the order.[71] This section focuses exclusively on the analysis of the MLA procedure, since it predominates in the exchange of information among law enforcement forces.

Mutual legal assistance was originally only regulated by the Council of Europe. In particular, the Convention on mutual assistance in criminal matters (hereinafter, MLA Convention) dates back to 1959 and has been ratified by all member states.[72] It is accompanied by two protocols, signed in 1978 and 2001. Although EU member states adopted rules on mutual legal assistance since 1959, the establishment of a MLA procedure within the EU to assist cross-border exchanges of information for law enforcement purposes became a major necessity back in mid-1990s.[73] During those years the Treaty of Amsterdam and Tampere European Council called for an enhancement of MLA in criminal matters as part of the programme for developing an AFSJ.[74]

MLA procedures were reinforced in 2000. That year, the Council adopted an act supplementing the MLA Convention between the member states (hereinafter, EU MLA Convention).[75] It was accompanied by a protocol,[76] which came into force in 2005. The EU MLA Convention includes new mechanisms for the exchange of information within the EU such as the creation of Joint Investigation Teams (hereinafter, JITs).[77] JITs were first regulated in the Council Framework Decision 2002/465/JHA[78] and consist of an agreement signed by two or more member states to conduct a criminal investigation together for a limited period.

---

[71] Mangiaracina A 2014, 'A new and controversial scenario in the gathering of evidence at the European level: The proposal for a Directive on the European Investigation Order', *Utrecht Law Review*, vol. 10, no. 1, pp. 115-116.
[72] Council of Europe, European Convention on Mutual Assistance in Criminal Matters, 20.4.1959.
[73] The Joint Action 98/427 on good practice in mutual legal assistance in criminal matters (OJ L 191, 07.07.1998), was adopted within this context.
[74] Jones 2011, p. 9.
[75] OJ C 197, 12.07.2000, pp. 1-23.
[76] OJ C 326, 21.11.2001, pp. 1-8.
[77] Article 13 EU MLA Convention. Later JITs were further regulated in Council Decision 2005/671/JHA, OJ L 253, 29.09.2005, pp. 22-24.
[78] OJ L 162, 20.06.2002, pp. 1-3.

Although MLA procedures have been designed to enable a fluent communication among EU police and judicial authorities, their use has been subject to several problems in practice. First, MLA procedures consist of a flexible and discretionary system that requires a case-by-case consideration by the requested member state. This procedure creates uncertainty because it is the requested country that decides whether it wants to provide the information or not. Second, the procedure does not always involve a court authorisation over the particular information collected.[79] Finally, the MLA Convention does not include rules on automated processes and response times for requests. Although Article 5(4) of the EU MLA Convention obliges the requested authority to inform without delay, there is no mandatory rule on the length of the procedure, so it tends to be slow. All of these issues cause uncertainty for the actors participating in the MLA procedures, since the system varies from one country to the other, and from case to case.

Trying to overcome the flaws of the MLA procedures, the EU decided to adopt complementary legal instruments, which facilitated the cooperation of law enforcement authorities in the exchange of data. These are the Swedish initiative, the Prüm Decisions, the ECRIS Decisions, and the EIO initiative.

### 2.2. Post-9/11 data-sharing instruments

The Madrid terrorist attacks of 2004 highlighted the necessity to create a better system for accessing and exchanging crime-related information between member states. In that sense, the Hague Programme noted that 'full use [had to] be made of new technology and that there [had to] be reciprocal access to national databases'.[80] At that time, the EU had only a few instruments regulating cross-border law enforcement data exchanges, such as the Europol and Eurojust Conventions, the EU Convention on Mutual Assistance in Criminal Matters 2000, and the Council Framework Decision on Joint Investigation Teams.

In particular, MLA procedures had too many limitations, since they were only designed to share information bilaterally and, as described above, it can take months from the moment a member state receives the information requested from another

[79] EDRI 2013, 'An introduction to Data Protection', *EDRI Papers*, no. 6, p. 18. Available from: http://www.edri.org/files/paper06_datap.pdf [23 October 2014].
[80] Council Decision 2008/615/JHA, recital 7. OJ L 210, 06.08.2008, pp. 1-11.

member state. For those reasons, the EU established other legal instruments to be implemented by member states in order to accelerate, simplify and intensify the cooperation between them in the exchange of information.

The first instrument adopted by the EU for improving the cooperation among EU member states in the exchange of criminal information was Council Framework Decision 2006/960/JHA[81] (hereinafter, the Swedish initiative or the Framework Decision) in 2006. According to Article 1 of the Framework Decision, it has the following purpose:

'To establish the rules under which Member States' law enforcement authorities may exchange existing information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations.'

This Framework Decision requires complying with the 'principle of availability',[82] which guarantees the requesting Member State 'equivalent access'[83] to that offered to the internal authorities. This principle, which was first introduced in the Hague Programme,[84] means that a Member State cannot request conditions stricter than those required for its national law enforcement authorities for a purely internal case.[85] Regarding the time limits, Article 4 establishes that transfers for urgent cases[86] should not exceed eight hours from the moment the request is sent. In contrast, non-urgent requests may take up to fourteen days until the requesting Member State receives the information.

The Swedish initiative was later complemented by the Prüm procedures. Prüm is a decentralised system of national databases that dates back to 2005. That year, five member states – Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria – signed the Prüm Convention,[87] which aimed at achieving a closer cooperation between member states in the investigation of crimes with a potential cross-border

[81] OJ L 386, 29.12.2006, pp. 89-100.
[82] Council of the European Union, 15278/11, 14.10.2011, p. 2.
[83] Communication from the Commission to the European Parliament and the Council. Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM), COM(2012)735, 07.12.2012, p. 2.
[84] The Hague Programme, point 2.1.
[85] Article 3 of Swedish initiative.
[86] Member states agreed that the notion of urgency should be interpreted in a restricted manner. Council of the European Union, 15278/11, 14.10.2011, p. 4.
[87] Council of the European Union, 10900/05, 07.07.2012.

dimension. As in the Swedish initiative, it sought 'to overcome lengthy mutual legal assistance bureaucratic procedures by establishing a single national contact point'.[88] Through these contact units, member state 'A' could send a request to Member State 'B' to check whether the latter had DNA, fingerprint, or vehicle data for a specific target. If so, a 'hit' would be sent to the requesting Member State and, only then, that country would be able to send a second request for accessing such data.[89]

Originally, the Prüm Convention was a purely intergovernmental agreement and, therefore, it fell outside the scope of the EU treaties. Criticism about the lack of transparency[90] led to a change in the Prüm Convention's nature in 2008. A proposal to integrate Prüm into the EU laws was presented in January 2007 by the German Presidency of the Council[91] and, one year later, the provisions of the treaty were transposed into EU instruments by Council Decisions 2008/615/JHA[92] and 2008/616/JHA[93] (hereinafter, the Prüm Decisions).

The Prüm Decisions are based on the main provisions of the former Prüm Convention, but they improve and speed up the exchange of information.[94] Exchange mechanisms for DNA, fingerprint (FP) and vehicle registration data (VRD) of the Prüm Convention have also been transposed into the legal framework of the EU.[95] In the new instrument, a distinction is made between DNA and FP exchange on the one hand, and VRD on the other. For the first two categories of data, which are biometric, the mechanism operates on a 'hit/no-hit' basis,[96] and the related personal data are only provided in response to a separate follow-up request. In other words, in the case of a hit, the national contact point conducting the search receives only a confirmation, but never

---

[88] Töpfer E 2011, 'Europe's emerging web of DNA databases', *Statewatch Journal*, vol. 21 no. 1. Available from http://database.statewatch.org/article.asp?aid=30566 [23 October 2014].
[89] Soleto Muñoz H & Fiodorova A 2014, 'DNA and law enforcement in the European Union: Tools and human rights protection', *Utrecht Law Review*, vol. 10, no. 1, p. 152.
[90] European Parliament, 'Working Document on a Council Decision on the stepping up of crossborder cooperation, particularly in combating terrorism and cross-border crime'. Rapporteur: Fausto Correia. Committee on Civil Liberties, Justice and Home Affairs, 10.04.2007.
[91] Hernanz N 2011, 'More surveillance, more security? The landscape of surveillance in Europe and challenges to data protection and privacy – Policy report on the proceedings of a conference at the European Parliament', *SAPIENT Deliverable 6.4.*, p. 8. Available from http://www.sapientproject.eu/docs/D6.4-Policy-Brief-submitted-January-2012-29.pdf [23 October 2014].
[92] OJ L 210, 06.08.2008, pp. 1-11.
[93] OJ L 210, 06.08.2008, pp. 12-72.
[94] They are also complemented by Council Decision 2008/617/JHA of 23 June 2008 on the improvement of cooperation between the special intervention units of the Member States of the European Union in crisis situations, OJ L 210, 06.08.2008, pp. 73-75.
[95] COM(2012) 735, 07.12.2012, p. 4.
[96] The hit/no hit system means that DNA profiles or fingerprints found at a crime scene in one Member State can be compared with profiles held in databases of other member states.

the information on the DNA or FP samples.[97] After a hit, the requesting authorities are required to use pre-existing bilateral or multilateral agreements (e.g. MLA procedures, the Swedish initiative, etc.) for obtaining the necessary biometric data.[98]

Along with the Swedish initiative and the Prüm Decisions, a further instrument was launched in 2004:[99] the European Criminal Records Information System (ECRIS). Designed for the exchange of information on convictions among member states, ECRIS was the successor of the Network of Judicial Registers, a tool set up by Germany, France, Spain and Belgium in 2003. In 2005, the Commission released a white paper shaping the initiative[100] and, a few months later, the Council adopted Decision 2005/876/JHA on the exchange of information extracted from the criminal record,[101] which was later amended as Council Framework Decision 2008/675/JHA.[102]

In the course of any national criminal proceeding, ECRIS allows police and judicial authorities to obtain information about all previous convictions registered in other member states. With the same purpose, the Commission adopted two other legal instruments in 2009: Council Framework Decision 2009/315/JHA on the exchange of information extracted from criminal records,[103] and the Implementation of the Council Decision 2009/316/JHA on the establishment of the European Criminal Records Information System[104] (hereinafter, the ECRIS Decisions). The ECRIS Decisions established rules among member states for the exchange of information on convictions and data extracted from criminal records. Through this system, any EU country could access comprehensive information on the offending history of any EU citizen, irrespective of the country in which the person was convicted. As a result, the possibility for offenders to escape their criminal past simply by moving from one Member State to another was extinguished.

As for the mechanisms for communication, messages are transmitted by the ECRIS software installed in every Member State. This software is programmed to notify the

[97] Hernanz 2011, p. 8.
[98] Council Decision 2008/615/JHA, recital 10.
[99] COM(2010) 385 final, 20.07.2010, p. 12.
[100] European Commission, White Paper on exchanges of information on convictions and the effect of such convictions in the European Union, COM(2005) 10 final, 25.01.2005.
[101] OJ L 322, 09.12.2005, pp. 33-37.
[102] OJ L 220, 15.08.2008, pp. 32-34.
[103] OJ L 93, 07.04.2009, pp. 23-32.
[104] OJ L 93, 07.04.2009, pp. 33-48.

end of the data retention after thirty days. Regarding the categories of data, the system allows the sending of fingerprint imagery and alphanumerical data.[105]

The last of the EU data-sharing instruments to be studied in this chapter is the European Investigation Order (EIO). The EIO is a judicial decision issued by a Member State in order to have one or several specific investigative measure(s) carried out in another Member State with the purpose of gathering evidence.[106] The EU decided to establish a comprehensive system for obtaining evidence in cross-border dimension cases[107] after some member states complained that existing instruments for sharing evidence constituted a fragmentary regime.[108] These countries submitted an initiative to the EP and the Council on which they proposed a Directive for the EIO. The proposal was officially launched in April 2010,[109] but this was not adopted until April 2014.[110] It is based on Article 76(2) TFEU and binds all member states except for Denmark and Ireland.[111]

The current ways of obtaining evidence from abroad are either by *commission rogatoires* or letters of request.[112] As seen above, MLA procedures have often been criticised for being slow and inefficient. In this sense, the EIO has partially replaced those systems of criminal evidence-exchange by integrating them into a single, efficient and flexible instrument for obtaining evidence. Based on the mutual recognition principle, it facilitates judicial cooperation, simplifying the procedure through a single instrument, and helping national law enforcement agencies become more effective in the combat of cross-border crime.[113]

As regards the types of data processed, the EIO applies to almost all investigative measures,[114] regardless of the type of evidence.[115] It includes bank data, phone records,

---

[105] Council of the European Union, 15196/13, 25.10.2013, pp. 16, 17 and 22.
[106] Council of the European Union, 9145/10, 29.04.2010, Article 1.
[107] Council of the European Union, 9145/10, 29.04.2010; see also the European Commission, Communication on delivering an Area of Freedom, Security and Justice for Europe's citizens: Action plan implementing the Stockholm Programme, COM(2010) 171, Brussels, 2010(a), para. 3.1.1.
[108] Belgium, Bulgaria, Estonia, Spain, Austria, Slovenia and Sweden.
[109] OJ C 165, 24.6.2010, p. 22. Before that, the Commission published a Green Paper. See COM(2009) 624 final, COM(2009) 624 final.
[110] OJ L 130, 01.05.2014, pp. 1-36.
[111] Recitals 44 and 45 of the EIO Directive.
[112] Sayers 2011, p. 1.
[113] Whitehead T & Porter A 2010, 'Britons to be spied on by foreign police', *Telegraph*, 26.07.2010. Available from http://www.telegraph.co.uk/news/uknews/law-and-order/7909314/Britons-to-be-spied-on-by-foreign-police.html [24 October 2014].
[114] Except for two types of interceptions of telecommunications for which complex rules are provided in articles 18-22 of the 2000 EU MLA Convention.
[115] This differs from the EEW, whose scope is limited to specific types of 'object[s], documents and data'.

DNA, statements from suspects or witnesses, the interception of communications, analyses of documents, and fingerprints, to name but a few.[116] Moreover, the EIO Directive is not only used to exchange existing evidence, but it also shares information that does not yet exist but might be necessary for an investigation. For example, France requests that Spain monitors certain suspects in real time, or asks it to obtain DNA samples and fingerprints.[117] The evidence does not exist yet, but this activity can still be requested through an EIO.

In conclusion, the growth of global terrorism in the last fifteen years has entailed the creation of several data-sharing instruments within the EU borders. These multilateral instruments coexist with the MLA procedures and they have the purpose of establishing better cooperation in the exchange of criminal information among member states. Leaving aside the debated added value of these instruments in practice,[118] the next section identifies their shortcomings in the terms of their implementation and use.

## 2.3. Shortcomings in the implementation and use of EU legal instruments for exchanging criminal information

The Swedish initiative, the Prüm Decisions, the ECRIS Decisions and the EIO initiative aim at facilitating the exchange of criminal information among police and judicial agents. However, these instruments have presented two main problems in practice: an enormous delay in their implementation, and confusion regarding how and when these systems should be used.

### *2.3.1. Delay in the implementation*

There is a general transposition failure among member states associated with the EU counter-terrorism measures.[119] This problem has been apparent in all aforementioned

[116] Articles 24-27 of the EIO Directive.
[117] Mangiaracina 2014, p. 120.
[118] There are some scholars who believe that the EU offers a very little added value to the existing security measures of its member states. In this sense, see Bossong RS 2008, 'The Action Plan on combating terrorism – A flawed instrument of EU security governance', *Journal of Common Market Studies,* vol. 46 no. 1, pp. 27-48; Coolsaet R 2010, 'EU counterterrorism strategy: value added or chimera?', *International Affairs*, vol. 86, no. 4, pp. 857-873; Bures 2011.
[119] Argomaniz J 2010, 'Before and after Lisbon: legal implementation as the 'Achilles heel' in EU counter-terrorism?', *European Security*, vol. 19, no. 2, pp. 297-316.

EU data-sharing instruments except for the EIO Directive, which member states have time to transpose until 22 May 2017.[120]

Several member states have not yet implemented the Swedish initiative.[121] In September 2014 the Council released new guidelines for accelerating the implementation process and use of this system. Member states were requested to fill out a factsheet with the list of information that is directly accessible to their national law enforcement authorities, other authorities, and private entities. Information that requires a prior court order to be accessed, the languages used, Single Point of Contact (SPOC) and their contact details were also requested. That information was communicated by 1 October 2014,[122] but the implementation process in these countries is not yet finalised.

In the case of the Prüm Decisions, although all member states have now legally transposed them the system is not yet fully operational. In particular, a few member states have not yet installed the Combined DNA Index System (CODIS) 7.0 for DNA data searches system,[123] and none of them have it up and running.[124] The same occurs with the Automated Fingerprint Identification System (AFIS) for fingerprints, which is only partially operational in all member states.[125] The European Car and Driving License Information System (EUCARIS) for vehicle registration data searches is more successful that the previous two programmes, but in only thirteen countries is it fully active.[126] Lastly, member states had to send a data protection questionnaires to the Council before the implementation of Prüm,[127] but only nineteen of the twenty-eight member states have submitted them to date.[128]

With regard to ECRIS, all member states implemented the system by April 2012, but many of them still lack the technical infrastructure to connect their criminal records

[120] Article 36 of EIO Directive.
[121] In the last document published by the Council Austria, Belgium, Greece, Italy, Ireland, Luxembourg, Malta and United Kingdom had not yet implemented the system. Council of the European Union, 7146/13, 26.03.2013, p. 2.
[122] Council of the European Union, 13034/14, 17.09.2014.
[123] This is the case of Ireland and the UK. The latter has not implemented it since Prüm is not on the opt-in list of TFEU, Protocol No 36, Title VII, article 10, on transitional provisions.
[124] Annex 3 of Council of the European Union, 5124/4/14 REV 4, 27.06.2014, pp. 12-16. For the specific problems faced by each Member State, see Jones 2012.
[125] Annex 4 of Council of the European Union, 5124/4/14 REV 4, 27.06.2014, pp. 18-21.
[126] These are Belgium, Bulgaria, Denmark, Spain, France, Lithuania, Luxembourg, Hungary, The Netherlands, Austria, Poland, Romania, Slovenia, Slovakia, Finland and Sweden. See Annex 5 of Council of the European Union, 5124/4/14 REV 4, 27.06.2014, pp. 23-25.
[127] Chapter 6 of Council Decision 2008/615/JHA.
[128] Annex 2 of Council of the European Union, 5124/4/14 REV 4, 27.06.2014, p. 11.

systems.[129] In order to fix this, in October 2014 the Council released guidelines describing ECRIS technical specifications to be followed by member states.[130] Moreover, the system might change in the near future, since the Commission is considering adding a supplementary index in the programme that stores criminal records from non-EU nationals who have committed crimes in a member state.[131]

There are many factors that explain the lack of implementation and usage of the EU information systems. Some of the reasons given include: the absence of political will, the existence of institutional weaknesses in some countries, and the fact that before Lisbon the Commission had no control over these measures because they were part of the third pillar.[132]

Particularly, the lack of political will is the main cause of the slow transposition of a counter-terrorism measure. Not all member states see the establishment of law enforcement measures as a priority at national level. In fact, even the member states that feel most threatened by terrorism do not always implement those measures on time.[133] Another additional problem is the lack of institutional resources. Some member states do not have the adequate structures to make the systems fully operational. For instance, in June 2014, only three member states (Denmark, Ireland and the UK) had national legislations on the establishment of DNA databases in the terms of Prüm.[134] Other member states lack the personnel training necessary to use these instruments.[135] All of these problems can be seen as part of domestic structural deficiencies.

[129] In 2012 the interconnection software necessary for using the system was only used by 23 member states. See Council of the European Union, 8327/12, 02.04.2012, p. 2.
[130] Council of the European Union, 14264/14, 17.10.2014; Council of the European Union, 14266/14, 17.10.2014; Council of the European Union, 14269/14, 17.10.2014.
[131] Available from https://e-justice.europa.eu/content_criminal_records-95-en.do [31 October 2014].
[132] COM (2012) 732 final, 07.12.2012, p. 4; COM(2012) 735, 07.12.2012, p. 8; Jones C 2012, 'Complex, technologically fraught and expensive - the problematic implementation of the Prüm Decision', *Statewatch Analysis*, p. 3. Available from www.statewatch.com [31 October 2014]; Argomaniz 2010, p. 306.
[133] Argomaniz 2010, p. 308.
[134] Annex 3 of Council of the European Union, 5124/4/14 REV 4, 27.6.2014, pp. 12-16.
[135] See the initiative launched by Estonia, Latvia, Lithuania and Poland on this issue: 'Implementation of PRUM decisions. Preparation for the joint police operations in Estonia, Latvia, Lithuania and Poland' Available from http://www.statewatch.org/news/2013/oct/ee-lv-lt-pl-prum-jpos.pdf [31 October 2014].

### *2.3.2. Complexities in the usage*

Many scholars have identified a lack of coherence in many aspects relating to the current EU counter-terrorism policy,[136] which includes inconsistencies among instruments like the Swedish initiative, the Prüm Decisions the ECRIS Decisions and the EIO initiative. It is probable that after they are fully implemented, their use by law enforcement authorities might still be confusing. The reason is that these legal tools have been designed to complement each other but sometimes their functionalities may overlap. This will cause uncertainty for the national authorities about when to use the particular instrument. The risk is that national police forces decide to use informal mechanisms of communication instead, in a way to circumvent the complexities of the existing EU instruments.

A first difficulty detected in these legal systems refers to the channels used for exchanging the information. Some of the systems incorporate new channels, but not all. For instance, the Swedish initiative takes place via the existing channels for international law enforcement cooperation, and the choice of channel is left to the member states.[137] Annex B of the decision mentions ENU/Europol Liaison Officers, Interpol National Central Bureau (Interpol NCB), SIRENE and Liaison Officers, but other options such as mutual assistance channels can be used. Similar channels are offered in the Prüm Decisions: Europol Liaison Officer, Interpol NCB, Sirene and bilateral Liaison Officers.[138] In contrast, in ECRIS the interconnection among national law enforcement authorities is carried out via the Commission's s-TESTA (Secured Trans European Services for Telematics between Administrations) network – which is a common communication infrastructure providing an encrypted network.[139] Finally, in the case of the EIO, various options for channels are available, since data can be transmitted from the issuing authority to the executing authority 'by any means capable of producing a written record'.[140]

---

[136] Eckes C 2011, 'The legal framework of the European Union's counter-terrorist policies: full of good intentions?' in *Crime within the AFJS: A European Public Order*, Cambridge University Press, Cambridge, pp. 127-158; Argomaniz 2012a, 'A coordination nightmare. Institutional coherence in European Union Counterterrorism' in *European Homeland Security. A European Strategy in the making?*, eds. C Kaunert, S Leonard & P Pawlak, Routledge, New York City, pp. 72-93.
[137] Commission Staff Working Paper, SEC(2011) 593, 13.05.2011, p. 7.
[138] COM (2012) 732 final, 07.12.2012, p. 7. Europol Liaison Officer and Sirene are analysed below.
[139] Council Decision 2009/316/JHA, p. 3.
[140] Article 7 EIO Directive.

Some member states will use the European Judicial Network (EJN) as a channel.[141] The EJN consists of a secure telecommunication system that prevents or minimises the risk of inappropriate access to personal data,[142] and provides contact points that establish direct connection between the issuing and executing authorities involved.

Therefore, too many channels are available. In this regard, the Council is currently working on setting up a Single Point of Contact (SPOC) in every Member State for international law enforcement information exchanges. SPOCs seek to improve the use of all these existing platforms for exchanging information, by constituting a 'one stop shop' for all of them. The SPOC will manage under the same structure the Europol National Unit (ENU), the Interpol National Central Bureau (NCB), the SIRENE Bureau, the foreign liaison officers, the Swedish Framework Decision, the Prüm Decisions, and the regional/bilateral contact points. It will also access databases of SIS, VIS, Eurodac, CIS, Europol (SIENA), Interpol, etc., and will be the unit in charge of replying to any international request sent to the Member State.[143]

In conclusion, this section has detected shortcomings in the implementation and use of the EU data-sharing systems, which are negatively affecting the EU multilateral cooperation in the AFSJ. The correct use of the measures is only possible after all member states fully implement them. Because of the challenges mentioned above, several member states have opted for exchanging criminal records through other traditional/CoE MLA procedures discussed above. MLA procedures are particularly attractive to law enforcement authorities because they allow free-text exchange of messages subject to lower levels of scrutiny.[144] However, as seen above, this procedure entails many problems regarding the efficiency and duration. Law enforcement authorities have also opted for exchanging data through regular email accounts or phone calls. A clear example of this practice was the communication between France and Spain in the past during investigations into the Spanish terrorist group ETA. None of the

[141] Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network, OJ L 348, 24.12.2008, pp. 130-134; Recital 13 and 7(4) of EIO Directive.
[142] Opinion of the European Data Protection Supervisor on the initiatives for a Directive of the European Parliament and of the Council on the European Protection Order and for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters, 05.10.2010, p. 9.
[143] Council of the European Union, 6721/14, 20.02.2014; Council of the European Union, 10492/14, 13.06.2014.
[144] Vermeulen M & Wills A 2011, 'Parliamentary oversight of security and intelligence agencies in the European Union', *European Parliament, Directorate General for Internal Policies, Policy Department C, Citizens' rights and Constitutional Affairs*, Brussels, p. 17.

EU provisions on cross-border policing precluded bilateral arrangements.[145] Thus, these two countries did not use any EU channel for exchanging information, nor did they involve any EU agency such as Europol or Eurojust. This is even more problematic since crime-related information is not exchanged through secure channels, meaning it can also be easily intercepted and exposed.

## 3. Expanding the information sources of member states: Data collected for non-criminal reasons but ultimately used for law enforcement

As pointed out by Hijmans & Scirocco, 'information tends to be used if it exists'.[146] The EU has gradually increased the number of information systems and databases accessible to law enforcement authorities. Particularly, the EU has amended legislation regulating the collection of personal data for commercial and border management purposes to allow the law enforcement sector to process such data. When personal data collected for one specific purpose is further accessed or processed for another purpose, this might infringe the 'purpose limitation principle'. This principle is included in Article 5(b) of 108 CoE Data Protection Convention,[147] Article 6(1)(b) of Directive 95/46/EC and Article 3 of EU Framework Decision 2008/977/JHA.[148] The following sections examine the systems and databases through which the EU has gradually widened the use of personal information for law enforcement purposes.

### 3.1. European information systems created for border management purposes

In November 2010 the Commission released a Communication on a comprehensive approach on personal data protection in the EU.[149] The communication discerned twenty different AFSJ actors dealing with the collecting and processing of personal data at the EU level. The list included the following European Information Systems: Schengen Information Systems (SIS/SIS II), Visa Information System (VIS), Customs

[145] Bi-lateral arrangements had their own security arrangements and mechanisms, outsite the scope of the EU.
[146] Hijmans H & Scirocco A 2009, 'Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?', *Common Market Law Review*, vol. 46, no. 5, p. 1491.
[147] Council of Europe, 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.01.1981.
[148] This Convention is examined in Chapter 5 of this thesis.
[149] COM(2010) 609 final, 04.11.2010.

Information System (CIS) and Eurodac. All of these were originally created for border control purposes; yet, terrorist attacks that have occurred in the last ten years have caused a shift in the use of these systems. This section examines how data collected by SIS, VIS, CIS and Eurodac can be now processed for law enforcement purposes too.[150]

### *3.1.1. Background*

The Schengen Information System (SIS) has its origins in the Schengen Agreement concluded in 1985. It regulated the control of member states' external borders, and the third-country nationals entering the EU territory. At first, only five member states signed the agreement: Belgium, France, the Netherlands, Luxembourg and West Germany. These member states implemented the agreement through the 1990 Schengen Agreement Application Convention (SAAC).[151] From that moment, they became part of the Schengen Area. This area was established to abolish internal checks and create a common external border, reinforcing the security measures to combat illegal immigration.[152] The SAAC included a chapter referring to Schengen Information System (SIS) and the Supplementary Information Request at the National Entry Bureaux (SIRENE). SIS consisted of a joint information system composed by national sections of each Member State that could rapidly and effectively transfer data relating to border checks and movement of persons to a central database. SIRENE was the channel used to exchange information.

SIS came into operation in 1995.[153] Its purpose is to strengthen the cooperation between immigration, police and custom authorities[154] for the maintenance of public order and State security.[155] Member states have the possibility to issue an alert on people a) wanted for arrest, b) in connection with police investigations or criminal proceedings, and c) to be refused entry to the entire Schengen area. It also informs on lost or stolen

[150] Other envisaged systems like the Enty/Exit system and the Registered Traveller Programme might also be used for law enforcement purposes in the future. However, since they are not yet in force they are not part of this study.
[151] Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic, on the Gradual Abolition of Checks at their Common Borders ("Schengen Implementation Agreement"), 19.06.1990. Available from: http://www.refworld.org/docid/3ae6b38a20.html [1 November 2014].
[152] Article 17 of Schengen Agreement.
[153] Articles 92-119 SAAC.
[154] Article 92 SAAC.
[155] Article 93 SAAC. The concept and scope of 'State security' or 'national security' is discussed in chapter 4 of this thesis.

vehicles, firearms, identity documents and bank notes.[156] Searches through SIS produce a 'hit', which specifies the action to be taken against the person who is denied the entry to the Schengen area.[157] There are currently more than 41,000 individuals included in SIS, and the system produces more than 1,000 hits every month.[158] It is worth adding that, as a result of the Paris attacks of 7 January 2015, the Commission has released a new proposal for a regulation of the Schengen Border Code that will intensify the police controls at the borders, for both EU and non-EU citizens.[159]

With respect to the Visa Information System (VIS), established in 2004 by Council Decision 2004/512/EC (2004 VIS Decision),[160] it aimed at supporting the EU common visa policy by establishing a common identification system for data on short-stay visas among member states. VIS is based on a centralised system called the Central Visa Information System (CS-VIS), connected to an interface in each member state (the National Interface (NI-VIS)) via the communication infrastructure[161] between the CS-VIS and the NI-VIS.[162] In order to implement the 2004 VIS Decision a regulation was adopted in 2008.[163] That new instrument stated that the main objectives of VIS were: i) to facilitate the visa application procedure, ii) to prevent 'visa shopping', iii) to facilitate the flight against fraud, iv) to facilitate checks at external border crossing points between member states, v) to assist in the identification of any person who may not fulfil the requirements for entry or stay on the territory of member states, vi) to facilitate the application of Dublin II Regulation,[164] and vii) to contribute to the prevention of threats to the internal security of any of the member states.[165]

VIS did not become operative until 2011.[166] It processed one million visa applications during the first year,[167] and more than four million during 2012-2013.[168]

---

[156] Article 95-100 SAAC.
[157] Hayes B & Vermeulen M 2012, *Borderline. The EU's new border surveillance initiatives assessing the costs and fundamental rights implications of EUROSUR and the "Smart Borders" proposals*, Heinrich Böll Foundation, Berlin, p. 31.
[158] 'Schengen Information System: 41,000 people subject to 'discreet surveillance or specific checks', *Statewatch*, 09.09.2014. Available from http://statewatch.org/news/2014/sep/sis-stats.htm [1 November 2014].
[159] COM(2015) 8 final, 20.01.2015.
[160] OJ L 213, 15.06.2004, pp. 5-7.
[161] The VIS and the SIS II share the same communication system (the European Commission's s-TESTA) and the same handling system for biometrics (the Biometric Matching System, specifically tailored for them). See Bigo et al. 2012, p. 21.
[162] Article 1(2) 2004 VIS Decision.
[163] OJ L 218, 13.08.2008, pp. 61-81.
[164] Regulation (EC) No 343/2003.
[165] Article 2 of VIS Regulation.
[166] 'More efficient and secure visa system goes live', European Commission Press Release, 11.10.2011.

The system is rapidly expanding year by year. In 2012 and 2013 it enhanced its competence to cover the entire African continent, the Near East, the Gulf Region; and it expects to cover the entire world by the end of 2015.[169]

The Customs Information System (CIS) has its origin in the Convention on the use of information technology for customs purposes,[170] and the convention on mutual assistance and cooperation between customs administrations.[171] These were created to combat smuggling. CIS was signed in 1995 but it did not come into force until 2005, after being ratified by all member states. The convention was replaced by a regulation adopted under the scope of the first pillar.[172] It regulated the collection of information on persons for the specific purposes of sighting and reporting, discreet surveillance and specific checks. CIS was thus used if there was enough evidence suggesting that the target has committed, is committing or will commit actions in breach of customs or agricultural legislation.[173]

Regarding the asylum seekers' data, in 1995 a convention determining the state responsible for examining applications for asylum in one of the member states of the former European Communities (Dublin Convention)[174] was signed. The examination was conducted through a centralised system that compared the asylum applicants' fingerprints. It was called Eurodac and its main purpose was to assist in determining which member state was responsible for examining an application for asylum. At the same time, it also prevented cases of asylum shopping[175] and refugees in orbit.[176] Eurodac was first regulated in 2000 by a council regulation[177] binding those countries that had implemented the Dublin *acquis* – namely, all member states plus the EFTA

---

[167] 'European Commission deploys Visa Information System developed by Steria-led consortium', STERIA Press Release, 10.09.2012. Available from http://www.steria.com/your-business/homeland-security/homelanddetail/article/european-commission-deploys-visa-information-system-developed-by-steria-led-consortium/ [1 November 2014].

[168] Council of the European Union, 7996/14, 21.03.2014, p. 3.

[169] Council of the European Union, 7996/14, 21.03.2014, pp. 3-4; Council of the European Union 5731/15, 30.01.2015.

[170] Council Act 95/C316/02 of 26 July 1995 drawing up the Convention on the use of information technology for customs purposes. OJ C 316, 27.11.1995, pp. 33–47.

[171] OJ C 24, 23.01.1998, pp. 1-22.

[172] OJ L 218, 13.08.2008, pp. 48-59.

[173] Data in the field of agriculture refer to imported goods; businesses; goods detained, seized or confiscated; etc.

[174] Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, Dublin, 15.06.1990.

[175] *Asylum shopping* is when multiple asylums applications are submitted simultaneously or successively by the same person in several member states.

[176] *Refugees in orbit* refers to a situation in which all member states claim not to be responsible for examining an asylum application.

[177] OJ L 316, 15.12.2000, pp. 1-10.

states.[178] Eurodac started its operations in 2003 and it established a centralised system that connected all twenty-eight national access points.

### *3.1.2. Shift from border control to law enforcement purposes*

What the above-mentioned systems have in common is that they eventually altered their original objectives, becoming today effective tools in the prevention, detection and investigation of crimes, in addition to their original roles. This change was a direct consequence of the 9/11 attacks,[179] since before 2001 very few EU instruments for exchanging migrants' data were used for law enforcement purposes.[180] This tendency emerged in 2005, the year in which SIS/SIS II, VIS, and CIS started to expand their initial purposes.

In December 2014, the Commission recommended intensifying the use of SIS by custom and law enforcement authorities for persons trying to enter the Schengen area.[181] However, law enforcement's access to the SIS is not new. In 1990, the SAAC introduced the possibility for police authorities to access data collected by the visa part of the system.[182] Later, the EU adopted two new legislative measures that granted competence to law enforcement authorities: Council Regulation 871/2004[183] and Council Decision 2005/211/JHA.[184] Europol also gained access to a limited amount of data entered into SIS.[185]

However, SIS was a system with limited capabilities, since it could only technically serve a maximum of eighteen countries. Because of the number of entries in the system was increasing every year,[186] the EU expressed the need to develop a second generation SIS (SIS II), which would incorporate the latest developments in the field of information technology.[187]

---

[178] Iceland, Norway, Switzerland and Liechtenstein. See OJ L 93, 03.04.2001, pp. 40-46; OJ L 53, 27.02.2008, pp. 1-2; and OJ L 160 18.06.2011, pp. 37-49.
[179] Baldaccini A 2008, 'Counter-Terrorism and the EU strategy for border security: Framing suspects with biometric documents and databases', *European Journal of Migration and Law*, vol. 10, no. 1, p. 39.
[180] For instance, Council Decision 2000/261/JHA of 27 March 2000, OJ L81, 01.04.2000, pp.1-3.
[181] Council of the European Union, 16880/14, 18.12.2014.
[182] Article 39(1) and 46 SAAC.
[183] OJ L 162, 30.04.2004, pp. 29–31
[184] OJ L 68, 15.03.2005, pp.44-48.
[185] Article 1(3) Council Regulation 871/2004 and Article 1(8) Council Decision 2005/211/JHA.
[186] It registered more than 42 million entries by January 2012. Council of the European Union, Note from the French Delegation – Document 8281/12, 28.03.2012.
[187] Recital 2 Council Regulation 871/2004 and Recital 2 Council Decision 2005/211/JHA. See also Hayes B 2004, 'From the Schengen Information System to SIS II and the Visa Information (VIS): the proposals

SIS II was first proposed as a package by the Commission on 31 May 2005[188] and adopted in December 2006[189] (SIS II Regulation) and June 2007 (SIS II Decision).[190] However, before the new system was completed, Portugal proposed a transitional system called 'SISone4all' that would enable the inclusion of the new member states. The system was temporarily called 'SIS 1+' and it was regulated in Council Decision 2008/839/JHA[191] and Commission Regulation 1104/2008.[192] Three years later, the Commission launched a recast proposal[193] on migration from SIS 1+ to SIS II, and SIS II finally became operational in April 2013.

The SIS II Decision[194] seeks to ensure a higher level of security within the AFSJ, by improving the conditions and procedures for alerts with respect to third-country nationals, as well as the exchange of supplementary information for the purpose of refusing their entry into a member state.[195] SIS II also introduces the possibility to gather biometric data, such as fingerprints and photographs,[196] from persons wanted for arrest, missing persons, persons sought to assist with judicial procedures (e.g. witnesses), and persons subject to discreet checks.[197] SIS II has a capacity of 100 million alerts and it is composed of three systems:[198] a) a central system (CS-SIS II), b) a national system (NI-SIS II) in each member state, and c) a communication infrastructure between C-SIS II and NI-SIS II, via SIRENE Bureaux. Each Member State has a SIRENE Bureau. If an alert is sent, supplementary information might be supplied through this channel.[199]

Regarding visa information, 2008 Council Decision[200] enhances Article 3 of the previous VIS Regulation by allowing law enforcement authorities to access VIS data.[201]

---

explained', *Statewatch Analysis*, p. 17. Available from http://www.statewatch.org/news/2005/may/analysis-sisII.pdf[1 November 2014].

[188] COM (2005) 236, COM (2005) 237, and COM (2005) 230, 31.05.2005.

[189] OJ L 381, 28.12.2006, pp. 1-23.

[190] OJ L 205, 7.8.2007, pp. 63-84.

[191] OJ L 299, 8.11.2008, pp. 43–49. It was later amended by Council Regulation (EU) 541/2012.

[192] OJ L 275, 16.10.2008, pp. 37-41. It was later amended by Council Regulation (EU) 542/2010.

[193] COM(2012) 81, 30.04.2012.

[194] Council of the European Union, 7215/13, 7/8.03.2013, p. 11.

[195] Article 2 SIS II Regulation; Article 4 SIS II Decision.

[196] Articles 20(2)(e) and (f) SIS II Regulation and SIS II Decision.

[197] Article 35 SIS II Decision.

[198] SIS II Regulation, recital 7 and Article 4.

[199] SIS II Regulation, Article 7; SIS II Decision, Article 7.

[200] Council Decision 2008/633/JHA, OJ L 218, 13.08.2008, pp. 129-136.

[201] It is worth highlighting that Ireland and the UK were excluded from the access to VIS data for law enforcement purposes. This was because neither of the countries is part of the Schengen area. In the case C-482/08, the UK unsuccessfully challenged such exclusion, with the CJEU ultimately deciding that there

Besides immigration and asylum authorities, and authorities responsible for carrying out checks at external border crossing points, 2008 Council Decision granted access to national law enforcement authorities, Europol, as well as third countries or international organisations. These bodies gained access on 1 September 2013.[202]

CIS data is also used for law enforcement purposes today. Besides the 'traditional' CIS, established by the above-mentioned first pillar Regulation (EC) 766/2008, a Council decision within the scope of the third pillar was adopted in 2008 (hereinafter, the CIS Decision).[203] The main purpose of the CIS Decision is 'to assist in preventing, investigating and prosecuting serious contraventions of national laws by making information available more rapidly'.[204] According to Article 5 of the CIS Decision, data entering into CIS is to be used by law enforcement authorities for the purposes of sighting and reporting, discreet surveillance, specific checks and strategic or operational analysis.[205]

The CIS Decision regulates the Customs Files Identification Database (FIDE).[206] FIDE allows national custom authorities, Europol and Eurojust to identify competent authorities of other member states that have investigated cases involving a particular person or business. The information can only be obtained if the case deals with serious crimes within less than twelve months, or with a sanction of at least 15,000 €.[207] The Commission manages the collection of information,[208] including personal data, in the following categories: commodities; means of transport; businesses; persons; fraud trends; availability of expertise; items detained, seized or confiscated; and cash detained, seized or confiscated.[209]

Finally, a proposal for the amendment of the Eurodac Regulation was released by the Commission in December 2008.[210] Nine months later, the Commission, influenced by

---

was no error in leaving both countries out of the scope of the contested council decision. O'Neill 2012, pp. 137-141.

[202] 'Law enforcement authorities to gain access to European visa database on 1 September', *Statewatch*, 3.7.2013. Available from http://www.statewatch.org/news/2013/jul/vis-lea-access.htm [1 November 2014].

[203] OJ L 323, 10.12.2009, pp. 20-30.

[204] Article 1(2) CIS Decision.

[205] Council of the European Union, 16427/1/10, 29.11.2010.

[206] Article 25 CIS Decision.

[207] Article 15(1) CIS Decision.

[208] Article 3(2) CIS Decision.

[209] Article 3(1) CIS Decision.

[210] COM(2008) 825 final, 03.12.2008.

the Council,[211] issued an amendment of this proposal in form of a package – a regulation[212] and a Council decision[213] – introducing the possibility for member states' law enforcement authorities and Europol to access Eurodac's central database for the purposes of the prevention, detection and investigation of serious criminal offences. The proposed Council decision addressed the possibility for law enforcement authorities to cooperate in the exchange of fingerprints. However, with the entry into force of the Treaty of Lisbon, the Commission decided to withdraw the provisions referring to the access for law enforcement purposes from the proposed package, and it presented a new proposal for regulation similar to that of 2008.[214] Yet that proposal was also replaced by a new one in May 2012,[215] which reintroduced the law enforcement provisions into a single instrument. It sought the alignment with the aforementioned SIS II and VIS databases in the identification of suspected perpetrators of terrorist or serious crimes, and was adopted in June 2013,[216] applying to all member states except Ireland and Denmark.[217]

Therefore, the EU has been modifying some of the instruments originally designed to control illegal immigration within the European borders, sharing the information obtained with law enforcement authorities for the prevention and investigation of crimes. It is worth noting that, except for CIS, all other systems are managed by a new EU Agency called the EU Agency for large-scale IT systems (or eu-LISA), which became operative in December 2012. The agency ensures that the information exchanged through such IT systems is secured and complies with the relevant data protection legislation. It also issues periodical reports on technical aspects to the EP and the Council,[218] and annual activity reports to the EU Council Delegations.[219] This centralisation of the management in one single institution is to be viewed with optimism. It will strengthen the relationships between JHA actors, and will increase the consistency among existing data-sharing systems in the field of law enforcement.

[211] Council of the European Union, 5291/07, 12.01.2007; Council of the European Union, 10002/07, 25.05.2007.
[212] COM(2009) 342 final, 10.09.2009.
[213] COM(2009) 344 final, 10.09.2009.
[214] COM(2010) 555 final, 11.10.2010.
[215] COM(2012) 254 final, 30.05.2012.
[216] OJ L 80, 29.06.2013, pp. 1-30.
[217] The UK decided to opt-in to the Eurodac Regulation.
[218] Article 50(3) of VIS Regulation.
[219] See the last annual report at Council of the European Union, 11056/14, 07.07.2014.

### 3.2. EU data-sharing instruments created under the basis of the EU internal market clause

EU measures originally created to control external borders are not the only ones experiencing an expansion of the purposes for which they are used. As the EDPS pointed out '[t]here is now a tendency to require that private actors cooperate with law enforcement authorities on a systematic basis'.[220] This section looks at some of the current private entities' databases that were originally been established within the scope of the internal market provision (Article 114 TFEU). The data they collect was primarily used for commercial reasons, but now it is also used for purposes related to the prevention, detection, investigation and prosecution of a crime. This analysis focuses on three particular cases: i) passenger data collected by EU airline companies, ii) financial data collected by the Belgian company SWIFT, and iii) data collected by European telecommunication and information society services.

#### *3.2.1. Exchange of passenger data within the EU*

More than 1.4 billion passengers pass through EU airports every year.[221] Aviation security has been one of the priorities within the EU internal security policy, seeking to 'keep up with the continuous innovation demonstrated by terrorist groups'.[222] In that sense, the Council adopted the Advanced Passenger Information system (hereinafter, API system or APIS)[223] in 2004, and the Commission proposed the EU Passenger Name Record Directive (hereinafter, EU PNR Directive) in 2011. In order to understand these instruments, it is necessary first to briefly introduce their international counterpart: the EU-US PNR Agreement.[224]

In response to the 9/11 attacks, the US authorities adopted measures that obliged airlines taking off, landing or flying through the US territory to turn over all their flight booking and departure data to the US government. This information is referred to as

---

[220] EDPS Opinion on the Communication from the Commission to the European Parliament and the Council entitled 'Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM), 29.04.2013, p. 5.
[221] Airport Council International. Available from https://www.aci-europe.org/policy/fast-facts.html [2 November 2014]
[222] COM(2013) 179 final, 10.04.2013, p. 8.
[223] OJ L 261, 06.08.2004, pp. 24-27.
[224] A careful assessment of existing PNR agreements, and especially the EU-US PNR Agreement, is carried out in Chapter 2 of the present study.

Passenger Name Record or PNR data. PNR data is defined as a record of the itinerary of a travelling person saved in the database of an airline, usually during the booking process.[225]

The EU-US PNR Agreement was first signed in 2004, after adopting Commission Decision 2004/535/EC[226] and Council Decision 2004/496/EC.[227] The conclusion of the agreement was based on ex Article 95 TEC (the internal market clause)[228] in combination with the implied powers doctrine.[229] The choice of this legal basis was made upon the consideration that the collection of PNR data by private companies was a purely economic activity, necessary for the sale of an airplane ticket. In fact, for decades, airline companies had customarily stored their passengers' personal data in private databases for commercial purposes. It was only after 9/11 that the US authorities began to seize and transfer such data to public databases for the fight against terrorism.

The EP, supported by the EDPS, challenged the decisions before the CJEU. The EP argued that the EU-US PNR Agreement had been adopted under the wrong legal basis since the main objective did not concern the internal market, but a matter of public security and criminal law (third pillar). The CJEU agreed with the EP and in May 2006 it annulled the decisions that enabled the PNR Agreement.[230] The Court observed that even if it were true that data was originally collected for commercial purposes, the use of such data had later changed from private to public hands. The Court found that the main purpose of the agreement was the prevention and combating of terrorism and, therefore, it considered that the measure should fall under the scope of the former third pillar and not as part of the Community law.

The Court's choice to annul the 2004 EU-US PNR Agreement entailed negative consequences for the enforcement of the EU data protection legislation. Subsequent EU-US PNRs adopted in 2006[231], 2007[232] and 2012[233] moved the matter from the first

[225] Hernanz 2011, p. 4.
[226] OJ L 235, 06.07.2004, p. 11.
[227] OJ L183, 20.05.2004, p. 83.
[228] This is not expressly stated in the agreement, which only refers to Directive 95/46/EC as the legal basis.
[229] De Busser 2009, p. 366.
[230] C-317 and 318/04, Parliament v. Council (PNR), 30.05.2006.
[231] OJ L 298, 27.10.2006, pp. 29-31.
[232] OJ L 204, 04.08.2007, pp. 18-25.
[233] OJ L 215, 11.08.2012, pp. 5-14.

pillar (ex Article 95 TEC) to the third pillar (ex-Article 24(1) TEU) and therefore, Directive 95/46/EC was no longer applicable.[234]

Another EU instrument for the identification of passengers was the Advance Passenger Information System (APIS). Parallel to the adoption of the EU-US PNR Agreement, the Council approved a directive[235] obliging air carriers to communicate passenger data from those persons arriving into the EU from third countries. According to the directive, when passengers checked in for a flight, airline companies would collect the full name, gender, date of birth, nationality, country of residence, type of travel document, and the travel document's number. That information would be then transferred to public authorities and retained for twenty-four hours.[236] The APIS was adopted under the first-pillar basis of ex Article 62(2)(a) and Article 63(3)(b) TEC[237] (current Articles 77 and 79 TFEU). These provisions regulate the improvement of border control and the combating of irregular migration. Interestingly, both EU-US PNR Agreement and APIS Directive referred to the European Council Declaration on combating terrorism to justify the obligation of carriers to communicate passenger data.[238] However, the PNR Agreement was a third-pillar instrument while the APIS Directive was part of the Community law. The reason why the second PNR Agreement was not based on ex Articles 62(2)(a) and 63(3)(b) TEC, like APIS, has no clear explanation to date.[239]

The necessity to clarify the real purpose of processing advance passenger information (API) was identified by Article 29 Data Protection Working Party (hereinafter, the Art. 29 WP) in 2006[240] and 2013.[241] Yet, although API collection and processing has led to a few legal disputes related to data protection issues,[242] in general

---

[234] This issue is better assessed in chapter 2 of the present study.
[235] OJ L 261, 06.08.2004, pp. 24-27.
[236] API Directive, Article 6.
[237] Article 62(2)(a) referred to standards and procedures to be followed by member states in carrying out checks on persons at such borders, and Article 63(3)(b) called for measures to combat illegal immigration.
[238] API Directive, recital 2.
[239] Docksey C 2014, 'The European Court of Justice and the decade of surveillance' in *Data Protection Anno 2014: How to restore trust? Contributions in honour of Peter Hustinx European Data Protection Supervisor 2004-2014*, eds. Hielke Hijmans, Herke Kranenborg, Intersentia, Cambridge.
[240] WP 127, 27.09.2006.
[241] Article 29 Data Protection Working Party, Letter addressed to Ms. Cecilia Malmström, Commissioner for Home Affairs, Ref. Ares(2013)2639121, 11.07.2013.
[242] See, for instance, Agencia Española de Protección de Datos, Expediente Nº: E/06406/2012, 20.09.2013.
Available from
http://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/archivo_actuaciones_2013/common/pdfs/E-06406-2012_Resolucion-de-fecha-20-09-2013_Art-ii-culo-33-LOPD.pdf [2 November 2014].

the API Directive has been less controversial than the PNR systems.[243] One reason is the limited number of items collected through APIS, and the short time of data retention. Moreover, the API Directive only requires the transfer of data after a request, whereas PNR agreements oblige the airline companies to systematically transmit data.[244] Lastly, API does not allow any kind of intelligence analysis on the travel patterns, while PNR systems do.[245]

During the negotiations of the PNR agreements, the EP voiced its concerns about the lack of reciprocity on PNR matters. With the adoption of these international agreements, passenger data was transferred from the EU to the US, but not vice versa. The trigger for the initial discussions on the possibility to create an EU PNR scheme was the failed car bomb attacks in London and at Glasgow Airport in June 2007.[246] In November that year, the Commission launched a proposal for a Council framework decision[247] with the aim to:

'[H]armonise Member State's provisions on obligations for air carriers operating flights to or from the territory of at least one Member State regarding the transmission of PNR data to the competent authorities for the purpose of preventing and fighting terrorist offences and organised crime.'[248]

However, in November 2008 the EP refused to issue a formal opinion on the proposal for not granting enough protection for the individual rights.[249] Therefore, in February 2011, the Commission presented a new proposal for an EU PNR Directive, this time with an impact assessment attached.[250] As in the current EU-US PNR Agreement, the main purpose is the prevention, detection, investigation and prosecution

[243] 'API, PNR, threat assessments, and data-mining: Member states push for access to travellers' personal data for customs authorities', *Statewatch*, 22.02.2013.
Available from <http://www.statewatch.org/news/2013/feb/12customs-pnr1.htm> [2 November 2014].
[244] Kaunert C, Léonard S & MacKenzie A 2012, 'The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT', *European Security*, vol. 21, no. 4, p. 486.
[245] Argomaniz J 2009, 'When the EU Is the "Norm-taker": The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms', *Journal of European Integration,* vol.31 no.1, p. 129.
[246] Argomaniz 2009, p. 130.
[247] COM(2007) 654 final, 06.11.2007.
[248] COM(2007) 654 final, 06.11.2007, p. 6.
[249] European Parliament, B6-0615/2008, 20.11.2008.
[250] SEC(2011) 132 and SEC(2011) 133 final, 02.02.2011.

of terrorist offences, serious crimes,[251] and serious transnational crimes. Unlike the 2004 EU-US PNR Agreement, the EU PNR Directive is based on Articles 82(1)(d) and 87(2)(a) TFEU and its main purpose is the prevention, combat and investigation of crimes.[252] Thus, we can observe a change in the purpose for collecting passenger data in the 2004 EU-US PNR Agreement and the APIS, and this EU PNR Directive.

The proposed EU PNR Directive also shows that the Commission has not always been consistent in the choice of legal basis for measures that regulate the exchange of information in the field of transport. On 6 May 2014, the CJEU decided to annul Directive 2011/82/EU facilitating the cross-border exchange of information on road safety related traffic offences.[253] That directive had been adopted under the legal basis of Article 87(2) TFEU, which is the same one used in the proposal for the EU PNR Directive. However, the Court agreed with the Commission that the main purpose of the instrument was to improve transport safety in the sense of Article 91(1)(c) TFEU, rather than to generally exchange information for criminal matters, as establishesd by Article 87(2) TFEU.[254] Accordingly, one month after the ruling, the Commission launched a new proposal – this time based under Article 91 TFEU.[255]

The EU PNR Directive could also have been adopted under Article 91 TFEU. Both Directive 2011/82/EU and the EU PNR Directive are internal instruments consisting of the exchange of cross-border information collected by transport companies (air and road transport) aiming at increasing the police cooperation, as well as the passenger safety. If the EU PNR Directive was based on Article 91 TFEU, data-sharing activities would fall within the scope of Directive 95/46/EC, and the UK, Ireland and Denmark could not opt-out of the Directive.

As it stands now, the EU PNR Proposal allows the collection of up to nineteen categories of data from both EU and non-EU citizens by airline companies at the moment of the ticket purchase. These will be sent to specific Passenger Information Units (PIUs) in the Member State prior the flight departure.[256] The PIUs will be in

---

[251] Pursuant to Article 2(2) of Council Framework Decision 2002/584/JHA, punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State.
[252] COM(2011) 32 final, 02.02.2011.
[253] OJ 2011 L 288, 25.10.2011, pp. 1-15.
[254] C-43/12, 06.05.2014.
[255] COM(2014) 476 final, 18.07.2014.
[256] Bellanova R & Duez D 2012, 'A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage', *European Foreign Affairs Review* vol. 17, no. 1/2, p. 115.

charge of cross-checking the data for predetermined criteria. In the case of a positive match, the specific data will be evaluated. Data will be encrypted from the moment they are collected by airline companies. It will be then stored in the specific PIU for five years. The goal is that, during that period of time, such data will produce information linked to subsequent passengers.[257] On the substance of the instrument, it is unclear whether it will apply exclusively to flights entering and leaving the EU, or also to intra-EU flights.[258] Likewise, it is unconfirmed that data collected will only belong to air passengers entering the EU, or whether it will also include persons arriving by boat, railway or vehicles.[259] In addition, questions as to the quality of encryption, the data subject's right of access, and the role of the data protection authorities[260] are still on the table.

The EP was doubtful about the necessity of collecting data from all types of passengers – suspects and non-suspects. Therefore, in April 2013 the proposal was rejected by the European Parliament Civil Liberties Committee (LIBE)[261] and, consequently, the EP suspended its voting in 2014.[262]

However, the terrorist attacks that occurred in Paris on 7 January 2015 revived the debate as to the necessity for an EU PNR system to combat terrorism. In order to prevent member states from installing national PNR regimes or the Commission from launching a new proposal,[263] the LIBE Committee finally suggested amendments on the 2011 proposal.[264] Among them, it suggests replacing the broad concept of 'serious

---

[257] Bellanova & Duez 2012, p. 120.

[258] 'EU Eyes Massive Collection of Air Passenger Data', *SpiegelOnline*, 12.10.2012. Available from http://www.spiegel.de/international/europe/european-parliament-to-debate-own-database-for-flight-passengers-a-871953.html [2 November 2014].

[259] 'API, PNR, threat assessments, and data-mining: Member states push for access to travellers' personal data for customs authorities', *Statewatch*, 22.02.2013. Available from <http://www.statewatch.org/news/2013/feb/12customs-pnr1.htm> [2 November 2014].

[260] Bellanova & Duez 2012, p. 120.

[261] Civil Liberties Committee rejects EU Passenger Name Record proposal, Commission Press Release, 24.04.2013. Available from http://www.europarl.europa.eu/pdfs/news/expert/infopress/20130422IPR07523/20130422IPR07523_en.pdf [2 November 2014].

[262] This was first delayed in June 2013 and later suspended due to the NSA scandal in the US. See Jennifer Baker, 'European Parliament delays vote in sharing passenger data with US authorities', *Netscaler*, 11.06.2013. Available from http://www.networkworld.com/news/2013/061113-european-parliament-delays-vote-on-270689.html [2 November 2014].

[263] 'EU PNR – the way forward. Following the Orientation Debate of 21 January 2015 on the European Agenda on Security', Commission, leaked on 28.01.2014.

[264] Committee on Civil Liberties, Justice and Home Affairs, 'Draft Report on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)0032 – C7-0039/2011 – 2011/0023(COD))', PE549.223v01-00. Rapporteur: Timothy Kirkhope, 17.02.2015.

crimes' for 'serious transnational crimes', retaining data for only four years in cases of serious transnational crimes, collect data for intra-EU flights, and enhancing the conditions for transferring PNR data to third countries. The PE will vote on these amendments on 25 March 2015.

### *3.2.2. Exchange of financial data within the EU*

Law enforcement authorities of the member states also expressed interest in accessing EU citizens' financial data. In 2000, a Council decision on the cooperation between financial intelligence units of the member states for exchanging information was adopted.[265] Yet, the creation of an EU system for the exchange of financial data was postponed in 2001 due to the 9/11 attacks: at the time the exchange of financial data between the US and the EU was the priority.

In December 2001, two Europol-US agreements were concluded for the exchange of information related to global financial movements.[266] They were part of the so-called Terrorist Finance Tracking Program (TFTP), established in secret by the Bush Administration to pull EU citizens' data from a private company, the Society for the Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT was based in Belgium, but the US authorities were able to access the data because it also had servers located in the US. Thus, depending on where the EU citizens' data was being processed, the company had to comply with either Belgian national laws implementing Directive 95/46/EC (first pillar)[267] or US laws. In this sense, the company always processed EU citizens' data through its servers located in the US in order to avoid potential clashes with European laws.

The TFTP was uncovered in 2006 by the New York Times.[268] It created a big debate within the EU and as a result SWIFT decided to move all of its servers completely to

[265] OJ L 271, 24.10.2000, pp. 4-6.
[266] 'Agreement between the United States of America and the European Police Office', 06.12.2001; 'Supplemental agreement between the Europol Police Office and the United States of America on the exchange of personal data and related information', 20.12.2002.
[267] Transfers originally responded to 'commercial purposes' and therefore they fell under the scope of the internal market clause.
[268] Eric Lichtblau & James Risen, 'Bank data is sifted by U.S. in secret to block terror', *The New York Times*, 23.06.2006.
Available from http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=all [2 November 2014].

the territory of the EU member states.[269] Since financial data from EU citizens were now processed on EU soil, the company had to comply with EU data protection laws. Consequently, the Commission urged the drafting of an agreement enabling data transfers from the EU to the US.

In the EU the only instrument for the prevention and combat of terrorist financing was Directive 2005/60/EC.[270] It was introduced as a consequence of the Madrid attacks and it obliged financial institutions within the EU to control and store their clients' data. If any suspicious transaction was noticed, it was to be communicated to the designated authorities. Nevertheless, that directive raised concerns about data protection, transparency and accountability rights.[271] Also, the fact that the banks were responsible for detecting terrorist transactions made the system quite ineffective since, clearly, the banks' primary mission is not related to national security.[272]

On 30 November 2009, the SWIFT Agreement came into force. The agreement was adopted under the scope of the ex-third pillar, with a combined legal basis of former Articles 24 and 38 TEU. The SWIFT Agreement was provisionally applied after signature, but this was then abrogated after the negative EP vote in February 2010.[273]

In the summer of 2010, a second SWIFT Agreement (SWIFT II) was adopted. One of the changes it included was the future creation of an EU programme equivalent to the US TFTP, called the European Terrorist Finance Tracking System (TFTS). In 2015, the scope and features of this system are still unclear. The only thing that is known is that the main goal of the TFTS will be to restrict the amount of bulk information that the US selects, processes and decrypts, by setting a control on EU soil. Likewise, the system seeks to increase the EU contribution to the detection of terrorist financing,[274] gaining autonomy from the US leads.

---

[269] Cremona M 2011, 'Justice and Home Affairs in a globalised world: Ambitions and reality in the tale of the EU-US SWIFT Agreement', *Austrian Academy of Sciences, Institute for European Integration Research,* Working Paper No. 04/2011, p. 13; Curtin D 2011, 'Top Secret Europe', Inaugural Lecture, *Universiteit vvan Amsterdam,* p. 6. Available from http://dare.uva.nl/document/2/103309 [2 November 2014].

[270] OJ L 309, 25.11.2005, pp. 15–36.

[271] Wesseling M 2014,'Evaluation of EU measures to combat terrorist financing', *European Parliament, Directorate General for Internal Policies, Policy Department C, Citizens' rights and Constitutional Affairs*, Brussels, p. 21.

[272] Wesseling 2014, p. 24.

[273] SWIFT and SWIFT II Agreements are thoroughly examined in Chapter 2 of the present study.

[274] Archick K 2013, 'U.S.-EU Cooperation against terrorism', *Congressional Research Service*, Report RS22030, p. 11.

In July 2011, the Commission launched a communication called 'A European terrorist finance tracking system: available options',[275] which was amended in November 2013.[276] The Commission proposed three different available options for the TFTS.[277] All of them conform to Article 72 TFEU about the EU legal limitations in the field of internal security:[278] a) the EU TFTS Coordination and Analytical Service, b) the EU TFTS Extraction Service, and c) the FIU Coordination Service.[279] They are hybrids between a full EU-centralised database and a decentralised national system. However, their feasibility in practice is still doubtful. The EU has not yet a reached full cooperation among its member states in the field of security, and the EP argues that the necessity of such system has not been sufficiently justified.[280]

In contrast, the Council has always supported the initiative, stating that it will ensure grater efficiency in the processing of information by police and intelligence agencies.[281] Indeed, the system might be advantageous in the sense that it will increase the exchange of intelligence within the EU, which many national intelligence services have long resisted.

The Commission has not launched any formal proposal for a TFTS yet, but other new initiatives seem to be accommodating the creation of this future system: on the one hand, the Commission proposed a directive and a regulation that will repeal Directive 2005/60/EC on the prevention of money laundering and terrorist financing.[282] It is based on Article 114 TFEU (the internal market provision) so the data collected, processed and stored by Financial Intelligence Units (FIUs) will have to comply with Directive 95/46/EC. The proposal is currently under negotiation in the Council and the EP.[283] On the other hand, the Council has included a provision on the cooperation between Europol and national FIUs in the proposed Europol Regulation. Although some member states have expressed their reservation on that issue, the provision as suggested by the Council allows the FIUs to collaborate with the EU agency through ENUs.[284] It makes

[275] COM(2011) 429 final, 13.07.2011.
[276] COM(2013) 842 final, 27.11.2013.
[277] The first option would be the creation of an EU TFTS coordination and analytical service, the second an EU TFTS extradition service, and the third would be a Financial Intelligence Unit coordination.
[278] COM(2011) 429 final, 13.07.2011, p. 6.
[279] COM(2013) 842 final, 27.11.2013, p. 12.
[280] Porter AL & Bendiek A 2012, 'Counterterrorism cooperation in the transatlantic security community', *European Security*, vol. 21, no. 4, p. 503.
[281] Council of the European Union, 11657/08, 09.07.2008, p. 39.
[282] COM(2013) 44 final and COM(2013) 45 final, 05.02.2013.
[283] Council of the European Union, 12243/14, 30.07.2014, p. 5.
[284] Council of the European Union, 8596/14, 07.04.2014, article 7(5b).

the aforementioned option for establishing a FIU Coordination System very probable, considering that the mirroring TFTP Agreement also involves Europol in the supervision of data requests.

The establishment of the TFTS would require the adjustment of the existing EU-US TFTP Agreement.[285] In this sense, the EDPS has argued that a better analysis should be conducted on the impact that a future EU TFTS will have on the SWIFT Agreement.[286] This issue might be one of the reasons why the Commission has delayed the proposal. In any event, if a proposal is finally released, the TFTS will be another example of how police authorities in EU member states are progressively expanding the EU security measures.

### *3.2.3. Exchange of telecommunication data within the EU*

Information collected and stored by telecommunication service providers (TSP)[287] and information society services (ISS)[288] has also been increasingly accessed by law enforcement authorities in the last fifteen years. The reason is the emerging use of broadband Internet and mobile devices by organised criminal bands and terrorists.[289] One example is found in the Madrid bombings of 2004, where terrorists used pre-paid SIM cards to detonate the bombs. Consequently, the EU adopted the Data Retention Directive and the Cyber Security Directive, which gave police authorities access to telecommunication data for the prevention, detection, investigation and prosecution of crimes. These directives have been highly controversial, as is seen in the following paragraphs.

[285] COM(2011) 429 final, 13.7.2011, 3; COM(2013) 842 final, 27.11.2013, p. 3.
[286] EDPS comments on the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS) and on the Commission Staff Working Document - Impact Assessment accompanying the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS), 17.04.2014.
[287] Definition in Article 2(c) of Directive 2002/21/EC, OJ L 108, 24.04.2002, pp. 33-50.
[288] Definition in Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC, OJ L 217, 05.08.1998, pp.18-25. See also Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, OJ L 178, 17.07.2000, pp. 1-16.
[289] COM(2013) 179 final, 10.04.2013, p. 2.

*a. Data Retention Directive*

Before 2006, the only mechanism to request telecommunication data was through the MLA procedures. As seen above, MLA requests can often be a very lenghty and inefficient process. Therefore, the Commission decided to adopt an instrument that would facilitate the retention, access and use of telecommunication data for law enforcement purposes: the Data Retention Directive.[290] It was adopted in 2006 with the purpose of harmonising domestic rules on the retention of traffic data stored by TSP for 'the investigation, detection and prosecution of serious crimes'.[291]

The Data Retention Directive was annulled by the CJEU in April 2014. The annulment did not come as a surprise, since the directive was controversial from the outset. The proposal was launched by the Council in order to establish in the EU a similar tool to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (hereinafter, the Patriot Act).[292] The Patriot Act was enacted in October 2001 following the 9/11 attacks as a measure to combat terrorism and money laundering activities. Section 215 of Patriot Act allows US law enforcement officials to collect metadata from TSPs located within the US territory during a criminal investigation. Yet, it is not only data from US citizens and residents that is processed through the Patriot Act. Third countries' data (including EU citizens' data) can also be accessed by the US authorities if they have been collected by a TSP located in the US, according to Section 702 of the Patriot Act.[293]

In order to prevent alleged clashes between the Patriot Act and the EU laws, the adoption of a similar piece of law in the EU became a necessity. Originally, the Council proposed that a retention provision was included in Directive 95/46/EC, but the EP rejected that proposal. Finally, the provision was included in Directive 2002/58/EC.[294] According to Article 15, 'Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph'.

The nature of the instrument was also an issue of debate. The Council proposed to draft a framework decision on data retention (a third pillar instrument), whereas the EP

[290] OJ L 105, 13.04.2006, pp. 54-63.
[291] Article 1(1) Directive 24/2006/EC, 15.05.2006.
[292] 107th Congress, First Session, H.R. 3162, 24.10.2001.
[293] This is examined further in Chapter 4 of this thesis.
[294] OJ L 201, 31.07.2002, pp. 37-47.

suggested adopting it in the form of a directive (a first pillar instrument).[295] In the end, the Commission followed the EP's suggestions and it launched a first-pillar proposal for a directive on data retention based on ex Article 95 TEC. The directive came into force in March 2006.

Four months later, Ireland, supported by Slovakia, challenged the directive before the CJEU. Ireland argued that the legislation should be adopted as a third-pillar measure because its purpose was clearly t0 combat serious crimes. That was the argument that the Court itself had followed in the previous PNR case, in which the Court concluded that when private companies collected personal data, even if the original purpose was purely economic, the measure could not fall under the scope of the internal market provision if data was later used for law enforcement. On the contrary, the Commission justified the legal basis for the Data Retention Directive by stating that it imposed direct obligations on TSP, rather than on governments.

Although it was expected that the Court would follow the precedent established in the PNR decision, this was not the case. In *Ireland* v. *Parliament*,[296] the Court contradicted its own jurisprudence by creating an artificial distinction between the reason for storing data and the purpose for processing such data.[297] Under that new test, the Court held that as long as the data was initially stored by a TSP to cover commercial activities, the directive was correctly adopted under the basis of ex Article 95 TEC. The Court added that 'the obligations relating to data retention have significant economic implications for service providers in so far as they may involve substantial investment and operating costs' (para. 68).

The argument used by the Court for PNR data transfers was then no longer valid.[298] Many scholars have speculated about the reasons why the Court changed its own argument.[299] A possible justification could be related to the different nature of the two

[295] Ni Loideain N 2011, pp. 258-259.
[296] Case C-301/06, 10.02.2009.
[297] Boehm F 2011, 'EU PNR: European Flight passengers under general suspicion. The Envisaged European Model of Analyzing Flight Passenger Data' in *Computers, Privacy and Data Protection: An Element of Choice,* eds: Gutwirth S, Poullet Y, de Hert P & Leenes R, Springer, Berlin, p. 193.
[298] The argument in the PNR decision was that the internal market provision does not apply when personal data is originally collected for commercial purposes by private companies and later transferred to government authorities for the purposes of national security and law enforcement.
[299] Hijmans & Scirocco 2009, p. 1506; Pateraki A 2011, 'The Implementation of the Data Retention Directive' in *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices,* eds. Akrivopoulou C & Psygkas A, IGI Global, Hershey, p. 318; Ni Loideain N 2011, 'The EC Data Retention Directive: Legal implications for privacy and data protection' in *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices,* eds. Akrivopoulou C & Psygkas A, IGI Global, Hershey, p. 260.

instruments. The EU internal market clause was easier to justify in a directive than in an international agreement, whose scope exceeds the territory of the 'EU internal market'. Another justification could be found in the categories of the data collected. In the PNR case, airlines were required to collect specific data that, before the agreement, was not collected at all. In contrast, the Data Retention Directive required operators to retain data that was already collected for commercial purposes.[300] Finally, another explanation could be that the Court sought to harmonise data retention rules within the EU with its new decision. Such harmonisation would have been difficult to achieve in the PNR agreements because third countries were involved.[301]

The directive established that member states could adopt domestic laws that obliged TSPs to retain data for a period of no less than six months and no more than two years. The categories of data retained in a communication were: a) the source; b) the destination; c) the time, date and duration: d) the type; e) the equipment; and f) the location.[302] However, in 2011 the Commission released an evaluation report that found that many provisions of the directive were too broad. For example, the main purpose was the prevention, combat and investigation of 'serious crimes', but the scope of that term was interpreted differently depending on the Member State. Some countries decided that a serious crime would be any offence with a minimum of one-year prison; whereas others decided to retain data related to all kinds of criminal offences.[303] Another controversial issue concerned the public actors that were able to access the data. These were not the same in all member states, and nor was the type of authorisation required for that access.[304]

In 2012, two new preliminary rulings on the validity of the Data Retention Directive were issued before the CJEU.[305] This time, the challenges did not concern the adequacy of its legal basis, but they questioned the substance of the instrument. The preliminary rulings claimed a potential clash between the directive and the rights enclosed in Directive 95/46/EC, the Charter of Fundamental Rights and the ECHR (especially, the right to privacy and data protection). In that sense, between 2008 and 2012, several constitutional courts of the member states had found that national laws implementing

[300] Hijmans & Scirocco 2009, p. 1506.
[301] Docksey 2014.
[302] Article 5 Directive 24/2006/EC.
[303] European Commission, 'Evaluation Report on Data Retention Directive', COM(2011) 225 final, 18.04.2011, p. 6.
[304] COM(2011) 225 final, 18.04.2011, p. 9.
[305] Case C-293/12, *Digital Rights Ireland* and Case C-549/12, *Seitzinger and others*.

the directive were contrary to their constitutional rights.[306] The two preliminary rulings were supported by the EDPS, who argued that the directive did not comply with the necessity principle, its purpose was not sufficiently precise, and it had not considered less-intrusive data retention mechanisms.[307]

In its defence, the Commission released a report with numerous cases in which the Data Retention Directive had helped in preventing and investigating crimes.[308] However, the report did not convince the CJEU, and in April 2014 the Court followed the Opinion of AG Cruz Villalón[309] and ruled that the directive was invalid for violating Directive 95/46/EC, as well as Articles 7, 8 and 52(1) of the Charter:

'[T]he obligation to retain for a certain period, data relating to a person's private life and to his communications, constitutes in itself an interference with the right guaranteed by Article 7 of the Charter. Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right. […] The fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.'[310]

The case is especially relevant since it is the first time that the CJEU has annulled an entire directive because of its incompatibility with the provisions of the EU Charter. Specifically, the main reason for the annulment was that the data retained failed to comply with the necessity and proportionality tests. Law enforcement authorities were able to access all EU citizens' communications even if there was no link to or evidence of any threat. No exceptions and distinctions depending on the categories of data were provided, either. Therefore, the Court considered that the nature of that measure was abusive.

---

[306] Particularly, Bulgaria, Hungary, Germany, Romania, Czech Republic, Slovakia and Cyprus.
[307] Opinion of the EDPS on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31.05.2011.
[308] For instance, it helped German police to identify individuals supporting the Al-Qaeda and the Uzbekistan Islamic Movement by distributing propaganda through Internet, and it allowed the identification of the person who uploaded a video on a terrorirst organisation in an Internet forum in 2010. For the complete list of cases, see European Commission, DG Home, 'Evidence for necessity of data retention in the EU', March 2013. Available from http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf [2 November 2014].
[309] Advocate General's Opinion in Joined Cases C-293/12 Digital Rights Ireland and C-594/12 Seitlinger and Others, 12.12.2013.
[310] Joined Cases C-293/12 and C-594/12, 08.04.2014, para. 34, 35 and 37.

After the ruling, the Art. 29 WP urged member states and the Commission to evaluate the consequences at the domestic and the EU level.[311] Although Commissioner Malmström stated that 'Member States' national legislation is not directly concerned by the judgment',[312] national data retention laws are indeed subject to the ruling. As Peers explains, national laws have to comply with the provisions of the Charter (and the general principles of law) when implementing EU law.[313] In that sense, several member states have started to invalidate or amend their implementation laws after the judgment, in conformity with the provisions of the Charter.[314] As for a future data retention directive, the Commission has not yet started any preparations, and no replacement is expected in the near future. It could be that the EU will not adopt a new data retention instrument at all in the future, considering that the court has been very clear in highlighting the intrusion it causes to the EU fundamental rights to data protection and privacy.

The potential implications of this decision for other data retention measures in the EU are unclear. Many questions need to find an answer yet, one of these issues being the future of other large-scale data retention systems after this judgment. Likewise, it is unclear to what extent the EU legislation / agreement needs to specify how Charter rights will be complied with. In this regard, a study concluded that the EU-US PNR Agreement, the EU PNR proposal, the EU-US TFTP agreement and the future EU TFTS could all be affected by this decision.[315] Any of these measures could be now challenged before the CJEU using the same arguments as in the Data Retention decision.

In contrast, the Legal Service of the EP has noted that the Data Retention judgment 'does not […] have any direct consequences for the validity of any other EU act'.[316] The

---

[311] WP 220, 01.08.2014.

[312] Parliamentary Question. Answer given by Ms Malmström on behalf of the Commission, 17.07.2014. Available from http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2014-005254&language=EN [2 November 2014].

[313] Peers S 2014, 'Are data retention laws within the scope of the Charter?', *EU Law Analysis. Blog about developments in EU Law*, 20.04.2014. Available from http://eulawanalysis.blogspot.com.es [2 November 2014].

[314] Particularly, Austria, Romania, Slovenia, the UK, Poland, Belgium and Slovakia. However, the Dutch government decided to maintain its data retention laws.

[315] Boehm F & Cole M.D. 2014, 'Data Retention after the Judgement of the Court of Justice of the European Union', *Greens/EFA Group, European Parliament*, Brussels. Available from http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf [2 November 2014].

[316] 'LIBE-Questions relating to the judgment of the Court of Justice or 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and others – Directive 2006/24/EC on data retention – Consequences of the judgement', Legal Opinion of the EP, para. 52.

Legal Service has thus underlined that each EU act benefits from a 'presumption of legality', so formally they remain valid. It has also noted that existing international agreements like PNR and SWIFT will not be reviewed by the CJEU in the sense of Article 218(11) TFEU, since this procedure can only be conducted before the international agreement is adopted.[317]

Lastly, another important issue emerging from the CJEU decision is the link the court poses between Articles 7 and 8 of the Charter and Article 8 of the ECHR. This close connection shows the important role of the EU in referencing other international organisations in the field of data protection. There is no doubt that the decision will be taken into consideration in the event of the establishment of global principles for data protection.

*b. Cyber Security Directive*

Because of the high number of cyberattacks suffered by private entities within the EU,[318] in February 2013 the Commission released a Cyber Security Strategy[319] and a proposal for a directive on network and information security (hereinafter, Cyber Security Directive).[320] Likewise, in August of that year the existing Council Framework Decision on attacks against information systems[321] was replaced with a directive.[322]

The purpose of the proposed Cyber Security Strategy is to 'ensure a high common level of network and information security (NIS)'. It was proposed under the basis of Article 114 TFEU (internal market clause), which, again, casts doubt on the adequacy of such choice[323] because of the involvement of law enforcement authorities in the data exchanges.

The proposed Cyber Security Directive will not only bind TSPs but also a broad category of 'market operators'. These are listed in Annex II of the proposal as: a) e-commerce platforms, b) Internet payment gateways, c) social networks, d) search

[317] This is actually the case of the proposed EU-Canada PNR Agreement, which is being reviewed by the CJEU since November 2014.
[318] For instance, in the UK alone 821 cyberattacks were registered in 2011. O'Brien KJ 2013, 'Europe weighs requiring to disclose data breaches', *New York Times*, 16 January. Available from <www.nytimes.com> [02.03.2015].
[319] JOIN(2013) 1 final, 07.02.2013.
[320] COM(2013) 48 final, 07.02.2013.
[321] OJ L 69, 16.03.2005, pp. 67-71.
[322] OJ L 218, 14.08.2013, pp. 8-14.
[323] Dutch MEP Sophie in 't Veld raised this issue during the CPDP2013 conference, 23-25.01.2013, Brussels.

engines, e) cloud computing services, f) application stores, g) energy, h) transport, i) banking, j) financial market infrastructures, and k) the health sector. In addition to the market operators, there are two other kinds of actors taking part in the prevention and investigation of cybercrimes: the NIS authorities and the law enforcement authorities. As illustrated in Table 1.1., both the NIS authorities and the law enforcement authorities are to be represented at the domestic and EU levels.

*Table 1.1.*

| | **NIS authorities** | **Law enforcement authorities** |
|---|---|---|
| **EU level** | Commission/ENISA<br>CERT-EU<br>Network competent authorities<br>EP3R | EC3/Europol<br>CEPOL<br>Eurojust |
| **National level** | National CERTS<br>NIS | National Cyber Crime Units |

Regarding the competent national authorities for NIS, they are regulated in Article 6 of the proposed Cyber Security Directive. Article 7 and Annex I of the directive set up the Computer Emergency Response Teams (CERTs), which may be part of the competent NIS authorities but this will not be mandatory. At the EU level, the European Network and Information Security Agency (ENISA) will act according to the subsidiarity principle, as stated in Article 8 of the proposed directive.

The law enforcement authorities also have a relevant role to play in this Cyber Security Strategy. For that reason, the proposal raised some concerns as to the adequacy of the legal basis, which addressed cybercrime as an internal market matter and not as an internal security issue. The National Cybercrime Units will be created to combat cyber crimes in the different member states, while in the EU the Cybercrime Centre (EC3) and Eurojust are the bodies in charge of that development. All law enforcement authorities will be directly connected with the NIS entities, and they will share information with each other.[324] The infrastructure used for the criminal-related data exchanges will be the existing secure information-sharing system TESTA.[325]

[324] Article 10(4) of Cyber Security Directive.
[325] Article 9 of Cyber Security Directive.

The proposal for a Cyber Security Directive has raised strong criticism[326] due to the following aspects: on the one hand, there is an expansion of the obligation to report data breaches beyond the traditional telecommunication databases:[327] not only will TSPs be accessed by law enforcement authorities, but all 'market operators' will be subject to the directive. Hence, ENISA and member states' powers exceed those granted under the void Data Retention Directive. On the other hand, there are doubts on the data breach notification regime established in the proposal, since the criteria do not coincide with the proposed EU Data Protection Regulation. In addition, the proposal does not include a clear separation of breaches caused by mere negligence from those resulting from cybercriminals.[328] In that sense, the EDPS pointed out that:

'A clear distinction should be made between accidental events, which are incidents that have occurred on a network or an information system, and malicious actions, which could have a connection with cybercrime.'[329]

In March 2014 the EP released 138 amendments on the directive that are currently being discussed at the Council.[330] The directive is expected to be adopted in 2015, but the recent annulment of the Data Retention Directive could raise new debates about the adequacy of the legal basis and substance of this proposal.

*c. The use of mutual legal assistance for accessing telecommunication data*

The traditional instrument for police and judicial authorities to access telecommunication data stored in TSPs is the MLA procedure. The Commission launched the Data Retention Directive and the Cyber Security Directive to facilitate the access of data for law enforcement purposes. However, the results have not been very successful. Whereas the Data Retention Directive has been annulled by the CJEU for being contrary to EU laws, the substance of the proposed Cyber Security Directive is

[326] 'ENDitorial: Questions On The Draft Directive On Cybersecurity Strategy', *EDRI Newsletter*, vol. 11 no.1, 16.01.2013. Available from Edri.org [2 November 2014].
[327] O'Brien 2013.
[328] Vaas L 2013 'Infosec pros give verdict on EU's new cybersecurity strategy: Nice try', *Naked Security*, 8 February. Available from http://nakedsecurity.sophos.com/2013/02/08/eu-cybersecurity-strategy/ [2 November 2014].
[329] EDPS comments on DG CONNECT's public consultation on improving network and information security (NIS) in the EU, 10.10.2012, p. 2.
[330] Council of the European Union, 13848/14, 03.10.2014.

being questioned for issues like the broad scope of the term 'market operators' and the expanded powers granted to ENISA.

Therefore, many law enforcement authorities have returned to the MLA procedures for intercepting telecommunication data from a TSP located in another Member State. This procedure is established in Articles 17 to 22 of the EU MLA Convention. It can also apply when law enforcement authorities need data collected and stored beyond the EU territory (e.g. in the US), but only if the two countries have previously signed a MLAT. For instance, the US has MLATs with the majority of member states, and even with the EU as a whole.[331] They cooperate with each other, sharing electronic information between their law enforcement authorities.

If police officers need to request specific information from a TSP, the first thing they need to know is where the headquarters of that particular private company is located as this will indicate the jurisdiction that the company is bound to. There are two ways to send a request to a TSP located in another Member State or a third country: a) the informal process, developing a direct relationship with the private entity or making the request through the police authorities of the requested country, and b) the formal process, sending the MLA request to the department of justice of the requested country, which will submit it to the competent court for the necessary warrant.[332]

Each private company decides in which circumstances it will accept an informal request. For instance, the popular social network Twitter, which has its main headquarters in the US, answers requests made by governmental authorities of EU member states by distinguishing between i) emergency requests, where there is a risk of death or serious injury to a person, and ii) non-emergency requests. Regarding the emergency requests, Twitter is available 24/7 and in such cases it responds without delay. In the non-emergency cases, requests need to be issued formally via the US courts through MLA.[333]

Within the EU, one of the main problems with the use of MLA procedures is that each Member State has its own criminal legal system, which contains specific

[331] MLATs with third countries and especially with the US are thoroughly analysed in Chapter 2 of this thesis.
[332] 'The use of the Internet for terrorist purposes', *United Nations Office on Drugs and Crime*, September 2012, New York, pp. 90-91. Available from http://www.unodc.org [3 November 2014].
[333] Blasi Casagran C 2013 'People c. Harris: El lado oscuro de la libertad de expresión en las redes sociales' in *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, eds. Cotino Hueso L & Corredoira Alfonso L, Centro Estudios Políticos y Constitucionales, Madrid, p. 423.

requirements and conditions for accessing TSP's data. For instance, some member states require a prior court order, whereas others permit the authorisation by the Secretary of State or a senior official.

In sum, as demonstrated by this study, the EU has adopted many instruments for the purpose of facilitating the exchange of information among law enforcement authorities. However, all of them reveal shortcomings with regard to their use and implementation. In the particular case of data collected by the TSP, the situation is no better. Since the Data Retention Directive was declared void by the CJEU and the proposed Cyber Crime Directive has been shelved by the Council. The next section examines an additional problem: all these data-sharing instruments contain different data protection rules, which leads to a fragmented EU data protection framework in the field of law enforcement.

## 4. The EU data protection legislation under the scope of the AFSJ

This study has identified and analysed the main EU instruments for processing information for law enforcement purposes. Any data processing requires compliance with data protection rules. In this sense, the Council of the European Union has emphasised that:

> 'Information exchange in the context of EU law enforcement cooperation will at all times respect the fundamental rights of citizens, in particular where it concerns the protection of personal data.'[334]

The main object of this section is to analyse the current and future laws regulating the protection of personal data collected, processed, stored and transferred within the EU for law enforcement purposes. It attempts to discern whether the EU has an effective data protection framework in the field of law enforcement, since this is the first step forward for achieving the establishment of global data protection principles in the area of security.

The analysis starts with an examination of the origins and evolution of the general data protection legislation before and after the Treaty of Lisbon. The specific data

[334] Council of the European Union, 7903/13, 25.03.2013, p. 3; Council of the European Union 7226/2/13, 26.04.2013, p. 5.

protection laws within the AFSJ are detailed next. The premise is that, although data protection legislation is harmonised at the EU level when it is encompassed within the internal market clause, the scope and limits of the EU protection of personal data are still very unclear when the processing is carried out for law enforcement purposes. This is added to the fact that general EU data protection laws might overlap with those data protection provisions included in each of the existing data-sharing instruments and systems in the field of criminal matters. The overall goal of this last analysis is to identify the flaws, if any, of the EU data protection rules applicable for data processing in the field of law enforcement.

## 4.1. General data protection rules in connection with the AFSJ

### *4.1.1. Origins of the EU data protection legislation*

The Council of Europe (CoE) and the Organisation for Economic Co-operation and Development (OECD) play an important role as the main influences of the EU data protection framework. On the one hand, the OECD released a Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines)[335] in September 1980. On the other hand, in 1981 the Council of Europe adopted the 108 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (the 108 CoE Data Protection Convention).[336] Unlike the OECD Privacy Guidelines, the standards and values of the 108 CoE Data Protection Convention are binding for all CoE Contracting Parties.[337]

The OECD Privacy Guidelines and the 108 CoE Data Protection Convention include the same foundational principles: i) the collection limitation principle, ii) the data quality principle, iii) the purpose specification principle, iv) the use limitation principle, v) the security safeguards principle, vi) the openness principle, vii) the individual participation principle, and viii) the accountability principle.[338]

---

[335] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23.09.1980.
[336] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.01.1981.
[337] Chapter 5 of this thesis will examine in dept the nature and content of these instruments.
[338] For a definition and further discussion of the principles, see http://oecdprivacy.org/ and http://conventions.coe.int/treaty/en/treaties/html/108.htm [3 November 2014].

As noted above, both frameworks served as the source of inspiration for the later EU data protection legislation. At first, the EU based data protection laws on its internal market clauses: Article 100a TEC (later amended as Article 95 TEC) and Article 286 TEC. Therefore, the Community had full competence to legislate on data protection matters. The reason behind the choice of the legal basis was simple. The creation of a common market had brought the free movement of goods, persons, services and capital, and with it, a free flow of personal data from one Member State to another. The objective was to systematise the substantial increase in the cross-border movement of personal data because of the intensification of social and economic activities within the EU. That came along with the technological progress for processing and exchanging data that emerged during the early nineties. Directive 95/46/EC was thus crucial to avoid a situation where that member states adopted different national laws on data protection.

### *4.1.2. Impact and scope of Directive 95/46/EC*

Directive 95/46/EC[339] is the first and main EU legislative act that regulates the protection of personal data within the EU. As explained above, the establishment of the EU internal market by the Maastricht Treaty increased significantly the quantity of personal data collected and stored for economic purposes. The free circulation of goods, services, persons and capital among member states led to the proliferation of databases in private companies and industries that interacted in the European market. Under these circumstances, Directive 95/46/EC was drafted as the legislative tool that would coordinate the collection, processing and storage of various personal data obtained for commercial reasons.

Directive 95/46/EC was inspired by the core privacy principles established in the OECD Privacy Guidelines and the 108 CoE Data Protection Convention. These were included in Directive 95/46/EC, and later implemented in the domestic legal frameworks of the member states. Particularly, the directive contains the following rules: the principle of lawfulness and fairness; the purpose limitation principle; the principle of adequacy; the principle of accuracy and necessity; data have to be kept no longer than necessary; the prohibition of the processing of special categories of data; the

[339] OJ L 281, 23.11.1995, pp. 31-50

right to data access; the right to erasure, blocking and deletion of data; the data subject's right to object; the legal prohibition on automated decision making; the confidentiality and security of processing; the obligation to notify the supervisory authority about the processing; the need for independent supervision; the obligation to establish appropriate technical measures against destruction, loss, alteration or unauthorised access or disclosure; and the obligation to establish provisions on remedies, liability and sanctions.[340]

From the moment Directive 95/46/EC came into force, member states started a reform of their domestic laws on data protection. However, the scope of the directive included a limitation: Article 3(2) expressly refrained from addressing those activities concerning public security, defence or state security. Hence, the member states retained the sole competence to legislate on the data processed by the judicial and police authorities.

The scope and limits of Article 3 was not always fully clear to member states during the implementation process. Therefore, the CJEU set jurisprudence on the interpretation of this provision. In the *Österreichischer Rundfunk*[341] and *Lindqvist* cases,[342] the Court showed a great flexibility in the interpretation of Article 3 regarding the connection between the internal market and the economic activity at stake.[343] In the first case, the Court found that the Austrian provision requiring private entities to inform the Austrian Court of Audit about the names and salary of their employees fell under the scope of the directive. In particular, the Court ruled that:

'The applicability of Directive 95/46 to situations where there is no direct link with the exercise of the fundamental freedoms of movement guaranteed by the Treaty is confirmed by the wording of Article 3(1) of the directive, which defines its scope in very broad terms.' (para. 40)

Therefore, the directive has often applied even when the data processing activity was not directly linked to the internal market. Likewise, in *Lindqvist*, a catechist had set up a home page on the Internet containing information about herself and various members of

[340] Articles 6, 8, 12, 14, 15, 16, 17, 18, 23, 24 and 28 of Directive 95/46/EC.
[341] C-465/00, C-138/01 and C-139/01, 20.05.2003.
[342] Case C-101/01, 06.11.2003.
[343] Tzanou M 2011, 'Data protection in EU Law: An analysis of the EU legal framework and the ECJ jurisprudence' in *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices,* eds. Akrivopoulou C & Psygkas A, IGI Global, Hershey, pp. 284-285.

her parish, without their consent. The Court found that the mention of an individual on an Internet home page fell under the scope of Directive 95/46/EC. Even if the creation of a web page did not constitute any economic activity (it was a non-profit-making activity), it concluded that:

'Charitable or religious activities such as those carried out by Mrs. Lindqvist cannot be considered equivalent to the activities listed in…Article 3(2) of Directive 95/46 and are thus not covered by that exception.' (para. 45)

In both cases the CJEU interpreted the scope of the directive broadly. The same occurred a few years later in the case of *Ireland v. Parliament* on the Data Retention Directive, mentioned above. In that case the CJEU inferred that a measure related to criminal law fell under the former EC competence if it was necessary to achieve the effectiveness of an EU policy.[344] In conclusion, the Court has often[345] offered a wide interpretation of the scope of Directive 95/46/EC[346] when determining whether the purpose for processing data was linked to the EU internal market policy.

### *4.1.3. Applicability of Regulation (EC) 45/2001 within the AFSJ*

Regulation (EC) 45/2001[347] was adopted for the purpose of regulating data processed among the EU institutions and bodies 'insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law'.[348] This regulation mirrors the majority of principles of Directive 95/46/EC and, although it is only applicable for data exchanges within the former first pillar, it has also developed a role under the scope of the AFSJ.

One example is found in the European information systems that were part of the former first-pillar bodies.[349] In particular, until 1 December 2012, the Commission had a

[344] Hijmans & Scirocco 2009, p. 1507.
[345] However, the PNR court decision did not follow this background, as examined in Chapter 2 of this study.
[346] Hijmans & Scirocco 2009, p. 1502.
[347] OJ L 8, 12.01.2001, pp. 1-22.
[348] Article 3 of Regulation (EC) 45/2001.
[349] Boehm F 2012c, 'Data processing and law enforcement access to information systems at EU level', *Datenschutz und Datensicherheit*, vol. 36, no. 5, p. 330.

relevant role in managing the systems of Eurodac, VIS and SIS. However, since December 2012, the EU agency eu-LISA has replaced those tasks.

Although Eurodac, VIS, SIS and also CIS were all initially established under the scope of the first pillar as border control instruments, as seen above, their scope has been extended to the field of criminal matters. The Commission was (and it still is, in the case of CIS) the institution in charge of the processing of personal data, in conjunction with the national authorities of the member states. In theory, Regulation (EC) 45/2001 only applies for data processed in the field of border control. However, in practice, it is very difficult to separate the purpose of border management from that of law enforcement, especially if the data collected is the same for both cases. Therefore, by extension, Regulation (EC) 45/2001 would also apply for information collected by Eurodac, VIS, SIS and CIS that is ultimately used for preventing, combating and investigating crimes.

Another case in which the Commission has to comply with Regulation (EC) 45/2001 is for the processing of personal data included on blacklists for terrorism suspects. The EU adopted Common Position 2002/402/CFSP[350] and Regulation (EC) No 881/2002[351] as restrictive measures based on the freezing of funds of certain persons and entities associated with Osama bin Laden, the Al-Qaeda network and the Taliban. They were implementing UNSC Resolutions 1267 (1999), 1333 (2000) and 1390 (2002). Restrictive measures were always composed of an intergovernmental instrument (a common position or a Council decision) and an EC/EU instrument (a EC regulation or Council regulation). The Commission includes the names of the persons whose funds are to be frozen. Regulation (EC) No 881/2002 has already been amended more than 220 times to date.[352] Every time the Commission processes personal data for listing or deleting terrorists, it needs to comply with the provisions of Regulation (EC) No 45/2001.

Finally, the majority of AFSJ agencies are also bound to the Regulation (EC) 45/2001. However, there is a difference between the agencies that were part of the first pillar before Lisbon, and those that fell under the scope of the third pillar. In the case of

[350] OJ L139, 29.05.2002, pp. 4-5.
[351] OJ L139, 29.05.2002, pp. 9-22.
[352] The last amendment is Commission Implementing Regulation (EU) 2015/64 of 16 January 2015 amending for the 224th time Council Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with the Al-Qaeda network, OJ L 11, 17.01.2015, pp. 65–67.

Frontex,[353] which was a first-pillar agency, it is subject to all provisions of the Regulation (EC) No 45/2001. In contrast, EU law enforcement agencies like Europol or Eurojust, which were former third-pillar bodies, are only bound to the core principles of Regulation (EC) No 45/2001.[354] However, Europol and Eurojust mandates will be replaced by new legislative instruments soon[355] and, when they enter into force, Regulation (EC) No 45/2001 will fully apply for these agencies.

### *4.1.4. The Treaty of Lisbon and the new data protection paradigm*

Before Lisbon, Article 286 TEC was the provision regulating data protection within the first pillar. For data processing within the scope of the second and third pillars, the EU competence was limited to secondary legislation in the field. According to several CJEU decisions,[356] international law was usually ranked more highly than EU secondary law but below EU primary law (EU Treaty provisions). Consequently, international agreements confronting EU secondary legislation on data protection for law enforcement purposes would always prevail.

The Treaty of Lisbon significantly changed the European framework regarding the protection of personal data. With the abolishment of pillars, the EU and its member states shared competences for legislation on data processed for criminal matters. Also, Articles 16 TFEU and 39 TEU were introduced as new legal bases for the right to data protection.

Article 16 TFEU replaces former Article 286 TEC. According to this new provision, the right to data protection is now applicable to all EU sectors. This right is entirely EU primary law and prevails over any international agreement confronting it. Likewise, Article 16(2) TFEU expands the scope of the provision by stating that rules on data protection are not only bound to EU institutions, bodies, agencies and offices, but also to 'Member States when carrying out activities which fall within the scope of Union law'. Hence, EU data protection legislation is today not only applicable to former first-pillar activities, but also to former second- and third-pillar matters, including data processing activities in the field of law enforcement. Some of these activities are

[353] Recital 19 of Council Regulation (EC) 2007/2004 of 26 October 2004 establishing the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. OJ L 349, 25.11.2004, pp. 1-11.
[354] Article 39 ECD.
[355] COM(2013) 173 final, 27.03.2013; COM(2013) 535 final, 17.07.2013.
[356] For instance, Case C-162/96 *Racke v Hauptzollamt Mainz* [1998] ECR I-3633, para. 46.

expressly foreseen in the Treaty. This is the case for the use of biometrics,[357] the freezing of funds,[358] border management,[359] and the data processed for the prevention, detection and investigation of crimes,[360] to name a few. Moreover, Article 216 TFEU enables the EU to conclude international agreements in cases specified by the Treaty, when it is necessary for achieving a EU objective, or if is provided for a legally binding EU act. This is, for example, the legal basis of the most recent EU-US PNR agreement, studied in Chapter 2 of this thesis.

Regarding the institutional amendments, before the Treaty of Lisbon the EP did not have any legislative role to play in the formulation of third-pillar laws. It was consulted but its opinion was not always taken into account in the negotiations of an international agreement. Since the Treaty of Lisbon, the EP participates in the ordinary legislative procedure and, therefore, it now has the right to veto EU international agreements. In this sense, Article 218 TFEU enshrines the so-called 'consent procedure', in which the EP needs to approve those international agreements adopted through ordinary legislative procedure. Likewise, the EDPS has enjoyed greater powers since the Treaty of Lisbon. The role of this body is no longer limited to the areas falling under the former first pillar. Now, the EDPS' supervisory tasks cover all EU institutions and bodies, including areas outside the scope of what used to be 'Community law'.[361]

The new EU data protection legislation increases the role of the CJEU on these issues, too. For example, before the Treaty, the Court did not address aspects relating to data protection when it clashed with individual restrictive measures in the field of security. Now the Court is able to examine any EU act and international agreement based on the processing of information for law enforcement purposes and to issue an opinion on the compatibility with the provisions of the Treaty.[362] Therefore, the fact that there is an explicit EU provision on the right to data protection, together with the new binding nature of the Charter of Fundamental Rights of the European Union, provides the Court with more instruments to protect that right.

The status of the Charter of Fundamental Rights of the European Union (hereinafter, the Charter) is also amended with the Treaty of Lisbon. Before the Treaty, the Charter was considered as part of the soft law for the courts, being a quasi-legal instrument with

[357] Article 77(3) TFEU.
[358] Article 75 TFEU.
[359] Article 77(2)(d) TFEU.
[360] Article 87(2)(a) TFEU.
[361] European Data Propection Supervisor, Annual Report 2010, p. 18.
[362] Article 218(11) TFEU.

no legally binding force. In contrast, the provisions of the Charter are now part of the hard law. Thus, they have a binding nature and the same value as the treaties.[363] As seen above, the right to data protection is included as a fundamental right in Article 8 of the Charter.

It is worth mention here that the Treaty of Lisbon also includes a provision on the EU accession to the European Convention of Human Rights (ECHR).[364] Although the accession procedure has been recently put back by the CJEU Opinion 2/13,[365] a future adhesion would allow the use of Article 8 ECHR on the right to respect for private and family life within the scope of the EU law.

In the view of the foregoing, Article 16 TFEU, the new nature of the Charter and the anticipated EU accession to the ECHR have caused a reinforcement of the EU right to data protection. However, in line with the exception of 108 CoE Data Protection Convention, Article 8(2) of the ECHR recognises that interferences of a public authority with a person's right to privacy may be justified as necessary in the interest of national security, public safety or the prevention of crime. This paragraph justifies that, in some circumstances, the EU and the member states can put collective security before the right to privacy.

In the same way, the Treaty of Lisbon has foreseen specific data protection rules in the context of the Common Foreign and Security Policy (CFSP). According to Article 39 TEU, the Council can adopt a special decision laying down the rules relating to data protection. If that occurs, Article 16 TFEU would be derogated for the processing of personal data for activities under the scope of the CFSP, and new rules would apply.

The relationship between Articles 16 TFEU and 39 TEU is today still unclear, since it is unknown in which situations Article 39 TEU will be applicable. It is presumed that Article 39 TEU, together with Declarations 20 and 21,[366] was introduced with the expectation that there will be situations in which general EU data protection laws might clash with third countries' security rules. In such situations, new standards will be adopted.

---

[363] Blasi Casagran C 2012, 'The reinforcement of fundamental rights in the Lisbon Treaty' in *The European Union after Lisbon*, ed. Søren Dosenrode, Ashgate Publishing Ltd, Surrey, pp. 79-80.
[364] Article 6(2) TEU.
[365] CJEU, Opinion 2/13, 18.12.2014.
[366] Declaration 20 recalls that this legal framework includes specific derogations when rules on the protection of personal data have direct implications for national security; and Declaration 21 acknowledges that data protection in the fields of judicial cooperation in criminal matters and police cooperation may require provisions specific to this area.

As part of the CFSP, rules adopted under Article 39 will exclude the control of the CJEU and the EP. In particular, no instrument based on this provision can be challenged before the CJEU,[367] and the decision-making process will only involve the Council, but not the EP. However, Article 39 TEU has never been used to date. Therefore, it remains to be seen what purpose lies behind this provision, and the level of data protection that it will introduce for data processing activities within the scope of external security.

The Treaty of Lisbon has also introduced two protocols that weaken Article 16 TFEU. On the one hand, Protocol 21 states that the UK and Ireland are not always bound to Article 16 TFEU in the processing of personal data within the field of police and judicial cooperation. On the other hand, Protocol 36 foresees a number of transitional provisions, by which EU acts and international agreements adopted before the treaty will be preserved. According to this protocol, the Commission has only been able to challenge an ex-third-pillar instrument under Article 258 TFEU since 1 December 2014, and this has not occurred yet. The same condition applies for the CJEU revision of third-pillar instruments adopted before the Treaty of Lisbon. Therefore, with these new powers, the CJEU could now start procedures against pre-Lisbon instruments like Framework Decision 2008/977/JHA or the Prüm Decisions.

### 4.2. Sector-specific data protection legislation within the AFSJ

Today there is no unified EU approach on data protection within the field of law enforcement. In fact, many data exchanges conducted by national law enforcement authorities are still entirely subject to national criminal laws. According to Article 3(2) of Directive 95/46/EC, EU data protection laws do not apply 'in any case to processing operations concerning public security, defence, State security…and the activities of the State in areas of criminal law'. This provision has been an obstacle every time the EC has attempted to incorporate new data-sharing instruments in the field of security. The third pillar had its own provisions, which regulated transnational law enforcement as opposed to national and state security, but no provisions were originally foreseen to protect data within the scope of that pillar. Thus, before 2008, the only solution for that was to 'mask' these laws as part of one of the EC former policies, as occurred with the 2004 EU-US PNR agreement and the Data Retention Directive.

[367] However, a possible way for the Court to review data processing agreements under the basis of Article 39 TEU is examined below.

In 2008 that paradigm changed. The EU adopted a framework decision under the former third-pillar on data protection aspects falling within the scope of police and judicial matters. Although it was seen as an improvement, the instrument was criticised from the beginning for being very broad, for giving too much room for implementation to the member states. This section analyses the scope and shortcomings resulting of Framework Decision 2008/977/JHA. After that, a comparison will be made between the framework decision and the proposal for a directive on data protection in the field of criminal matters.

### *4.2.1. The limited scope of Framework Decision 2008/977/JHA*

Framework Decision 2008/977/JHA (hereinafter, FD 2008/977)[368] was adopted as the first EU data protection instrument in the field of the former third pillar. The necessity to have EU law that would regulate cross-border exchanges of law-enforcement information was first stressed in the Hague Programme four years earlier.[369]

FD 2008/977 was proposed in 2005[370] and it included rules on data subjects' rights, supervisory authorities, data processing and data transfer similar to those established in Directive 95/46/EC. However, the first draft proposal was significantly modified because of its lack of precision in several provisions.[371] A new proposal was not launched until 2008.

FD 2008/977 was based on former Articles 30(a) and (b) TEU – today Articles 87-88 TFEU. The main purpose of the act was to ensure that data made available between member states had a high level of data protection while guaranteeing public safety.[372] It included data protection rules such as the lawfulness and fairness of data processing; the purpose limitation principle; accuracy of the processing; the rights to erasure, blocking and deletion of data; appropriate technical measures against destruction, loss, alteration or unauthorised access or disclosure; rules on confidentiality and data security; remedies, liability and sanctions; and the obligation for an independent supervision.[373]

---

[368] OJ L 350, 30.12.2008, pp. 60-71.
[369] Hague Programme, 10 priorities for the next five years, Recital 4. OJ C 236 of 24.09.2005, pp. 9-11.
[370] COM(2005) 490 final, 12.10.2005.
[371] de Hert P & Papakonstantinou V 2009, 'The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for', *Computer Law & Security Review*, vol. 25, p. 407.
[372] Article 1(1) of Framework Decision 2008/977/JHA.
[373] Articles 3(1), 6(1)(b), 4(1), 7, 8, 18, 19, 21, 22, 24 and 25.

Law enforcement authorities would need to comply with the act every time data was transferred to another Member State for the 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'.[374] However, it would not apply to purely internal situations in which information was collected and used for one single Member State. That was a criticism that was levelled at the instrument after its adoption.[375] Other issue of complaint referred to the nature of the instrument: One the one hand, member states' compliance with a framework decision cannot be enforced by the Commission and, on the other hand, the instrument was limited by the subsidiarity principle.[376] Being the AFSJ an area of shared competence between the EU and the member states, national laws on data processing for security purposes might still apply if an action can be more effectively taken at national, regional or local levels.

The fact that data protection principles of FD 2008/977 were not fully equivalent to Directive 95/46/EC was also seen as controversial.[377] For instance, FD 2008/977 does not contain any provision prohibiting the processing of special categories of data. Instead Article 6 FD 2008/977 states that data on race, politics, religion or philosophical beliefs, trade-union membership, health or sex life are permitted if strictly necessary and under adequate safeguards.[378] Another difference is found in the requirement to notify and inform the data subject. This condition is included in recital 26 of FD 2008/977, but according to recital 27 national laws can determine exceptions to it. The individual right to access is not equivalent in the two instruments either. Recital 29 of the Framework Decision introduces that right similarly to Directive 95/46/EC. Yet, paragraph 2 of Article 17 FD 2008/977 establishes a number of restrictions in its applicability. Also, unlike Directive 95/46/EC, the Framework Decision does not foresee the individual's right to object, and includes several vague derogations of the

[374] Recital 6 of Framework Decision 2008/977/JHA.
[375] de Hert & Bellanova R 2009, 'Data protection in the Area of Freedom, Security and Justice. A system still to be fully developed?', *European Parliament, Directorate General Internal Policies of the Union, Policy Department C, Citizens' Rights and Constitutional Affairs*, PE 410.692, p. 6.
[376] Article 5 TEU.
[377] For a discussion on the disappointments of FD 2008/977 in comparison to the provisions of Directive 95/46/EC, see de Hert & Papakonstantinou 2009; de Hert & Bellanova 2009, pp. 6-7; Boehm 2012a, pp. 138-144; Hijmans & Scirocco 2009, p. 1494; Nino M 2010, 'The protection of personal data in the fight against terrorism. New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon', *Utrecht Law Review*, vol. 6 no. 1, pp. 67-69.
[378] Interestingly, Europol (which is excluded from the scope of FD 2008/977) offers in this respect a higher level of data protection, since Article 10 ECD does not allow any processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life. A complete analysis of the Europol data protection framework is examined in Chapter 3 of this thesis.

requirement of prior consent before transferring data to third countries or international bodies.[379] Lastly, both the Directive and FD 2008/977 specify powers for an independent data protection authority for the oversight; but the Framework Decision does not establish any body similar to the Art. 29 WP within its scope.

The major disappointment as regards the content of FD 2008/977 was the exclusion of several sector-specific EU legislative instruments from its scope.[380] For instance, the framework decision does not apply to data processed by Europol, Eurojust, Schengen Information System (SIS), Customs Information System (CIS), Prüm, existing agreements with third countries (e.g. PNR agreements),[381] and other existing EU acts on the exchange of criminal-related information.[382] Although such instruments contain their own particular data protection rules and usually refer to the data protection principles of the Council of Europe, a general fully-fledged regime through FD 2008/977 would have ensured a minimum data protection threshold for all EU information systems.[383]

That said, it can be concluded that, although the adoption of FD 2008/977 brought some progress with respect to the protection applicable to that data processed within the field of criminal law, the instrument has several shortcomings. One of them is the exclusion of data processed by Europol, Eurojust, SIS, CIS, Prüm, international agreements with third countries and any other existing EU act on data exchanges (e.g. the Swedish initiative). FD 2008/977 is thus only applicable to data exchanges through mutual assistance procedures (according to CoE and EU MLA provisions), VIS, ECRIS and Eurodac systems. The need for a new legislative act on data protection for police and judicial matters in the EU emerged because of these limitations, especially after the entry into force of the Treaty of Lisbon.

---

[379] Article 13 of Framework Decision 2008/977/JHA.
[380] Recital 39 of Framework Decision 2008/977/JHA. This restriction regarding the scope was not foreseen in the original proposal by the Commission in 2005, but it was added afterwards due to the political interest of some member states. Hijmans & Scirocco 2009, p. 1497.
[381] Article 26 of Framework Decision 2008/977/JHA.
[382] Article 28 of Framework Decision 2008/977/JHA.
[383] As for this lack of a minimum common denominator for data processed in the field of law enforcement, Chapter 3 of this thesis suggests using Europol's data protection framework as the model system for every cross-border exchange of crime-related information.

### *4.2.2. EU data security classification regime*

Below, a few lines are dedicated to the current classification regime on data security within the EU. First of all, it is worth highlighting that data protection is directly linked to data security. Such a link was not considered in the nineties, with the adoption of Directive 95/46/EC. However, a few years later, with the rapid progress of new technologies and the factual vulnerability of the digital law, the establishment of security measures became crucial.

In 2011 the Commission adopted Council Decision 2001/264/EC,[384] which was amended in 2004,[385] 2011[386] and 2013.[387] Its regulatory framework is divided into security rules for data in the industrial sector and provisions dedicated to national security.[388] It also classifies the levels of security into four categories: restricted, confidential, secret or top secret.[389] The classification of the particular data processed is decided at the discretion of the Member State.

Interestingly, Europol is excluded from the Council decision's legal framework. The agency has its own data security classification, which was first established in Council Act of 3 November 1998. Although the Europol act is in many aspects similar to the EU data security legislation – the security classification, for instance – this duplicity of rules supposes a fragmentation in the processing of information within the EU. Moreover, the proposed EU data protection directive for judicial and police cooperation also includes specific data security rules, which will complement the existing EU data security framework.[390] This proposal is examined in the next section.

### *4.2.3. Proposal for a directive on data protection for police and judicial cooperation in criminal matters*

FD 2008/977 does not fulfil the criteria of Article 16 TFEU because it does not apply to domestic data processing activities and it excludes the participation of the EP.[391]

[384] OJ L 101, 11.04.2001, pp. 1-66.
[385] OJ L 193, 23.07.2005, pp. 31-36.
[386] OJ L 141, 27.05.2011, pp. 17-65.
[387] OJ L 274, 15.10.2013, pp. 1–50.
[388] O'Neill 2012, p. 75.
[389] Article 2(2) of Council Decision 2011/292/EU.
[390] Articles 27-29 of the proposed Directive.
[391] Hijmans & Scirocco 2009, p. 1519; de Hert & Bellanova 2009, p. 7.

Therefore, when the Treaty of Lisbon entered into force, FD 2008/977 needed to be amended or replaced. In this sense, Declaration 21 attached to the Treaty of Lisbon enables the EU to adopt specific rules on data protection within the police and judicial sectors, taking due account of the specific nature of these fields.

The Stockholm Programme was the first post-Lisbon initiative to establish new legislation within the AFSJ, including rules on the management of the flow of information for security purposes.[392] Later, the European Council and the Commission concretised the programme by adopting a communication[393] and a strategy[394] with the purpose of dealing with EU data protection rules within the AFSJ. The communication launched by the Commission was the first step for laying down a new EU data protection framework. It pinpointed some new challenges such as the impact of new technologies, the lack of harmonisation on data protection legislation among member states, the not enterily satisfactory schemes of international data transfers, and an ineffective and incoherent data protection framework. The Commission also put forward some key objectives like increasing transparency, ensuring greater control over one's own data, raising awareness about the risks related to the processing of personal data, strengthening rules on consent, harmonising the conditions for the processing of sensitive data, and establishing effective remedies and sanctions. Finally, the Commission referred to the need to revise data protection rules in the area of police and judicial cooperation in criminal matters.

As a result, on 25 January 2012 the Commission launched two proposals: the Proposal for the General Data Protection Regulation (hereinafter, the proposed Regulation)[395] and the Proposal for Police and Criminal Justice Data Protection Directive (hereinafter, the proposed Directive).[396] This study focuses only on the latter.

The proposed Directive will repeal current FD 2008/977.[397] If we compare the two instruments, a number of improvements can be discerned in the future act. For instance, the proposed Directive will confer direct effect on individuals; it will be subject to the

[392] However, the Hague Programme in 2004 had already set out information exchange as one of the key objective for the next five years, foreseeing the reinforced collection and exchange of data with the aim of managing migration flows as well as for the prevention and control of crime. See OJ C 53, 03.03.2005, pp. 1-14.
[393] European Commission, COM(2010) 609 final, 04.11.2010.
[394] 'Internal Security Strategy for the European Union: Towards a European security model', European Council, 26.03.2010.
[395] COM(2012) 11 final, 25.01.2012.
[396] COM(2012) 10 final, 25.01.2012.
[397] Article 58 of the proposed Directive.

Charter of Fundamental Rights; it involves the EP in the legislative procedure and it will fall within the jurisdiction of the CJEU.[398]

As for the substance of the proposal, it enhances the scope of application of the FD 2008/977: it will not only apply to cross-border data exchanges within the EU, but also for the processing of personal data at the purely national level. Some member states have opposed to this new issue, arguing that if the directive regulates national data processing, it might be contrary to the EU subsidiarity principle. Other member states have expressed doubts about the feasibility of harmonising data protection laws in the field of law enforcement,[399] or they simply find the data protection rules in the current FD 977/2008/JHA sufficient.[400]

The proposed Directive also includes small improvements as for individual rights, like the obligation to notify data subjects about the processing of their data.[401] Unfortunately, rights like the duty to inform[402] and the right of access[403] are subject to numerous exceptions. In this regard, the Art. 29 WP has argued that the possibility to exempt entire categories of personal data from these rights should be deleted from the proposal.[404]

Particularly interesting is the provision on different data processing procedures depending on the category of the data subjects (suspects, convicts, victims, witnesses, contacts or associated persons, and other persons).[405] For instance, Article 8(1) states that personal data classified as 'sensitive'[406] cannot in principle be processed.[407] This general rule has been another issue of debate at the domestic level, since many national law enforcement authorities consider that sensitive data may be relevant for a criminal

[398] Peers S 2012, 'Analysis. The Directive on data protection and law enforcement: A Missed Opportunity?', *Statewatch*, pp. 2-3. Available from <www.statewatch.com> [4 November 2014].
[399] That was argued by Germany. Council of the European Union, 14901/2/13, 30.10.2013, p. 4.
[400] That was the argument of the UK. Council of the European Union, 11624/1/13, 02.10.2013, p. 2; Council of the European Union, 14901/13, 09.12.2013, p. 2; Council of the European Union, 14901/13, 09.12.2013, p. 3.
[401] Article 11 of the Proposed Directive.
[402] Article 11(4) and (5) of the Proposed Directive.
[403] Article 13 of the Proposed Directive.
[404] WP 201, 26.02.2013, p. 3.
[405] Recital 23 and Article 5 of the proposal. An amendment by the LIBE Committee is proposed to delete such distinction, see LIBE AM 314-317.
[406] Sensitive data are those personal data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, genetic data or data concerning health or sex life.
[407] Article 8 of the proposed Directive.

investigation and, therefore, should be processed.[408] In fact, the majority of member states prefer the wording in the FD 2008/977, which is not formulated as a prohibition.

Although the proposed Directive improves the current framework decision, numerous aspects have brought disappointment among the pro-privacy community. One of these issues was that an unofficial proposal leaked in November 2011[409] offered better safeguards for the individuals than the final version released in January 2012.[410] By way of example, the final proposal does not contain any mention of data protection impact assessments, which was originally included in the leaked draft.[411] Another criticism refers to the removal of Article 1(5) of the FD 977/2008. This provision establishes that the framework decision cannot preclude member states from providing higher data protection safeguards than those established in the law. A similar provision is not found in the current proposal, even though some member states have already expressed the will to adopt stricter domestic rules than those in the proposal.[412]

Further discontent relates to the data retention rules in the proposal. Article 24 of the proposed Directive states that personal identification will be allowed for the data processing 'as far as possible'. This ambiguity is reinforced in Article 4 paragraph (e) of the proposal, which establishes that 'data will be kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed'. The risk of this wording is that the information could be used for multiple investigative purposes with no temporal limitation.[413]

The annulment of the Data Retention Directive has also stirred up debate over the lack of precise rules on public-private cooperation, profiling measures, and the need to define the term 'serious crime' in the proposed Directive. As Boehm and Cole noted, the proposal should be revised to include the Court's argumentation on such aspects.[414]

Although the inclusion of an independent supervisory authority supposes 'a big step

---

[408] Council of the European Union, 14901/2/13, 30.10.2013, pp. 23, 58-59; Council of the European Union, 14901/13, 02.12.2013, p. 6.
[409] 'Observatory on data protection in the EU', Statewatch. Available from http://www.statewatch.org/eu-dp.htm [4 Novemebr 2014].
[410] Bäcker M & Hornung G 2012, 'Data processing by police and criminal justice authorities in Europe - The influence of the Commission's draft on the national police laws and laws of criminal procedure', *Computer Law & Security Review*, vol. 28 no. 6, p. 628 and fn. 9.
[411] Bäcker & Hornung 2012, p. 629.
[412] 'Tough Negotiations For The Law Enforcement Data Protection Directive', *Edri.org*, 23.10.2013. Available from edri.com; Council of the European Union, 14901/13, 09.12.2013, p. 3.
[413] Council of the European Union, 14901/13, 02.12.2013, p. 5.
[414] Boehm & Cole 2014, pp. 85-87.

forward',[415] these authorities will have very limited powers. In that sense, the Art. 29 WP recommended extending Article 46 of the proposed Directive on supervisory authorities' powers and adding the possibility to access 'all necessary documents for the exercise of their investigative powers'.[416] That change would offer a complete supervision on the processing of data within the field of police and judicial cooperation, aligning it to Directive 95/46/EC.

Furthermore, the fact that the proposal has not been adopted in the form of a regulation has drawn criticism from various EU data protection 'watchdogs'. In particular, the EDPS,[417] the Art. 29 WP[418] and the EP[419] expressed their disappointment about this issue. They highlighted the inadequate level of protection in the proposed Directive as being greatly inferior to the proposed General Data Protection Regulation.[420] In contrast, some member states have argued that the whole data protection package should be released in the form of a directive as a way to overcome any overlap between the two proposals.[421] In the end, the separation of instruments (a regulation and a directive) will remain. The Commission has justified the specific nature of the proposed Directive by referring to Declaration 21 of the Treaty of Lisbon, which acknowledges specific rules for the protection of personal data in the field of criminal matters. In addition, the majority of member states prefer a directive to a regulation because they do not want to lose national sovereignity in the field of criminal law.

The proposed Directive does not specify if it will operate in cases where data is collected by private entities for internal market purposes but later processed by police authorities. In my view, it will depend on who is conducting the data processing activity. If it is carried out by a public authority then the proposed Directive will apply; but if a private company is the data processor instead, it will fall under the scope of the proposed Regulation. In this regard, the Council has clarified that if a private entity collects data for commercial purposes and it has a legal obligation to share it with law

[415] WP 201, p. 5.
[416] WP 201, p. 7.
[417] EDPS Opinion on the data protection reform package, 7.3.2012, p. iv.
[418] WP 191, 23.03.2012, p. 26.
[419] European Parliament resolution of 22 May 2012 on the European Union's Internal Security Strategy ((2010)2308 (INI)), point 26.
[420] For a comprehensive comparison between the proposed Regulation and the proposed Directive, see Bäcker & Hornung 2012, pp. 628-629.
[421] Council of the European Union, 11624/1/13, 02.10.2013, p. 2.

enforcement bodies, the proposed Regulation applies (for example, data stored by TSPs, airline companies and financial entities).[422]

Article 2(3) of the proposed Directive explicitly excludes from the scope of application the processing of data by EU institutions, bodies and agencies.[423] It means that, for instance, data processed by Europol will not be covered by the proposal.[424] As a result, the divergence of data protection frameworks within the AFSJ will remain in the future. The proposal has thus missed the opportunity to finally set up minimum EU rules for data exchanges carried out within the field of police and judicial cooperation.[425]

In conclusion, despite the proposed Directive bringing significant progress with regard to the data protection rules in the field law enforcement, it will not end the current fragmentation of rules. Many EU information systems will be excluded from the scope of the proposal, which means that it will not achieve full harmonisation of EU data protection rules in the field of law enforcement.

### 4.3. Comparative study of the specific data protection provisions in EU data-sharing instruments

As mentioned above, both the current FD 2008/977 and the proposed data protection directive on police and judicial matters explicitly exclude numerous EU data-sharing instruments. The reason for such limitation was mainly political, since some member states thought that by centralising data protection rules in one single act, they would lose authority over the way they regulate security measures. Both the current FD 2008/977 and the proposed Directive include a clause stating that any prior specific rules on data protection will always take preference over the act.[426] Yet, only the framework decision foresees that if sector-specific rules on data protection are more restrictive than those in the act, the former will apply.[427]

---

[422] Council of the European Union, 11109/14, 30.06.2014, p. 5.
[423] This has been criticised by the Committee of the Regions, see OJ C 391, 18.12.2012; and by Belgium, Germany, Spain, Finland, Latvia, Portugal, Romania and Sweden.
[424] This is addressed in chapter 3 of the present study.
[425] In this sense, the EP, supported by the EDPS,[425] has proposed an amendment for extending the scope of the proposal to EU institutions, bodies and agencies,[425] but it needs to be approved by the Commission and the Council. 'Additional EDPS comments on the data protection reform package', European Data Protection Supervisor, 15.03.2013, p. 12; LIBE AM 270-272.
[426] Article 28 of Framework Decision 2008/977/JHA, Article 59 of proposed Directive.
[427] Recital 40 of Framework Decision 2008/977/JHA.

The majority[428] of EU data-sharing instruments within the AFSJ include data protection provisions. Some of these instruments are preventive measures and store data from untargeted individuals, while others process data as a response to a specific criminal investigation. The main problem stemming from these instruments is that they do not have their data protection rules aligned with each other. Not even the preventive measures themselves contain similar rules.

Preventive tools are specifically the proposals for an EU PNR system and an EU TFTS, the APIS, the SIS/SIS II, the VIS, the Eurodac, and the CIS.[429] Table 1.2. presents a comparison of such instruments in light of four different criteria: data retention, data items collected, entities with data access, and individual rights.

*Table 1.2.*

| | **Duration of data storage** | **Categories of data collected** | **Entities with data access** | **Rights of data subject** |
|---|---|---|---|---|
| **EU PNR** | 30 days, and 5 years in a masked out state | 19 (+API) | PIUs | Access, deletion /correction, blockage, judicial redress, compensation |
| **EU TFTS** | Undefined | *Undefined* | FIUs or Europol/Eurojust | *Undefined* |
| **APIS** | 24 hours | 9 | Border authorities | Judicial redress |
| **SIS/SIS II** | 5 or 10 years max. Review after 1 or 3 years. | 10/15 | Border authorities; police and customs authorities; judicial authorities; visa and immigration authorities; Europol and Eurojust; vehicle registration authorities; Interpol. | Access, deletion /correction, judicial redress, compensation |
| **VIS** | 5 years max. | 34 | Border authorities; visa and immigration authorities; designated law enforcement authorities; Europol; third countries or international organisations. | Access, deletion /correction, judicial redress |

[428] This is not the case in Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, OJ L 253, 29.09.2005, pp. 22-24.
[429] The Data Retention Directive was initially included in the matrix, but it was removed after it was declared void by the CJEU.

| | | | | |
|---|---|---|---|---|
| **Eurodac** | 10 years; or 2 years | 12 | National asylum authorities; designed law enforcement authorities; Europol. | Access, deletion /correction, judicial redress, compensation |
| **CIS** | 3 years; 6 years, or 10 years max. Review after 1 year. | 14 | Designated customs administrations; other national authorities; third countries, international/regional organisations | Access, deletion /correction, blockage |

The first thing that is evident from Table 1.2. is that none of these measures for the prevention of crimes coincides from a data protection perspective. The retention of information goes from twenty-four hours, in the case of APIS,[430] up to ten years in SIS and Eurodac systems. After the CJEU declared void the Data Retention Directive, many conclusions can be made regarding these retention rules. The first is that the majority of these retention periods are longer than that established in the annulled directive, which ranged from six months to two years. In the case of the PNR Directive, the period of thirty days does not impede PIUs from accessing unmasked data after that period, so the real retention period is five years. Therefore, in line with the aforementioned Court decision *Commission* v. *Ireland* and / or *Digital Rights Ireland*, these periods of time could be contrary to the EU principles of necessity and proportionality.[431]

As for the number of items collected, they also vary significantly from one instrument to another. For example, CIS has fourteen data categories, whereas VIS collects thirty-four different items. In all cases the data can easily disclose a wide range of information about individuals, such as their dietary habits are, what type of card they are paying with, who they are travelling with, etc. All this information can easily clash with the right to private live[432] and, similarly to the Data Retention Directive, be contrary to Articles 7 and 8 of the Charter of Fundamental Rights.

Regarding the authorities and institutions allowed to access the information, API is the less intrusive system. All the others allow access to law enforcement authorities,[433]

[430] Article 6(1) Council Directive 2004/82/EC.
[431] Boehm & Cole 2014, pp. 67-68 and 80.
[432] Boehm & Cole 2014, p. 69.
[433] This is the case of SIS/SIS II, VIS, Eurodac, CIS and Data Retention Directive. See Article 27 SIS II Regulation, Article 3 VIS Decision, Article 5 and 6 of 2012 Eurodac Proposal, Article 7 CIS Decision and Article 4 Data Retention Directive, and Article 21 ECD.

or even Europol[434] and Eurojust.[435] The main issue of concern is that these broad categories of actors may translate into a very high number of people with access to personal data. For instance, nobody knows what the PIUs composition in the PNR Directive is going to be, or who the 'verifying authorities' of Eurodac are. As Boehm and Cole point out, this imprecision 'leaves room for an arbitrary expansion of the persons who may access the data sets'.[436] They also propose the appointment of an independent body among law enforcement authorities for the control of the access.[437]

Finally, the rights guaranteed to individuals are insufficient in most of the measures. In fact, only the proposed EU PNR Directive offers all basic rights – *i.e.* right to access, right to delete or correct, blockage of data, judicial redress, right to compensation – aligned to Directive 95/46/EC.

Considerably different is Table 1.3. on EU instruments processing information for specific criminal investigations, rather than as a preventive tool. I refer particularly to the Prüm Decisions, the ECRIS initiative, the EIO and the Swedish Initiative.

*Table 1.3.*

| | **Duration of data storage** | **Categories of data collected** | **Entities with data access** | **Rights of data subject** |
|---|---|---|---|---|
| **Prüm Decisions** | 2 years max. | 10 | Competent law enforcement authority | Right to access, right to delete or correct, judicial redress, right to compensation |
| **Swedish Initiative** | _ | 15 | Competent law enforcement authority | _ |
| **ECRIS** | Until they are deleted in the Member State | 13 | Competent law enforcement authority | _ |
| **EIO** | _ | 11 | Competent judicial and law enforcement authority | General mention art.14, judicial redress |

[434] Like in SIS/SIS II, VIS, Eurodac and perhaps the EU TFTS. See Article 7 VIS Decision, Article 7 of Eurodac Regulation, and section 6 of the TFTS communication. On VIS access, see 'European police to gain access to visa database', *Statewatch,* 26.04.2013. Available from http://www.statewatch.org/news/2013/apr/05eu-vis-europol.html [4 November 2014].
[435] Like in SIS/SIS II and perhaps the EU TFTS.
[436] Boehm & Cole 2014, pp. 70, 79.
[437] Boehm & Cole 2014, p. 70.

Following the same matrix as before, Table 1.3. shows that, rather than a divergence among data protection rules, the main problem among these instruments is a lack of rules per se. Therefore, it is not possible to carry out an adequate comparison.

The consequence of having a data-sharing instrument with poor data protection rules is that it might lead to abuses by law enforcement authorities. For example, in ECRIS the consequence of not restricting data processing to specific purposes means that member states can easily use the data for purposes other than criminal proceedings.[438] Likewise, in the case of the EIO Directive, nothing is said about the possibility to make copies of the evidence – nor the retention periods for such copies.[439] For all these measures, except for Prüm, the FD 2008/977 applies subsidiarily.[440] However, as explained above, the framework decision is very broad and does not cover certain aspects of the particular data processing activity.

It is not a coincidence that the Prüm Decision is the only instrument offering a full-fledged data protection framework. A data protection regime in Prüm is particularly important due to the explicit exclusion of this measure from the FD 2008/977 and from the proposed Directive. This exclusion does not translate into a lower data protection framework, but quite the opposite: Article 25 of Council Decision 2008/615 establishes the condition that a Member State can only participate in the exchange of Prüm data if it demonstrates a compliance with all data protection requirements.[441] No similar provision is found in the FD 2008/977 and the Proposal for Police and Criminal Justice Data Protection Directive.

Data security provisions included in FD 2008/977 will also apply those systems which do not contain specific rules on classified information. For instance, the proposed EU TFTS[442] and SIS II[443] include data security requirements, while the Prüm Decisions, the Swedish initiative, the EIO and the ECRIS do not. In the cases where no reference is made on data security, the general rules established in Council Decision 2001/264/EC and its amendment in Council Decision 2011/292/EU apply by default.[444]

---

[438] Article 6(2) of Council Framework Decision 2009/315/JHA.
[439] Mangiaracina 2014, p. 125.
[440] Article 18a of EIO Decision; Recital 18 of ECRIS Decision.
[441] Soleto Muñoz & Fiodorova 2014, p. 159.
[442] Section 4.3 of the TFTS Communication.
[443] Article 10 and Article 16 of SIS II Regulation. See also O'Neill 2012, p. 80.
[444] O'Neill 2012, p. 80.

When looking to understand the reason for the lack of a consistent data protection framework in almost all of the aforementioned instruments we might consider their specific *raison d'être*: all these instruments are used as a response to specific criminal investigations and data processed is already focused on a particular target. Therefore, any data protection limitation could potentially obstruct the ongoing criminal investigation. In any case, the EDPS has already called for an alignment of such instruments with the propos Proposal for Police and Criminal Justice Data Protection Directive.[445]

### 4.4. The purpose limitation and the necessity principles

There are two data protection principles that have been especially controversial in all EU data-sharing systems. These are the purpose limitation principle and the necessity principle.

Looking first at the purpose limitation principle, it is established in Article 6(1)(b) of Directive 95/46/EC. According to the Art. 29 WP, it consists of collecting personal data 'for specified, explicit and legitimate purposes' that must 'not be further processed in a way incompatible with those purposes'.[446] This has often been challenged by the increasing 'function creep' of the existing European information systems. A function creep is the gradual expansion of the use of a system or database, beyond the purpose for which it was originally intended,[447] which is exactly what has happened in many of the aforementioned systems. They were initially created either to develop the European borders or for commercial purposes, but they have been ultimately used – or are expected to be used – as tools for the detection and investigation of crimes.

For instance, the VIS was created to support the common visa policy, and Eurodac was established to prevent asylum seekers from filing multiple asylum applications in different member states simultaneously. Yet, data processed through these systems are now accessed by law enforcement authorities of member states and by Europol to fight terrorism. Therefore, once the information is collected and stored in the EU centralised systems, it can easily be used for other purposes. Likewise, before the adoption of PNR

[445] European Data Protection Supervisor Opinion on the Communication from the Commission to the European Parliament and the Council entitled 'Strengthening law enforcement cooperation in the EU: the European Information Exchange Model' (EIXM), 29.04.2013, p. 7.
[446] Opinion 03/2013 on purpose limitation, WP 203, 02.04.2013.
[447] European Data Protection Supervisor, Eurodac Opinion, 05.09.2012, p. 5.

agreements, booking details (PNR data) collected by airline companies were only processed for commercial purposes. However, the initial collection of PNR data does not correspond today to the final processing based on law enforcement purposes. Another example is found in Article 5(5) of the EU PNR Proposal. It leaves the door open to add other offences to the list established in Articles 1 and 2 of the EU PNR Proposal. According to this provision, it could occur that an police agent requests PNR data invoking the exception of Article 5(5) to investigate a minor offence that is not included onthe list.[448] That would weaken the original purpose for which the proposal was drafted. In this sense, the Art. 29 WP has considered that all the above-mentioned cases are incompatible with the purpose limitation principle.[449]

At this stage, one might wonder what limits should apply in the processing of personal data. According to the Art. 29 WP, the limit should be set by the necessity principle. All instruments include a clause about their compliance with the necessity and proportionality principles. The Art. 29 WP has stressed that the purpose limitation principle should be restricted for any processing in which the data is not necessary to safeguard important interests (Article 13 Directive 95/46/EC). However, the problem is that there are no strict parameters for assessing the necessity to access EU information systems' data by law enforcement authorities. Therefore, in order to conduct an objective examination of the necessity and proportionality, impact assessments in the use of instruments should be always conducted.[450] Unfortunately, the Commission has not always carried out impact assessments before adopting data-sharing systems. For example, the Eurodac proposal launched by the Commission in May 2012 did not include any impact assessment. The EDPS was the first to react to this, arguing that the Commission did not demonstrate any substantive reason for which asylum seekers' data was needed. It then urged the Commission to provide solid evidence and reliable statistics for the need to access Eurodac data.[451] The Europol Joint Supervisory Body (JSB) also published a report in October 2012 examining that particular aspect on Eurodac access. It stated that there was a 'lack of evidence that such access is actually

[448] Boehm & Cole 2014, p. 66.
[449] WP 203, pp. 68-69.
[450] On impact assessments regarding privacy, see Wright D & de Hert P 2012, 'Privacy Impact Assessment', *Springer*, Berlin.
[451] EDPS, Eurodac Opinion, 05.09.2012.

necessary and proportionate for countering terrorism and other serious crimes'.[452] The JSB also noted that:

'Europol's mission to support the EU in preventing and combating all forms of serious international crime and terrorism cannot be seen as separate from the mission of national law enforcement authorities in these crime areas.'[453]

The JSB also called for a careful assessment and demonstrable evidence of the necessity for Europol's access. Consequently, the Council later issued a document with examples of real cases where the comparison of fingerprint data taken at a crime scene had contributed to a criminal investigation.[454] In fact, member states are interested in encouraging the function creep, allowing them to expand accessible systems during the investigation of a crime.

The principles of purpose limitation and necessity were acknowledged by the CJEU in the recent ruling *Commission* v. *Ireland* and *Digital Rights Ireland*. The Court annulled that directive precisely because the necessity of the retained data was not justified. The argument of the Court was that the interference applied 'even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime'.[455]

The same processing of an untargeted person's data occurs in all other instruments studied in this chapter. Therefore, it remains to be seen if the fact that since December 2014 the CJEU has had jurisdiction over former third-pillar measures results in more challenges before the court. Using the same argumentation as in the Data Retention case, other data-sharing instruments are likewise to be disputed in the future.

## 5. Conclusion

In the last fifteen years, the EU has contributed significantly to the adoption of instruments for the prevention and combat of terrorism and other serious crimes. This first chapter has conducted a comprehensive analysis of the measures facilitating the

[452] Opinion of the Joint Supervisory Body of Europol 12/52, with respect to the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of EURODAC, 10.10.2012.
[453] Joint Supervisory Body Opinion, p. 3.
[454] Council of the European Union, 16990/12, 03.12.2012.
[455] Joined Cases C-293/12 and C-594/12, 08.04.2014, para. 58.

exchange of information among member states for law enforcement purposes. Many legal instruments (e.g. the Swedish Initiative and the Prüm Decisions) and information systems (e.g. SIS, VIS and Eurodac) have been added to the traditional MLA mechanism for exchanging crime-related data.

This chapter has identified divergent data protection rules in the existing EU data-sharing instruments, which would ultimately impede the establishment of global data protection standards for security purposes. Moreover, there is a delay in the implementation and a lack of use of these measures. As a result, law enforcement authorities often apply MLA procedures or even informal communication tools for the exchange of data with other member states.

This chapter has also scrutinised whether it is possible to approximate these rules and achieve a common EU data protection framework for the information shared for law enforcement purposes. In order to do that, an in-depth analysis of the data protection laws within the AFSJ has been conducted. It has determined that the Treaty of Lisbon has clearly reinforced the protection of personal data. However, the Treaty establishes limitations when data is processed for law enforcement purposes. These restrictions are seen in Article 39 TEU, Declaration 21 and Protocol 36.

Moreover, Framework Decision 2008/977/JHA and the proposed Directive on data protection for police and judicial cooperation in criminal matters have been minutely examined and compared. Although the proposed Directive introduces many new aspects (e.g. the coverage of pure domestic data transfers, a bigger role from the EP, and the CJEU revision), its wording is still disappointing from a data protection perspective. The main dissatisfaction stemming from the proposed Directive is the restricted scope of the instrument. It excludes data processed by EU agencies such as Europol and Eurojust, Prüm transfers, data exchanged through SIS and CIS, as well as data collected by private companies and later processed by law enforcement authorities. This last limitation sets aside the processing of PNR data, SWIFT data and data collected by TSPs. Another problem is that other EU instruments might find their provisions overlapping with the proposed Directive, causing confusion and uncertainty: in some situations there will be two or more systems applicable; while in others there will be no applicable instrument at the EU level at all.[456]

[456] Hijmans & Scirocco 2009, p. 1524.

In light of the foregoing considerations, it can be concluded that too many instruments and data protection frameworks are converging in the AFSJ. The current complexity of the security environment within the EU blocks the possibility to apply common data protection standards for the information shared among law enforcement agents. The major consequence of this issue is that, if personal data is not equally protected within the EU, the risk of disparities increases for data transfers between the EU and a third country. This is precisely the object of study in the next chapter.

## Chapter 2: Data exchanges for law enforcement purposes between the EU and a third state

Terrorism and other serious crimes are not always demarcated within a specific territory. A terrorist group might commit an attack in France today, and repeat a similar atrocity in Chicago tomorrow. Therefore, member states and the EU itself have strengthened their cooperation with police forces in third countries. As a result, the EU is now competent to adopt international agreements with third countries in the fight against globalised terrorism and other serious crimes.

After an examination of the EU instruments that collect and exchange information among member states for the prevention, combat, investigation and prosecution of crimes, this chapter will focus on the exchange of information beyond the European borders. The feasibility of a global data protection framework will depend to great extent on the consistency among current agreements between the EU and third countries. If international agreements for the exchange of information among law enforcement authorities do not yet have common data protection rules, it will make the establishment of a universal catalogue of data protection principles difficult to achieve.

This chapter is divided into two parts. The first part will examine the great external influences, especially from the US, on current EU counter-terrorism measures. The terrorist attacks of 11 September 2001 caused an increase in the number of measures taken by the EU for the collection, processing and storage of personal data. These measures regulate not only the exchange of information within the EU but also with non-EU countries. Within this context, I will assess the main EU external data-sharing instruments. My contention is that, although the EU has influenced certain third countries' norms, the US rules have mostly shaped the EU security norms. In other words, as the EU is widening its role in the global security environment, it also becomes a 'norm-taker' when US counter-terrorism measures based on the exchange of information are at stake. In order to prove this point I will thoroughly analyse the agreements on mutual legal assistance, passenger name records (PNR), financial data, as well as air and maritime security partnerships between the EU and the US.

The second part of this chapter will study the data protection safeguards for transfers carried out between the EU and a third country. In Chapter 1 I have concluded that there is no consistent EU data protection framework in the field of law enforcement. Does it

imply that data protection provisions of international agreements between the EU and a third country are likewise discrepant? I will examine this below.

## 1. The external dimension of the AFSJ in the fight against terrorism

### 1.1. Origins and evolution

Although the original purpose of the AFSJ was to provide a framework in which the EU and its member states could cooperate for increasing public order, internal peace and security, a parallel external mission has been developed over the last ten years. Threats to the EU internal security have often been originated outside the EU territory.[457] To respond to these threats, the EU institutions have engaged in joint actions with third countries.[458]

The external dimension of the AFSJ stemmed from three correlative events: i) the initiatives in the Tampere European Council of 1999; ii) the global impact of the terrorist attacks of 9/11; and iii) the external strategy proposed in the Hague Programme since 2005.[459] These three episodes acted as 'critical junctures' or key moments that led the EU to conduct institutional reforms in its external security policy.[460] Yet, differences need to be distinguished between the Tampere European Council and the other two events.

First, the main goal of the Tampere European Council[461] was to make better use of the EU competences in the field of external relations. In that sense, the Conclusions of the Presidency underlined the need to achieve a greater coherence between internal and external policies of the EU (point 59 of the Conclusions). A closer cooperation between the Council and the Commission was encouraged. The external dimension of the AFSJ

[457] Wolff, Wichmann & Mounier 2009, p. 11; Lavenex & Wichmann 2009, p. 84; Wesser RA, Marin L & Matera C 2011, 'The external dimension of the EU's Area of Freedom, Security and Justice' in *Crime within the Area of Freedom, Security and Justice. A European Public Order*, eds. Eckes C & Konstadinides T, Cambridge University Press, Cambridge, p. 277.
[458] Pawlak 2009a, 'The external dimension of the Area of Freedom, Security and Justice: Hijacker or hostage of cross□pillarization?', *Journal of European Integration*, vol. 31, no. 1, p. 33.
[459] Wesser, Marin & Matera 2011, pp. 179-180.
[460] Sarah Wolf also identifies also the massacre of 1972 Munich Olympic Games as a 'critical juncture'. See Wolf S 2009, 'The Mediterranean Dimension of EU Counter-terrorism', *European Integration*, vol. 31, no. 1, p. 139.
[461] See the Presidency conclusions of the Tampere European Council (15–16 October 1999). Available from http://www.europarl.europa.eu/summits/tam_en.htm [19 November 2014].

as defined in Tampere was not supposed to be an independent policy, but rather an action complementing the internal AFSJ.[462] In this sense, the declaration stated:

'All competences and instruments at the disposal of the Union, and in particular, in external relations must be used in an integrated and consistent way to build the area of freedom, security and justice.'[463]

The purpose of enhancing external relations within the AFSJ launched in Tampere was later reiterated in the Santa Maria da Feira European Council,[464] as well as in the 'Multi-Presidency Work Programme' on external relations released by the Council in July 2001.[465]

The 9/11 terrorist attacks had a substantial political impact on the AFSJ legislation. Only ten days after the attacks, the European Council conducted a meeting with all the heads of the member states in order to discuss the EU cooperation with the US and how to achieve the strengthening of EU counter-terrorism measures.[466] The same discourse took place during the European Council of Seville one year later.[467]

In 2003, the former High Representative for Common Foreign and Security Policy (CFSP), Javier Solana, drafted a European Security Strategy. It stressed the new multidimensional nature of security[468] in which the EU had to contribute to global security through its external action.[469] Frequent dialogue began between the EU and US officials in order to harmonise police, judicial and border control policy matters. The counter-terrorism policy thus became a priority on both sides of the Atlantic.

Many international agreements on border security and criminal matters were signed between the EU and the US shortly after the attacks. The EU–US agreements on extradition and mutual legal assistance,[470] as well as the agreements between Europol

[462] Wesser, Marin & Matera 2011, p. 180; Cremona M 2008a, 'EU External Action in the JHA Domain: A Legal Perspective', *EUI Working Papers Law* 2008/24, *European University Institute*, Florence, pp. 3.
[463] Presidency conclusions of the Tampere European Council, para. 59.
[464] Santa Maria da Feira European Council, Conclusion of the Presidency, 19-20.06.2000.
[465] Council of the European Union, 10741/01, 12.07.2001.
[466] European Council, 'Conclusions and Plan of Action of the Extraordinary European Council Meeting', 21.09.2001.
[467] European Council, 'Seville European Council Presidency Conclusions' 21–22.06.2002, pp. 31-34.
[468] Longo F 2013, 'Justice and Home Affairs as the new dimension of the European security concept', *European Foreign Affairs Review*, vol. 18, no. 1, p. 37.
[469] Council of the European Union, European Security Strategy, *A secure Europe in a better World*, 12.12.2003.
[470] These agreements are examined in section 2 of this chapter.

and the US[471] were two of these. In addition, the External Security Strategy of 2003 increased the role of the Council in the decision-making process for measures falling under the external dimension of the AFSJ.

Lastly, the Hague Programme, approved in November 2004, also had a significant impact on the expansion of the external dimension of the AFSJ. The programme was a direct consequence of the Madrid terrorist attack of 2004, in which synchronised detonations of bombs were carried out in the city's commuter train system. The Hague Programme aimed at strengthening the cooperation between law enforcement agencies of member states, while consolidating the internal/external nexus of the AFSJ. On 7 July 2005, a similar attack occurred on three underground trains on a bus in central London. The European Council issued several declarations after these attacks,[472] highlighting the need to adopt common measures on the retention of telecommunications data as soon as possible.

The Commission also launched a series of communications[473] encouraging the coordination of counter-terrorism activities among EU institutions and member states. These communications suggested the establishment of an integrated approach on the fight against terrorism, which would give the Commission a more direct involvement in both internal and external security policies. During that period, the Counter-terrorism Working Group (COTER)[474] and the European Union Counter-Terrorism Strategy[475] were also established. Both initiatives dealt with external aspects of terrorism.

The Hague Programme emphasised the necessity to establish coherence between the internal and the external dimensions of the AFSJ in the fight against terrorism. As in the former Tampere Declaration, the Hague Programme considered that external police operations had the ultimate purpose of improving the internal security of the EU.[476] The external dimension of the AFSJ became a priority in the EU agenda and, therefore, the European Council invited the Council and the Commission to draft strategies on that matter.[477] As a result, in 2005 the Commission released a communication for 'a strategy

[471] These agreements are examined in Chapter 3 of the present thesis.
[472] Council of the European Union, 'Declaration on combating terrorism', 25.03.2004; Council of the European Union, 'Declaration on condemning the terrorist attacks on London', 13.07.2005.
[473] COM(2004) 376 final, 18.05.2004; COM (2004) 429 final, 16.06.2004; COM(2004) 698 final, COM(2004) 702 final, COM(2004) 701 final and COM(2004) 700 final, 20.10.2004.
[474] Council of the European Union, 9791/04, 25.05.2004.
[475] Council of the European Union, 14469/4/05, 30.11.2005.
[476] OJ C 53, 03.03.2005, pp. 1-14, point 2.4.
[477] OJ C 53, 03.03.2005, pp. 1-14, point 4.

on the external dimension of the Area of Freedom, Security and Justice'.[478] The communication underlined that the external dimension of the AFSJ had to be conceived as a projection of the internal AFSJ. That communication served as a basis for the Council 'Strategy for the External Dimension of JHA: Global Freedom, Security and Justice'.[479] Together with the Council and the Commission, the EP also promoted the external dimension of the fight against international terrorism,[480] despite its limited competences in the EU decision-making process at that time.[481]

In order to comply with the US demands, the EU concluded many international agreements in the field of security. However, the appropriate legal basis for those agreements was not entirely clear since they had a cross-pillar nature.[482] Some of them were adopted under the internal market clause (e.g. the 2004 EU-US PNR Agreement)[483] through the Community implied powers;[484] while others were adopted under the scope of the third pillar. That was the case of the 2006 and 2007 EU-US PNR Agreements.[485] The Commission used Article 24 TEU in conjunction with Article 38 TEU as the legal bases for concluding such agreements.[486]

New legal bases for the AFSJ were included in the Treaty of Lisbon. Particularly, the treaty includes express provisions for the conclusion of international agreements in two matters: immigration and asylum.[487] However, it does not add any general legal basis for the conclusion of international agreements in the AFSJ. It is a step backwards compared to the pre-Lisbon legal framework. Before Lisbon, Article 38 TEU was the legal basis to conclude international agreements under the scope of the AFSJ, but the provision was removed with the Treaty of Lisbon, so now agreements on criminal cooperation are based on EU implied powers.

There are, however, many issues in the Treaty of Lisbon that have contributed to the strengthening of the external dimension of the AFSJ. According to Article 21(3) TEU,

---

[478] COM(2005) 491 final, 12.10.2005
[479] Council of the European Union, 14366/3/05, 30.11.2005
[480] OJ C 287 E, 29.11.2007, pp. 524-535.
[481] O'Neill 2012, p. 166.
[482] Wesser RA 2010, 'Cross-pillar Mixity: Combining Competences in the Conclusion of EU International Agreements' *in Mixed Agreements Revisited. The EU and its Member States in the World,* eds. Hillion C & Koutrakos P Hart Publishing, pp. 30-55; Cremona 2008a, p. 16; Wesser, Marin & Matera 2011, p. 291.
[483] 2004 EU-US PNR Agreement is examined in section 2.2.2 of this chapter.
[484] Cremona 2008a, pp. 5-6; Monar 2012, 'The External Dimension of the EU's Area of Freedom, Security and Justice. Progress, potential and limitations after the Treaty of Lisbon', report no. 1, *Swedish Institute for European Policy Studies*, Stockholm, pp. 22-23.
[485] 2006 and 2007 EU-US PNR Agreements are also examined in section 2.1.2 of this chapter.
[486] Wesser, Marin & Matera 2011, pp. 289-290; Cremona 2008a, p. 13.
[487] See articles 78(2)(g) and 79(3) TFEU.

external objectives of the EU do not only refer to general external policy issues, but also to those 'external aspects of its other policies' like the external dimension of the AFSJ.[488] Also, the abolishment of pillars ends with the distinction between the first and third-pillar matters of the AFSJ. All fields are now reviewable by the CJEU. Likewise, the Treaty of Lisbon removes the separation between the EU and EC international agreements, now gathered under one single legal basis: Article 218 TFEU. The new procedure for concluding international agreements allows both member states and the EU to participate in the negotiations. The EP is involved in the legislative procedure too, but in a more limited way: in some cases it has to approve the agreement (Article 218(6)(a) TFEU);[489] whereas in others it only has a consultative role (Article 218(6)(b) TFEU).[490]

Since the Treaty of Lisbon, new initiatives within the scope of the external dimension of the AFSJ have been released. The first instrument launched was the Stockholm Programme in December 2009.[491] The programme highlighted that the external dimension was crucial to the successful implementation of the objectives of the programme.[492] Also, it sought a 'greater coherence between external and internal elements of the work' in the AFSJ.[493] The two main priorities of the programme in relation to the external dimension of the AFSJ were the control of migration flows on the one hand, and the improvement of security in Europe on the other.[494] The programme also included new policies connected to external threats such as the fight against cybercrime.[495]

According to the Stockholm Programme, an Internal Security Strategy (ISS) was to be drafted by the Council and the Commission. In this regard, the Council released a 'Draft Internal Security Strategy for the European Union: Towards a European Security Model',[496] and the Commission issued a communication on 'The EU Internal Security Strategy in Action: five steps towards a more secure Europe'.[497] The Commission's

[488] Cremona 2008a, pp. 5 and 8.
[489] The involvement of the EP in the adoption of the SWIFT agreement is discussed in section 3.2. of this chapter.
[490] This is the case, for example, of operational cooperation in internal security matters (Article 87(3) TFEU) and family law matters with cross-border implications (Article 81(3) TFEU).
[491] OJ C 115, 04.05.2010, pp. 1-38
[492] OJ C 115, 04.05.2010, p. 5.
[493] OJ C 115, 04.05.2010, p. 6
[494] OJ C 115, 04.05.2010, pp. 4-5 and 34.
[495] OJ C 115, 04.05.2010, p. 22.
[496] Council of the European Union, 5842/2/10, 23.02.2010.
[497] COM(2010) 673 final, 22.11.2010.

communication established clear objectives, which included the disruption of international crime networks with the creation of a EU PNR Directive, and the prevention of terrorism by cutting off terrorists' access to funding and materials and by following their transactions. The ISS, like the Stockholm Programme, considered that the internal security was increasingly dependent on external security matters.[498]

All the EU institutions approve the existing link between the ISS and external security measures.[499] They acknowledge that internal and external aspects of the EU security are complementary and, therefore, stronger coordination between policies should be promoted. Likewise, AFSJ agencies such as Europol, Eurojust and FRONTEX have strengthened their competences in the field of external action, and they are currently able to conclude cooperation agreements with third countries and non-EU organisations.

### 1.2. Data exchanges for security purposes. The blurry line between the AFSJ and the CFSP/CSDP

As Cremona states, there is not one single external policy within the scope of the AFSJ.[500] Instead, this area is constituted by several integrated policies that, to some extent, are to be achieved in cooperation with third countries. These include the immigration policy, the counter-terrorism policy, and the fight against organised and serious crime, among others.[501] For the purpose of this study, the following paragraphs will focus solely on the law enforcement area and, particularly, on measures consisting of the processing of information for security purposes.

As seen earlier, the number of counter-terrorism measures adopted by the EU institutions has dramatically increased in the last decade, leading to an expansion of the AFSJ. Yet, counter-terrorism is not an exclusive AFSJ matter. The events of 9/11 also strengthened the Common Foreign and Security Policy (CFSP) and the Common

[498] Cremona 2011, p. 6.
[499] European Parliament resolution of 22 May 2012 on the European Union's Internal Security Strategy ((2010)2308 (INI)), point 9; EP on the development of the common security and defence policy following the entry into force of the Lisbon Treaty, 2010/2299(INI), 29.04.2011; Council of the European Union, 14819/1/12, 19.10.2012; Council of the European Union, 14081/1/14, 13.11.2014, p. 7; COM(2013) 179 final, 10.04.2013, p. 17.
[500] Cremona 2008a, pp. 1 and 7.
[501] Trauner F & Carrapiço H 2012, 'The External Dimension of EU Justice and Home Affairs after the Lisbon Treaty: Analysing the Dynamics of Expansion and Diversification', *European Foreign Affairs Review*, vol. 17, no. 2/1, p. 4.

Security and Defence Policy (CSDP) areas through new military missions and partnership agreements with third countries.[502] Before the attacks, neither the CFSP nor the CSDP were conceptualised as tools for fighting terrorism[503] but, in the aftermath of 9/11, many EU institutional documents started to consider the CFSP/CSDP as necessary tools in this area.[504] As a result, it has not always been easy to distinguish which counter-terrorism activities belong to the AFSJ and which are part of the CFSP/CSDP.[505]

The Treaty of Lisbon has sought to ensure consistency between the CFSP/CSDP and the AFSJ by incorporating Article 21(3) TEU.[506] The Treaty has also created a new body: The European External Action Service (EEAS), which is led by the EU High Representative of the Union for Foreign Affairs and Security Policy. The fact that the High Representative is both president of the Foreign Affairs Council and Vice-President of the Commission shows the EU's aim of ensuring consistency of the Union's external action.[507] The strategic link between the CFSP/CSDP and the AFSJ is also stressed in the Stockholm Programme. It highlights that 'CSDP missions also make an important contribution to the Union's internal security in their efforts to support the fight against serious transnational crime'.[508]

Determining which counter-terrorist activities that are part of the CSDP and which fall under the AFSJ is not always clear-cut. That debate is found, for instance, in missions carried out by police agents beyond the EU territory. The EU has eleven civilian CSDP operations ongoing in Ukraine, Georgia, the Palestinian Territories, Kosovo, Libya, Afghanistan, the Democratic Republic of Congo, Mali, Niger, and the

---

[502] Wolf S 2009, 'The Mediterranean Dimension of EU Counter-terrorism', *European Integration*, vol. 31, no. 1, p. 146.
[503] Ferreira-Pereira LC & Oliveira Martins B 2012, 'The external dimension of the European Union's counter-terrorism: an introduction to empirical and theoretical developments', *European Security*, vol. 21, no. 4, p. 541.
[504] See Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001; Declaration on Combating Terrorism, 25.3.2004; and Conceptual Framework on the ECDP dimension of the fight against terrorism.
[505] Cremona 2008a, p. 7; Longo 2013, pp. 29-46; Monar 2012, p. 46; Wesser, Marin & Matera 2011, p. 277; Trauner & Carrapiço 2012, pp. 11-12; Wolff, Wichmann & Mounier 2009; Kurowska X & Pawlak P 2009, 'Introduction: The Politics of European Security Policies', *Perspectives on European Politics and Society*, vol. 10 no. 4, pp. 474-485; Schroeder UC 2009, 'Strategy by Stealth? The Development of EU Internal and External Security Strategies', *Perspectives on European Politics and Society*, vol. 10 no. 4, pp. 486-505.
[506] It establishes that 'the Union shall ensure consistency between the different areas of its external action and between these and its other policies. The Council and the Commission, assisted by the High Representative of the Union for Foreign Affairs and Security Policy, shall ensure that consistency and shall cooperate to that effect'.
[507] Article 18(4) TEU.
[508] Stockholm programme, point 7.1.

group of Djibouti, Somalia, Seychelles, Tanzania and Yemen. Likewise, it has four military missions in Somalia, Atalanta, Mali and the Central African Republic.[509] In the theoretical framework, Article 43(1) TEU establishes that civilian and military operations 'may contribute to the fight against terrorism'.[510] In practice, military bodies are often seen on the scene after a terrorist attack. For instance, Spanish military forces were deployed at several train stations in Spain after the attacks of 11 March 2004,[511] and France deployed more than 10,000 military troops after the recent shootings in Paris.[512]

A lot of information is processed during civilian and military missions. Police agents who are part of a CSDP mission often gather intelligence and pass it to agencies concerned with internal security (e.g. Europol, FRONTEX[513] and CEPOL) and member states' law enforcement officers.[514] For instance, one of the main focuses of the civilian mission in Niger is to find 'ways for the different authorities responsible for security to collect and share information'.[515] Likewise, the mission strategy in Mali includes the exchange of operational information for combating the illicit trafficking of cocaine.[516] As for the mission taking place in Moldova and Ukraine, the mandate includes the improvement of cross-border cooperation and information exchange to prevent and detect smuggling, trafficking of goods and human beings, and customs fraud.[517] Most recently, the European External Action Service (EEAS) has signed a cooperation

---

[509] EEAS website, ongoing missions and operations available from http://www.eeas.europa.eu/csdp/missions-and-operations/index_en.htm [20 November 2014].

[510] Yet, the added value of these civilian/military missions in the field of counter-terrorism has been often questioned. See Coolsaet 2010, p. 871; Oliveira Martins B & Ferreira-Pereira LC 2012, 'Stepping inside? CSDP missions and EU counter-terrorism', *European Security*, vol. 21, no. 4, pp. 537-556; Ferreira-Pereira & Oliveira Martins 2012, p. 467; Argomaniz J 2012b, 'A rhetorical spillover? Exploring the link between the European Union Common Security and Defence Policy (CSDF) and the external dimension in the EU counterterrorism', *European Foreign Affairs Review*, vol. 17, no. 2/1, p. 50.

[511] Pulido Gragera J 2004, 'El papel de la inteligencia en la PESD', *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional*, Dirección General de Relaciones Institucionales de la Defensa. Instituto Español de Estudios Estratégicos, Grupo de Trabajo número 5/04, p. 79.

[512] Blachier G & Irish J 2015, 'France mobilizes 10,000 troops at home after Paris shootings', *Reuters*, 12 January. Available from www.reuters.com [1 February 2015].

[513] See for instance, the EU Border Assistance Mission (EUBAM) in Libya, available from www.eeas.europa.eu 20 November 2014].

[514] 'Plans emerge for the collection of personal data outside European borders to obtain comprehensive situational awareness and intelligence support', *Statewatch*, 30.10.2012. Available from http://www.statewatch.org [20 November 2014].

[515] EEAS website, EUCAP SAHEL Niger, mission description available from www.eeas.europa.eu [20 November 2014].

[516] EEAS, Strategy for Security and Development in the Sahel, available from www.eeas.europa.eu [20 November 2014].

[517] EEAS, European Union Border Assistance Mission to Moldova and Ukraine, available from www.eeas.europa.eu [20 November 2014].

arrangement with the European Gendarmerie Force[518] that also covers the exchange of classified information collected during the CSDP missions.[519]

Another example of data processing in the area of external security is found in the different associations,[520] partnerships[521] and cooperation agreements that the EU concludes with third countries.[522] The majority of these agreements are not CFSP instruments, but mixed agreements. Yet, they tackle issues related to international security and defence diplomacy. Since 2005[523] they have included clauses on confidentiality of data for the fight against terrorism. These provisions are called 'counter-terrorism clauses' and allow the EU to obtain information collected by third countries on terrorist groups and networks. They are usually elaborated on a case-by-case basis,[524] but follow similar templates.[525]

Despite the recent EEAS efforts to clarify the way data is exchanged between CFSP bodies and AFSJ agencies,[526] more detailed information is needed. It is unclear, for example, how information gathered during CSDP missions is disseminated at the EU level by the EU Intelligence Analysis Centre (IntCen) and by the Intelligence Division of the European Military Staff.[527] IntCen belongs to the EEAS and its mandate tackles both internal and external security areas. It is composed of more than 100 staff members, 70% of which are intelligence officials in the member states.[528] One of IntCen's basic functions is the exchange of intelligence and the drafting of terrorism

[518] This force became operational in 2006 and it currently gathers police officers of seven member states: France, Italy, the Netherlands, Portugal, Spain, Romania and Poland.
[519] EEAS, Cooperation with the European Gendarmerie Force (EUROGENDFOR) under the Common Security and Defence Policy - Explanatory brief, EEAS 01207/14, 16.06.2014.
[520] See, for instance, Article 90 of the Euro-Mediterranean Agreement establishing an Association between the European Community and its Member States, of the one part, and the People's Democratic Republic of Algeria, of the other part. OJ L 265, 10.10.2005, pp. 1-228.
[521] The notion of 'partnership' was firstly introduced in the Council's JHA External Strategy of 2005.
[522] See, for instance, Article 5 of the Framework Agreement on Comprehensive Partnership and cooperation between the European Community and its Member States, of the one part, and the Republic of Indonesia, of the other part. Council of the European Union, 14032/09, 21.10.2009.
[523] The inclusion of counter-terrorism clauses was agreed in November 2005 EUROMED Summit (Barcelona), by the adoption of a 'Code of Conduct on the Prevention of Terrorism'. Available from http://eeas.europa.eu/euromed/summit1105/terrorism_en.pdf [20 November 2014].
[524] Wolf 2009, p. 148.
[525] See, for instance, Article 90 of the Euro-Mediterranean Association Agreement (EMAA) concluded with Algeria, 22.4.2002, and Article 59 of the EMAA Agreement concluded with Egypt, 25.6. 2001.
[526] EEAS, 'Strengthening Ties between CSDP and FSJ: Road Map implementation. Second annual progress report', 02230/13, 14.11.2013.
[527] 'EU: Plans emerge for the collection of personal data outside European borders to obtain comprehensive situational awareness and intelligence support', *Statewatch,* 01.10.2012. Available from http://www.statewatch.org [20 November 2014].
[528] Hillebrand 2012, p. 30.

assessments as part of its counter-terrorism analytical task.[529] IntCen analysts often travel to crisis zones and CSDP operation locations to gain the necessary data for their counter-terrorism reports.[530] Yet, it is not clear whether all IntCen data exchanges fall under the scope of the CFSP, or whether some of them belong to the AFSJ.[531]

### 1.3. Questioning the scope and purposes of Article 39 TEU

In light of the foregoing considerations, it is important to examine the legal consequences of considering a counter-terrorism measure as part of the external dimension of the AFSJ, or as part of the CFSP/CSDP.

In certain areas, the Treaty of Lisbon has incorporated dual legal bases, one under the scope of the CFSP and one as a non-CFSP policy. The reason for that is to offer two different decision-making processes for the same purpose: one is adopted under the ordinary legislative procedure, while the other falls under the unanimous decision of the Council. There is no prioritisation in the application of these two legal bases. The CJEU is responsible to decide case-by-case the suitable legal basis.[532]

The CJEU has issued a landmark case that will probably have an impact on the unclear dichotomy between CFSP and AFSJ. In the ruling, the CJEU decided the adequate legal basis on EU restrictive measures on the freezing of assets. Before the Treaty of Lisbon, restrictive measures against individuals within the EU were adopted under ex Articles 60 and 301 TEC. Article 301 TEC was the basis for economic sanctions against third states, and Article 60 was the legal basis for necessary urgent measures on the movement of capital on payments to the third countries concerned (e.g. freezing funds). However, it was not clear whether economic sanctions could be adopted against individuals, since they were not explicitly regulated in the treaties. In *Kadi*, the CJEU solved that question by applying together ex Articles 60, 301 and 308 TEC as the legal basis for economic sanctions against individuals.[533]

---

[529] Argomaniz, 2012b, p. 50.
[530] Cross MKC 2013, 'A European transgovernmental intelligence network and the role of IntCen', *Perspectives on European Politics and Society*, vol. 14 no. 3, p. 393.
[531] Further analysis about IntCen is carried out in Chapter 4, section 5.1.
[532] Article 40 TEU.
[533] On the issue of Community competence to adopt restrictive measures, Cremona M 2009, 'EC competence, 'Smart Sanctions' and the Kadi case', in *Challenging the EU Counter-terrorism Measures through the Courts*, eds Cremona M, Francioni F & Poli P, EUI Working Papers AEL 2009/10, Florence, pp. 71-98.

The Treaty of Lisbon incorporates two different legal bases dealing with restrictive measures regarding the freezing of assets. Each of them has specific aims and functions: Article 215 TFEU (replacing Article 301 TEC) regulates the adoption of restrictive measures against individuals – economic and non-economic. In contrast, Article 75 TFEU establishes that the EP and the Council, through the ordinary legislative procedure, need to adopt administrative measures on capital movements and payments such as 'the freezing of funds, financial assets or economic gains belonging to, or owned or held by, natural or legal persons, groups or non-State entities'.

Thus, instruments under Article 75(1) TFEU are adopted under the ordinary legislative procedure by the EP and the Council, whereas measures authorised under Article 215 TFEU require a CFSP act approved by the Council on a joint proposal from the High Representative and the Commission. Here, the EP is only informed thereof.

The controversy arose with regard to the EU Council Regulation[534] amending Regulation (EC) No 881/2002. That Regulation implemented a UN Resolution about the freezing of funds of certain persons and entities associated with Osama bin Laden, the Al-Qaeda network and the Taliban. It was adopted on the basis of Article 215(2) TFEU and not on the basis of Article 75 TFEU. The EP argued that the contested regulation was adopted under the wrong legal basis. It maintained that Article 75 TFEU was the right basis for adopting restrictive measures aimed at combating terrorism. However, the Council took the opposite position. It claimed that the contested regulation against international terrorism pertained to the CFSP, because it fell under the scope of the EU's external action. Furthermore, the Council made a distinction between international or external terrorism, on the one hand, and internal terrorism, on the other.

This lack of clarity on the proper legal basis persisted among the EU institutions[535] and legal scholars[536] until the CJEU issued the decision in July 2012. The CJEU decided

[534] Council Regulation (EU) No 1286/2009 of 22 December 2009 amending Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Osama bin Laden, the Al-Qaeda network and the Taliban.

[535] With respect to the confusion among EU institutions on Article 75, the Commission (DG HOME) organised many expert meetings to discuss and clarify with member states (MS), the Council Secretariat and the Counter Terrorism Coordinator the scope and application of Article 75 TFEU (for instance, Council of the European Union, 15062/11, 17.10.2011). Likewise, the EP encouraged the proposal for a framework for administrative measures such as freezing of the funds of persons suspected of terrorism pursuant to Article 75 TFEU. See European Parliament resolution of 22 May 2012 on the European Union's Internal Security Strategy ((2010)2308 (INI)), point 14.

[536] See, for instance, Cremona M 2008b, 'Defining Competence in EU External Relations: Lessons From the Treaty Reform Process' in *Law and Practice of EU External Relations*, eds. Dashwood & Maresceau, Cambridge, pp. 34-69; Hinarejos A 2009, 'Judicial Control in the European Union. Reforming Jurisdiction in the Intergovernmental Pillars', *Oxford Studies in European Law*, pp. 154-163.

that the proper legal basis for adopting the EU Council Regulation of freezing of funds was Article 215 TFEU.[537] That decision supported the Advocate General Bot's reasoning.[538] Bot had considered that the action came from the international stage and, therefore, the objective of preserving peace and strengthening international security had to be regarded as falling within the sphere of the CFSP. To the same conclusion, the CJEU explained that ex Articles 60 and 301 TEC mirrored Article 215 TFEU and not Article 75 TFEU.[539] The court's arguments were based on the idea that Article 215 is appropriate where the EU is implementing an UN policy and there is a CSFP decision to that effect. In contrast, Article 75 TFEU may be used for the non-UN security measures. The judgment is a clear evidence of how decisive the interpretation of the CJEU can be, even when the contested legislation falls within the scope of the CFSP.

However, the argument used by the court to justify the legal basis of restrictive measures have not fully solved the blurry delimitation of CFSP and AFSJ competences in the field of external security measures. Another CFSP/AFSJ duality of legal basis needs to be interpreted by the Court. This time the controversy arises with regard to Article 16 TFEU and Article 39 TEU concerning the right to data protection. The Treaty of Lisbon offers in Article 16 TFEU a specific provision regarding the protection of personal data within the EU territory. It establishes that 'everyone has the right to the protection of personal data concerning them'. Yet, the treaty has also included a way of enacting specific data protection rules in the context of the CFSP. Article 39 TEU states that, in derogation of Article 16(2) TFEU, the Council can adopt a special decision laying down the rules relating to data protection and the free movement of such data when member states are acting within the field of CFSP.

The relationship between Article 16 TFEU and Article 39 TEU is unclear. There is no document specifying in which cases Article 39 TEU should apply, derogating the EU data protection general rules. It is, however, apparent that Article 39 will limit the role of the CJEU and the EP. The CJEU will not solve any question relating to the interpretation and application of Article 39, unless it refers to the determination of the proper scope of the two articles to ensure compliance with Article 40 TEU. Regarding

---

[537] Case C-130/10, 12.07.2012. On this case, see Van Elsuwege P 2014, 'The interface between the Area of Freedom, Security and Justice and the Common Foreign and Security Policy in the European Union: Legal constraints to political objectives' in *Freedom, Security and Justice in the European Union. Internal and External Dimensions of Increased Cooperation after the Lisbon Treaty*, eds. Holzhacker RL & Luif P, Springer, Berlin, pp. 130-135.
[538] Advocate General Bot's Opinion on Parliament v. Council, Case C-130/10, 31.01.2012.
[539] Case C-130/10, 12.07.2012, para. 51-54.

the EP, this institution will be excluded from the decision-making process of any instrument based on Article 39 TEU.

However, there is positive a way of interpreting the existence of Article 39 TEU. One could see the provision as a tool for ensuring that data protection also applies in the CFSP sphere, in contrast to the pre-Lisbon regime. For instance, recent PNR agreements with the US, Canada and Australia have been based on Article 82(1)(d) TFEU and 87(2)(a) TFEU, in conjunction with Article 218(6)(a) TFEU. These international agreements fall under the scope of the AFSJ and they have been brought forward under Article 16 TFEU. Yet, it could occur that a future data-sharing agreement for security purposes is based on Article 39 TEU. This legal basis would guarantee minimum data protection safeguards, avoiding a divergent regulation among member states.

As will be examined in Chapter 4 of this thesis, a possible use of Article 39 could emerge from the information gathered by EU IntCen as well as police agents in CSDP missions. From the opinion of the Advocate General Bot in the Mauritius case[540] it could also be deduced that Article 39 TEU applies in the collection of records of pirates operating off Somalia, which are then made available to the Union.[541]

Either way, the fact that Article 39 TEU has never been used today shows how far the external dimension of the AFSJ can reach. The EDPS has recommended the the Commission present, as soon as possible, common rules for the CFSP based on Article 39 TEU.[542] Only with a clarification from the Commission or from the CJEU, we will be able to discover what purpose this provision intends to fulfil.

### 2. International agreements for exchanging information

The EU has developed many partnerships with strategic countries for cooperating in the exchange of crime-related information. For instance, a special link has been established between the EU and Russia for the fight against terrorism based on a Memorandum of Understanding (MoU),[543] a cooperation agreement with Europol,[544] and a Joint Statement on counter-terrorism.[545] Another example is found in the agreement on

[540] Case C-658/11, 21.12.2011.
[541] See Opinion of the Advocate General Bot on the Case C-658/11, 30.01.2014.
[542] EDPS, Opinion of the European Data Protection Supervisor on the data protection reform package, 07.03.2012, p. 6.
[543] European Commission, COM 2008 740 final, 05.11.2008.
[544] Europol agreements are examined in chapter 4 of this thesis.
[545] EU-Russia Joint Statement on Counter-terrorism, 11.11.2002.

mutual legal assistance in criminal matters between the EU and Japan.[546] That agreement brought both parties closer in terms of the management of criminal justice. Finally, it is no coincidence that any partnership agreement between the EU and a third country would include a 'counter-terrorism clause'.

The following analysis will focus mainly on the bilateral cooperation between the EU and the US. The reason for this delimitation is that the cooperation between these parties constitutes the most developed to date, tackling numerous (if not all) important legal issues regarding the EU external security instruments.

The EU maintains a very close relationship with the US authorities. They established diplomatic relations as early as 1953, and their cooperation was formalised for the first time in 1990.[547] In the last decade, numerous agreements have been adopted between the two parties.[548] Also, foreign policy, collective security and trade issues have been discussed in regular transatlantic meetings.[549] In the particular field of security, the EU has always cooperated closely with the US. After World War II, the US became the protector of the European countries against the Soviet Union through the Marshall Plan and the establishment of North Atlantic Treaty Organisation (NATO). In exchange, the EU supported the US interests during the American-Russian confrontation. In the post-Cold war era, the US interests in protecting Europe decreased and this brought uncertainty about what role NATO was going to play.

However, during the nineties both actors continued cooperating in diverse security issues.[550] They set up a partnership for security areas through the following events: a) annual EU-US Summit meetings,[551] b) the 1995 New Transatlantic Agenda (NTA), c) the Joint EU-US Action Plan, d) the 1999 Transatlantic Legislators' Dialogue (TLD), and e) the Transatlantic Group on Counter-terrorism.

The existing security cooperation between the two has expanded into the field of criminal matters since 2001, following the 9/11 attacks. The US enlarged its counter-

[546] OJ L 39, 12.02.2010, p. 3.
[547] Transatlantic Declaration on EC-US Relations, 1990. Available from http://www.eeas.europa.eu/us/docs/trans_declaration_90_en.pdf [21 November 2014].
[548] See, for instance, OJ C 298 E, 08.12.2006, 226 and OJ C 117 E, 06.05.2010, p. 198.
[549] See the EU-USA Transatlantic Partnership Agreement, P6_TA(2006)0238, 01.6.2006; and the Transatlantic Legislators' Dialogue (TLD) between Members of the Congress and MEPs, available from http://www.europarl.europa.eu/intcoop/tld/default_en.htm [21 November 2014].
[550] For a more detailed analysis of the US-EU security history, see Rees W 2011, '*The US-EU Security Relationship: The Tensions between a European and a Global Agenda'*, Palgrave Macmillan, Basingstoke, pp. 1-11.
[551] U.S.-EU Summit in London on May 18, 1998; U.S.-EU Summit in Bonn, Germany, on June 21, 1999; U.S.-EU Joint Statements on December 17, 1999. Available from http://useu.usmission.gov/us_eu_summits.html [21 November 2014].

terrorism policy on the basis of the start of a 'war on terror', and it called for the support to all countries, threatening that they were either with them or against them.[552] Essentially, the US authorities were interested in establishing closer cooperation with the EU institutions and its member states because there were at that time many visa-exempt Western European jihadists[553] who could easily fly to the US. In fact, Al-Qaeda cells had already been detected in some member states, and several individuals were arrested in Belgium, France, Germany, Italy, Spain and the UK as coordinators of the 9/11 attacks.[554] NATO invoked its collective defence clause six hours after the event.[555] According to Article 5 of the Washington Treaty '[t]he Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them'. Moreover, on 20 September of that year, the EU Justice and Home Affairs Council adopted eight broad initiatives encouraging the cooperation with the US[556] and, one month later, George W. Bush suggested the Commission enhance their cooperation on counter-terrorism measures.[557]

The collaboration with the US in the field of law enforcement became a top priority within the EU. Many US agencies included international relations departments and, simultaneously, the DG JHA in the European Commission enhanced its external competences.[558] However, initially the EU and the US developed different counter-terrorism approaches: while the US counter-terrorism strategy focused on the increase of military measures and the use of force, the EU counter-terrorism programme tended to prioritise preventive measures through law enforcement and intelligence agencies.[559] Therefore, the EU has usually been identified as a 'civilian' or 'soft power' because it promotes non-military and non-coercive measures; whereas the US has been defined as a 'hard power', which exports its values with the use of force if necessary.[560]

---

[552] Kaunert, Léonard & MacKenzie 2012, p. 475.
[553] Argomaniz 2009, p. 125.
[554] Archick 2013, p. 1.
[555] Monar J 2005, 'The European Union and the challenge of September 11, 2001: Potential and limits of a 'new' actor in the fight against international terrorism' in *September 11, 2001: A turning point in international and domestic law?*, eds. Eden P & O'Donnell, Transnational Publishers, Inc, Ardsley, NYC, p. 411.
[556] Council of the European Union, 12156/01, 25.09.2001, pp. 10-12.
[557] 'Text of US letter from Bush with demands for EU for cooperation', *Statewatch*, 01.11.2001. Available from www.statewatch.org [21 November 2014].
[558] Pawlak 2009b, 'Network Politics in Transatlantic Homeland Security Cooperation', *Perspectives on European Politics and Society*, vol. 10 no. 4, pp. 560-581, p. 567.
[559] Porter & Bendiek 2012, p. 498. In this regard, Ferreira-Pereira and Martins question whether the EU has really opted for legal measures over military and political sanctions, or it is only the result of the complexity of terrorism issues within the EU. See Ferreira-Pereira & Oliveira Martins 2012, p. 465.
[560] Rees 2011, pp. 22-28.

The influence of the US security strategy within the EU is today unquestionable. Specific examples of this impact are found in the 2003 European Security Strategy, which was adopted after the US National Security Strategy in 2002;[561] the EU-US agreements on security matters, influenced by the 2004 Intelligence Reform and Terrorism Prevention Act[562] and the 2004 EU-US Declaration on combating terrorism;[563] or the creation of the overall EU Counter-terrorism Strategy of 2005.[564] They all indicate the important role played by the US authorities in shaping EU interests.

Under the Treaty of Lisbon, new forms of cooperation between the EU and the US were established. The EU-US 'Declaration on Counter-terrorism' of 2010,[565] and President Obama's National Security Strategy (NSS) for Counter-terrorism of 2011[566] show how the EU-US partnership continues to be a priority on both sides of the Atlantic. Through these strategies, both parties have agreed to prioritise preventive measures over military intervention.[567] As a result, they organise regular meetings between the EU institutions and the Secretary of State, the US Attorney General and the Secretary of Homeland Security to address counter-terrorism issues.[568]

Many divergences remain, however, between the EU and the US in addressing security challenges. They have tried to prove their similar goals by emphasising shared transatlantic values such as democracy, rule of law, market economy and human rights.[569] However, in reality, the two parties have not always shared the same objectives in addressing security challenges. This lack of an 'alliance of values' has resulted in a

[561] Ferreira-Pereira & Oliveira Martins 2012, p. 465.
[562] Act to reform the intelligence community and the intelligence and intelligence-related activities of the United States Government, and for other purposes, PUBLIC LAW 108–458—DEC. 17, 2004. Available from http://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf [21 November 2014].
[563] Council of the European Union, 10760/04 (Presse 205), 26.06.2004.
[564] Council of the European Union, 14469/05, 30.11.2005, p. 7.
[565] EU-US and Member States 2010 Declaration on Counterterrorism, 03.06.2010.
[566] National Agenda for Counterterrorism, 06.06.2011, p. 15. Available from http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf [21 November 2014].
[567] Porter & Bendiek 2012, p. 500.
[568] Archick 2013, p. 4.
[569] Rees 2011, p. 29; European Parliament, P7_TA(2013)0280, 23.6.2013, para. 26. See also George W. Bush's 'Address to Nation on the Terrorist Attacks', joint session of Congress on Thursday night, 20.9.2001. Available from http://www.presidency.ucsb.edu/ws/?pid=58057 [21 November 2014]; Council of the European Union, 11116/05 (Presse 187), Extraordinary Council meeting Justice and Home Affairs, Brussels, 13.7.2005, p. 6. See also the values of the EU in Article 2 TEU.

decrease of mutual trust between them, especially after the Snowden revelations,[570] as will be analysed in Chapter 4 of this thesis.

The next section analyses the current data-sharing agreements between the EU and the US based on security matters. It focuses specifically on the Mutual Legal Assistance (MLA) agreement, the Passenger Name Records (PNR) agreement, the SWIFT agreement, and the EU-US agreements on air and maritime security partnership. The analysis will demonstrate that there is a clear US influence in each of these agreements. After that, returning to the already mentioned blurry line between the CFSP and the AFSJ, the implications resulting from the choice of an AFSJ legal basis for all international agreements adopted between the EU and the US will be examined.

### 2.1. Data-sharing agreements between the EU and the US

There are different ways to exchange crime-related information between the EU and the US. De Busser distinguishes between judicial requests through rogatory letters, subpoenas issued by national courts, informal contacts between police authorities, and the prior adoption of an agreement between both parties.[571] This section examines only the latter of these four suppositions.

As explained above, not only are member states able to conclude data-sharing agreements in the field of law enforcement with third countries[572] but the EU itself also has the competence for that. A few agreements between the EU and the US on the collection, storage, processing, analysis and exchange of relevant information have been concluded using Articles 87(2)(a) and 218 TFEU (ex Articles 24 and 38 TEU). In fact, having the EU as a partner has been very attractive for third countries, which have often preferred to submit one single initiative to the Union as a whole, rather than to negotiate criminal issues with each Member State individually.[573]

The necessity for data-sharing agreements has emerged from the increasingly transnational nature of crimes, which often affect multiple countries or even multiple continents. These agreements have expanded considerably after 9/11. They are part of

[570] Commission Communication on Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final, 27.11.2013.
[571] De Busser 2009, pp. 307-310.
[572] See, for instance, the agreement between Germany and the US on the exchange of DNA and fingerprint data: 'Nachverhandlungen des deutsch-amerikanischen Abkommens zum Austausch von DNA- und Fingerabdruckdaten', *Deutscher Bundestag*, Drucksache 18/1407 18. Wahlperiode, 9.5.2014.
[573] Monar 2012, p. 71.

the external dimension of the AFSJ, and they mainly address issues on international criminal justice (e.g. the MLA treaties) and cooperation on law enforcement (e.g. the PNR agreements). The following sub-sections examine the main agreements concluded between the EU and the US consisting in the exchange of information for the prevention, combat, investigation and prosecution of crimes.

### *2.1.1. The EU-US Mutual Legal Assistance Agreement*

The EU-US Mutual Legal Assistance Agreement (EU-US MLA Agreement) was concluded two years after the 9/11 attacks, because of the continuous US pressures expressing the need to access data from police authorities and telecommunication service providers (TSPs) located in any of the EU countries. As an example, since the EU-US MLA Agreement is in force, judiciary authorities on both sides have access to bank accounts and can get financial data for the investigation of a crime.

The EU-US MLA Agreement was not the first instrument of mutual assistance between both parties. Before the conclusion of that agreement, sixteen countries in Europe had already signed bilateral mutual legal assistance treaties (MLATs) with the US authorities,[574] and some existing UN Conventions also included mutual legal assistance clauses.[575] At the EU level, the Council of Europe has had a Convention on MLA since 1959, and the EU adopted a Convention on Mutual Assistance in Criminal Matters between the member states and the European Union a year before the 9/11 attacks.[576]

On 20 September 2001, The JHA Council announced the initiation of negotiations for an EU-US judicial cooperation agreement. In a letter sent by the former US President George W. Bush to the Commission President Prodi on 16 October 2001, it was requested that '[w]henever possible, permit urgent MLAT requests to be made orally, with follow-up by formal written requests'.[577] The mandate for negotiating the agreement was adopted on 26 April 2002, the day that the Commission negotiations

[574] These were: Austria (1995), Belgium (1988), Cyprus (1999), the Czech Republic (1998), Estonia (1998), France (1998), Greece (1999), Hungary (1994), Italy (1982), Latvia (1997), Lithuania (1998), Luxembourg (1997), Poland (1996), Romania (1999), Spain (1990), the UK (1994 and amended 2001).
[575] For instance the Convention against Illicit Trafficking in Drugs, the Convention for the Suppression of the Financing of Terrorism, Convention against Transnational Organized Crime (TOC), Convention against Corruption. See De Busser 2009, pp. 312-313.
[576] OJ C 197, 12.07.2000, pp. 3-23.
[577] 'Text of US letter from Bush with demands for EU for cooperation', *Statewatch*, 01.11.2001. Available from www.statewatch.org [21 November 2014].

with the US Department of Justice (DoJ) began. The agreement was signed the following year on 25 July 2003. For the first time[578] the Commission used ex Articles 24 and 38 TEU[579] as legal bases for concluding an international agreement between the EU and a third country in the field of judicial cooperation in criminal matters.[580]

When the EU-US MLA Agreement was adopted, only Bulgaria, Finland, Malta, Portugal, Slovakia and Slovenia did not already have a bilateral MLAT with the US.[581] According to Article 3 of the agreement, existing bilateral treaties between member states and the US would remain in force, so there would be no replacement with the EU-US MLA Agreement. Moreover, pursuant to Article 14 a possibility to conclude future bilateral treaties with the US remained open. As for the new provisions included in the agreement, Article 4 restricted the banking secrecy, Article 5 allowed the creation of Joint Investigation Teams (JITs), Article 6 permitted videoconferences and Article 9 gave the possibility to share information as evidence before a court.

However, a lack of use of MLA instruments between the EU (or its member states) and the US has been identified in recent years. Problems commenced with the ratification process of the EU-US MLA Agreement. Some of the member states have been extremely slow in ratifying the agreement, which only came into force on 1 February 2010.[582] But even after the ratification, member states have raised other issues of concern about the use of this instrument. In the last questionnaire sent by the Council,[583] the Czech Republic, Malta, Poland, Romania and Slovakia complained about the enormous length of time that the whole procedure takes from the issuing of a request to its execution.[584] Likewise, Spain highlighted obstacles in executing requests about e-mail content information at an early stage of an investigation because, according to the Spanish system, information can only be provided by a Spanish judge after the pre trial investigation. Finally, a problem regarding the lack of use of the MLA channel among

[578] Together with the EU-US Extradition Agreement, also signed on that very same day.
[579] On this specific legal nature, see Stessens G 2008, 'The EU-US Agreements on extradition and on mutual legal assistance', *Justice, Liberty, Security: New Challenges for EU External Relations,* eds. Martenczuk B & van Thiel S, VUBPress, Brussels, pp. 142-146.
[580] Faull J & Soreca L 2008, 'EU-US Relations injustice and Home Affairs', *Justice, Liberty, Security: New Challenges for EU External Relations*, eds. Martenczuk B & van Thiel S, VUBPress, Brussels, p. 406.
[581] MacKenzie A 2012, 'The external dimension of European homeland security', *European Homeland Security. A European strategy in the making?*, eds. Kaunert C, Leonard S & Pawlak P, Routledge, New York, p. 107.
[582] 'U.S./EU Agreements on Mutual Legal Assistance and Extradition Enter into Force', U.S. Department of Justice Press Release, 01.02.2010.
[583] Council of the European Union, 14253/2/12, 24.10.2012, pp. 2-4.
[584] Council of the European Union, 14253/2/12, 24.10.2012, pp.13-14.

member states has been identified. Many countries often acquire data stored by companies in another country without any mutual legal assistance request. The same occurs with data stored by US authorities; member states usually contact them informally through email.[585]

From the US side, the Review Group on Intelligence and Communications Technologies also detected some current problems regarding the use of MLA procedures. First of all, the Group noted that the procedure is slow, taking on average ten months or longer. There is also no online submission form for such procedures, so many governments do not know how to send a request, or what the formal requirements are. In addition, the steps to follow are too long. When a MLA request is sent to the US, the Office of International Affairs (OIA) first examines it; then it sends it to the US Attorney of the district where data is held; and finally the Department of Justice also needs to explore the request.[586] It makes the procedure significantly protracted and inefficient.

### *2.1.2. Agreements on passenger name records*

Another agreement influenced by the US counter-terrorism policies is the Passenger Name Records (PNR) Agreement. Although the Commission confirmed that the need for a EU-US PNR Agreement derived from the general EU counter-terrorism strategy, scholars have demonstrated that it has been shaped by the US requirements.[587] In fact, the agreement was a direct consequence of a US law adopted in November 2001,[588] under which any EU airline company with flights taking off or landing within the US territory was obliged to provide the Bureau of Customs Border Protection (CBP) with electronic access to PNR data.[589]

Airline companies have been collecting and exchanging registration data for passenger arrangement purposes for more than sixty years now.[590] However, before

[585]Council of the European Union, 14253/2/12, 24.10.2012, p. 11.
[586] 'Liberty and Security on a changing world. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies', 12.12.2013, pp. 226-228.
[587] Kaunert, Léonard & MacKenzie 2012.
[588] U.S. Aviation and Transportation Security Act, Pub.L. 107–71, 115 STAT. 597, 19.11.2001.
[589] Aviation and Transportation Security Act (ATSA), 19.11.2001 (Public Law 107-71, 107th Congress, 49 USC Section 44909(c) (3) (2001)). For an analysis about the US security measures on aviation before the 9/11, see De Busser 2009, pp. 360-362.
[590] 'Frequently asked questions: The EU-US agreement on the transfer of Passenger Name Record (PNR) data', European Commission, MEMO /13/1054, 27.11.2013.

2001, US law enforcement authorities could only access the necessary data by manual means, on a case-by-case basis and with a prior court order by a European judge.[591] After 9/11, new US laws obliged all airline companies to systematically transfer passenger data of flights arriving in, transiting through, and exiting the country through electronic means before the flight departure.

PNR data has thus become an asset in the fight against terrorism. It includes information on the name of the passenger, the itinerary, supplemental information such as baggage and special requests, and data on the changes made. The CBP collects around sixty-eight million PNR a year.[592] This information is then stored in a common format in the Automated Targeting System (ATS), which is a custom-designed system used by the CBP officers at the Passenger Analysis Unit to detect individuals at high risk of committing terrorist crimes, or other crimes punishable by prison sentences of three-years prison or more.[593] The system has a module called ATS-Passenger (ATS-P), which identifies flight numbers arriving or leaving the US territory. It then processes information on passenger and crew members of the particular flight prior to entry into or departure from US territory. It also deploys an override mechanism, by which it registers those flights that, for unforeseen reasons, need to land on US soil.[594]

The ATS is used in conjunction with other databases such as the Advance Passenger Information System (APIS) for biographical information; the Terrorist Screening Database (TSDB) for certain goods entering the country; the DHS Watchlist Service (WLS); the Electronic System for Travel Authorisation (ESTA); and the US Immigration and Customs Enforcement (ICE). In addition, results of queries from the FBI's Interstate Identification Index and the National Insurance Crime Bureau's database are stored in the ATS.[595] By creating patterns linked to potential criminals (a

[591] Barros X 2012, 'The external dimension of EU counter-terrorism: the challenges of the European Parliament in front of the European Court of Justice', *European Security*, vol. 21 no. 4, p. 524.
[592] SEC(2013) 630 final, 27.11.2013, p. 7.
[593] 'A report on the use and transfer of Passenger Name Records between the European Union and the United States', U.S. Department of Homeland Security, Privacy Office, 3.07.2013, p. 4.
[594] SEC(2013) 630 final, 27.11.2013, p. 5.
[595] 'A report on the use and transfer of Passenger Name Records between the European Union and the United States', *US Department of Homeland Security, Privacy Office*, 03.07.2013, p. 97.

practice known as 'profiling' or 'data mining'),[596] PNR data has helped the CBP identify around 1,750 suspicious cases every year.[597]

If any airline company decided not to comply with the post-9/11 mandate, it could suffer serious consequences, such as the removal of all landing rights within the US territory, the exclusion from the American market, and fines of up to $5,000 for each passenger whose data were not transferred. However, by complying with the US laws, EU airline companies were infringing the EU legal framework, and particularly Directive 95/46/EC on the protection of personal data. Article 25 of the directive establishes that any third country receiving data from member states need a prior adequacy decision from the Commission; and the US border control authorities did not have any.

In an effort to avoid conflicts between the US law and the existing EU data protection legislation, the Commission asked the US authorities for an extension to comply with the new rules[598] and decided to start formal negotiations for the establishment of a PNR agreement with the US. The agreement would solve the problem of infringing Directive 95/46/EC because it would include adequate data protection standards in the sense of Article 25 of the directive.

The Commission, in December 2003, launched a communication on the PNR global approach[599] and, two months later, the Council authorised the start of negotiations with the US.[600] The main institutions that took part in the negotiations were the Commission (DG RELEX) from the side of the EU, and the Department of State on behalf of the US.[601] The EP was only consulted under ex Article 300 TEC. Therefore, neither the EP resolution opposing the EU-US PNR agreement,[602] nor the warning to go to the CJEU

[596] On this concept, see the EP Recommendation on Profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control, P6_TA(2009)0314, 24.04.2009.
[597] 'How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel', *US Department of Homeland Security, Privacy Office*, 05.05.2011, p. 2.
[598] Kaunert, Léonard & MacKenzie 2012, p. 484.
[599] COM(2003) 826 final, 16.12.2003.
[600] de Hert P & de Schutter B 2008, 'International transfers of data in the field of JHA: The lessons of Europol, PNR and Swift' in *Justice, Liberty, Security: New Challenges for EU External Relations, from Justice, Liberty, Security: New Challenges for EU External Relations*, eds. Bernd Martenczuk & Servaas van Thiel, VUBPress, Brussels, p. 327.
[601] Pawlak 2009, p. 563.
[602] European Parliament, P5_TA-PROV(2004)0245, 31.03.2004.

for an opinion of compatibility with the Treaties[603] were taken into consideration by the Commission.

After the adoption of Council Decision 2004/496/EC on the conclusion of an agreement between the European Community and the US on the processing and transfer of PNR data by air carriers to the US DHS, the Bureau of Customs and Border Protection,[604] the (first) EU-US PNR Agreement was formally concluded in Washington D.C. on 28 May 2004. As seen in Chapter 1 of this study, the EU-US PNR Agreement was signed under ex Article 95 TEC. Since the main debate referred to the adequacy of the data protection in the agreement, the US guaranteed an adequate protection of passenger data on 6 July 2004.[605] Similarly, the Official Journal of the European Communities published (on the same day) Commission Decision 2004/535/EC on the adequate protection of personal data contained in PNR transfers.[606]

In 2004 the EU-US Policy Dialogue on Border and Transport Security (PDBTS) was established. It was constituted by homeland security officials from both sides of the Atlantic that would informally discuss issues related to security in the area of transportation. Unsurprisingly, neither the EP nor the national data protection authorities participated in those meetings.[607]

As the EP had announced, it challenged Council Decision 2004/496/EC and Commission Decision 2004/535/EC before the CJEU. The EP argued that, on the one hand, the agreement constituted a breach of the fundamental principles of Directive 95/46/EC and, on the other hand, it was based on the wrong legal basis.

It has been explained in Chapter 1 that in May 2006 the Court based its decision exclusively on the legal basis matter, and it annulled the Commission decision and the Council decision for not being founded on the appropriate provision. The EU rushed the negotiations and the adoption of a second EU-US PNR Agreement, which was provisionally adopted in October 2006.[608] This time the agreement fell under the scope of the former third pillar and it was concluded between the EU (not the EC) and the US,

---

[603] 'European Parliament votes to go to court on EU-US PNR deal', *Statewatch*, 21.04.2004. Available from www.statewatch.org [21 November 2014].
[604] OJ L 183, 20.05.2004, p. 83.
[605] 'Undertakings of the Department of Homeland Security, Customs and Border Protection', Federal Register, vol. 69 no.131, 06.07.2004.
[606] OJ L 235, 06.07.2004, p. 11.
[607] Pawlak 2009, p. 567.
[608] OJ L 298, 27.10.2006, pp. 29-31.

culminating with Council Decision 2006/729/CFSP/JHA.[609] As noted above, international agreements on data transfers signed under the basis of the first pillar had to comply with the 'adequacy principle' of Article 25 of Directive 95/46/EC. Yet, it was not the case when the agreements fell under the third pillar, where member states could apply their own standards. Thus, while that new agreement solved airline companies' concerns of infringing the EU data protection legislation, new concerns arose within the EU, this time because the new agreement no longer required 'adequate' data protection safeguards for international transfers.

According to ex Article 24(1) TEU, the negotiations of the second PNR agreement were conducted by the Council, which authorised the participation of the Presidency and the Commission.[610] As for the role of the EP, it enjoyed only an 'observer' status, despite maintaining bilateral contact with the US authorities.[611]

The second PNR Agreement expired on 31 July 2007 and it was immediately replaced by a third agreement.[612] The third EU-US PNR Agreement was signed and provisionally applied through Council Decision 2007/551/CFSP/JHA.[613] That agreement was considered an effective tool by the US authorities. Americans stated that, thank to the agreement, they identified during 2008 and 2009 more than 3,000 individuals with potential ties to terrorism. For example, the Mumbai attacks' plotter David Headley, who was arrested in 2008 at Chicago's airport, was identified through his PNR data. Faisal Shahzad, the perpetrator of the failed NYC Time Square bombing in May 2010, and Najibullah Zazi, who pleaded guilty to plotting to bomb New York City subways,[614] were also arrested after the US police had access to their PNR.

However, the 2007 EU-US PNR Agreement was never formally concluded because the EP never gave consent to the proposal.[615] The reason for this was mainly that many

---

[609] Council Decision on the signing, on behalf of the European Union, of an 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, 13226/06, 06.10.2006.
[610] EU/US Passenger Name Record (PNR) Agreement, House of Lords, European Union Committee, 21st Report of Session 2006–07 p. 27.
[611] Pawlak 2009, p. 571.
[612] OJ L 204, 04.08.2007, pp. 18-25.
[613] OJ L 204, 04.08.2007, p. 16-17.
[614] Rep. Patrick Meehan Speech in Subcommittee Hearing: Intelligence Sharing and Terrorist Travel: How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel, 05.10.2011. Available from http://homeland.house.gov [21 November 2014].
[615] European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, P7_TA(2010)0144; COM(2009)702 final, 17.12.2009.

MEPs were not convinced by the agreement but they did not want to reject it because they thought it could create legal uncertainties for travellers and airline companies.[616] Therefore, they decided to postpone the vote.[617] As in the previous agreement, the role of the EP, the national DPAs and the EDPS was very limited. However, the establishment of the High Level Contact Group on data protection offered a new oversight on data transfers.[618]

In 2009 the Treaty of Lisbon abolished the previous division of EU policies in pillars. Although the 2007 EU-US PNR Agreement was expected to remain operational until 2014, the EP's postponement of the vote, combined with the fact that not all member states had ratified the agreement,[619] made the drafting of a new PNR agreement between the EU and the US a matter of urgency. Therefore, in September 2010 the Commission issued a new 'global external PNR strategy',[620] which was welcomed by the EP.[621]

Negotiations for the fourth PNR agreement with the US authorities were officially launched in December 2010.[622] Despite the opposition from the US government to modify the 2007 EU-US PNR Agreement,[623] these negotiations between the Commission and the US were successfully concluded in May 2011.[624] The new proposal for the EU-US PNR Agreement was officially released in November 2011.[625] It was signed on 14 December 2011 under the substantive legal basis of Articles 82(1)(d) and 87(2)(a) TFEU. The procedure for the adoption of the agreement followed the wording of Article 218 TFEU. Particularly, paragraph 6 of Article 218 TFEU gives new competences to the EP, which is now required to give its consent before concluding specific international agreements.

Compared to the previous agreement, the current EU-US PNR Agreement includes new safeguards for passengers. For instance, data is only retained for six months, before it passes to another database where it is depersonalised and 'marked'. In addition, there

---

[616] Archick 2013, p. 12.
[617] European Parliament, P7_TA(2010)0144, 05.05.2010.
[618] This group is examined in section 3.3.2 of this chapter.
[619] 'A report on the use and transfer of Passenger Name Records between the European Union and the United States', *U.S. Department of Homeland Security, Privacy Office*, 03.07.2013, p. 9.
[620] COM/2010/0492, 21.9.2010.
[621] Resolution P7_TA-PROV(2010)0397, European Parliament, 11.11.2010.
[622] Archick 2013, p. 13.
[623] House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, 'How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel', 112th Congress, 05.10.2011.
[624] Archick 2013, p. 13.
[625] COM/2011/0807, 23.11.2011.

are more restrictions regarding the personnel authorised to access data, and there is more legal certainty regarding the judicial redress.[626] Finally, airline companies are now obliged to provide passenger details up to ninety-six hours before the flight departure, in comparison with the seventy-two hours required under the 2007 EU-US PNR Agreement.[627]

The agreement was very well received among member states.[628] Even the EP, which voiced initial concerns,[629] found that having that agreement was better than having no agreement at all, thus the majority of MEPs voted in favour (409 in favour and 226 against).[630] After being approved by the EP[631] and the Council,[632] the agreement entered into force on 1 July 2012 and it will be up for automatic renewal by 2019 at the latest.[633]

### *2.1.3. SWIFT agreements*

Another EU-US agreement that has been largely influenced by US requirements is the SWIFT Agreement. Although the EU has always tried to justify the adoption of such an agreement as beneficial for the fight against terrorism in Europe and 'necessary to ensure protection of EU citizens' privacy,[634] the present section proves that the EU followed the US mandate as regards the content of both the first and the second SWIFT agreements.

On 11 September 2001 the US and the EU started to exchange financial data. In December 2001, two US–Europol agreements were concluded in order to facilitate the exchange of information related to global financial movements.[635] They were part of the Terrorist Finance Tracking Program (TFTP), created by the Bush administration after

---

[626] Further analysis on data protection safeguards in PNR agreements is found in section 3.2.1 of this chapter.
[627] Travis, A 2011, 'US to store passenger data for 15 years', *The Guardian*, 25 May. Available from <www.theguardian.com> [21 November 2014].
[628] All member states except Austria and Germany approved the agreement in December 2011. Archick 2013, p. 15.
[629] Pop V 2011, 'Unhappy MEPs to approve passenger data deal', *EU Observer*, 11 November. Available from <http://euobserver.com/justice/114252> [21 November 2014].
[630] Archick 2013, p. 15.
[631] European Parliament, P7_TA-PROV(2012)0134, 19.04.2012.
[632] Council of the European Union, 9186/12, PRESSE 173, 26.04.2012.
[633] Archick 2013, p. 9; MEMO /13/1054, 27.11.2013, p. 3.
[634] European Commission, MEMO/13/1060, 27.11.2013.
[635] Agreement Between the United States of America and the European Police Office, 6.12.2001; Supplemental Agreement Between the Europol Police Office and the United States of America on the Exchange of Personal Data and Related Information, 20.12.2002.

9/11 as one of the counter-terrorism measures resulting from Executive Order 13224[636] and the UN Resolution 1373 (2001).[637]

Under the TFTP the US authorities were able to pull EU citizens' data from the private company the Society for the Worldwide Interbank Financial Telecommunication (SWIFT). The programme was secret and it did not involve the EU at all, since the company was based in Belgium but had servers located in the US territory, particularly in Virginia. The US could only get the financial data from SWIFT in the form of standardised messages by sending administrative subpoenas to the institution. The programme was very attractive for the US law enforcement sector, since the company collects personal data from 10,000 financial institutions in more than 200 countries.[638] Although SWIFT executives always insisted that the transfers were not voluntary,[639] SWIFT never contested the subpoenas.[640] The US gathered information from up to 12.7 million financial transactions a day,[641] and once the information was pulled, messages were stored for a period of 124 days.[642]

The TFTP was uncovered in 2006 by the New York Times[643] and from that moment many concerns were raised within the EU about its potential violation of EU data protection laws. Even though the company always processed EU citizens' data through its servers located in the US, due to the fact that SWIFT headquarters were in Belgium the company had to comply with Belgian national law implementing Directive 95/46/EC.

In November 2006, the Art. 29 WP issued an opinion stating that the programme breached EU data protection laws.[644] SWIFT joined the Safe Harbour principles in 2007

---

[636] Blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism. Title 31 Part 595 US Code of Federal Regulations, 23.09.2001.
[637] United Nations, S/RES/1373(2001), 28.09.2001.
[638] MacKenzie 2012, p. 107; 'European Data Protection Authorities investigate bank data security. The Dutch and Belgian DPAs join hands for a security investigation of SWIFT', *Commission for the Protection of Privacy*, 13.11.2013. Available from <https://www.ip-rs.si> [21 November 2014].
[639] Pell SK 2012, 'Systematic government access to private-sector data in the United States', *International Data Privacy Law*, vol. 2, no. 4, p. 253.
[640] de Goede M 2012, 'The SWIFT Affair and the Global Politics of European Security', *Journal of Common Market Studies*, vol. 50, no. 2, p. 221.
[641] Pell 2012, p. 253.
[642] de Hert & de Schutter 2008, p. 331.
[643] Lichtblau E & Risen J 2006, 'Bank data is sifted by U.S. in secret to block terror", *The New York Times*, June 23. Available from www.nytimes.com [21 November 2014].
[644] WP128, 22.11.2006. For a criticism of the opinion, see Moerel L 2014, 'SWIFT revisited- When do the Directive and the proposed Regulation apply' in *Data Protection anno 2014: How to restore trust. Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014),* eds. Hijmans H & Kranenborg H, Mortsel, pp.159-174.

and, that same year, the company decided to move its servers completely to Europe,[645] relocating its servers in Virginia (US) to Switzerland.[646] This made the need for an agreement enabling SWIFT transfers in compliance with EU laws particularly urgent. The EP released two resolutions in 2006 and 2007[647] calling for the adoption of an agreement, which would regulate SWIFT data transfers to the US. These claims convinced the German Presidency of the Council about the necessity for an agreement with the US Department of the Treasury that avoided potential clashes with EU data protection laws.[648]

On 30 November 2009, under the legal basis of the former Articles 24 and 38 TEU, the EU and the US signed the first official SWIFT Agreement, exactly one day before the Treaty of Lisbon came into force. The agreement became operational on 1 February 2010 and it was supposed to be applied temporarily until 31 December of that year. However, the legal basis to conclude international agreements changed with the Treaty of Lisbon and so did the powers of the EP: since the Treaty of Lisbon the Council can only adopt a decision authorising the conclusion of an agreement after obtaining the consent of the EP.[649] Under these new competences, the LIBE Committee wrote a report on 5 February 2010 recommending the rejection of the interim SWIFT agreement.[650]

The main concerns expressed by the EP related to privacy. In particular, it stated that a) there was a lack of necessity and proportionality of the agreement, b) it did not respect the purpose limitation principle, c) it did not foresee any judicial remedy for EU citizens, d) data were transferred by a pull system, causing the storage of 'bulk data',[651] and e) it was necessary to establish a EU TFTP to process the data within the EU.

Despite intense lobbying from the Commission, member states and the US authorities, on 11 February 2010 the EP rejected the adoption of the SWIFT

---

[645] Cremona 2011, p. 13, Curtin 2011, p. 6; Suda Y 2013, 'Transatlantic politics of data transfer: Extraterritoriality, counter-extraterritoriality and counter-terrorism', *Journal of Common Market Studies*, vol. 51 no. 4, p. 782.
[646] MacKenzie 2012, p. 107
[647] OJ C 287 E, 29.11.2007, pp. 349; OJ C 303 E, 13.12.2006, p. 843.
[648] OJ C 166, 20.07.2007, pp. 18-25.
[649] Article 218(6) TFEU.
[650] European Parliament, 'Recommendation on the proposal for a Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program', PE 438.440v02-00, 05.02.2010.
[651] It is defined as 'the authorised collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g. specific identifiers, selection terms, etc.)'. See 'Signals Intelligence Activities', *The White House Office of the Press Secretary*, 17.01.2014, p. 3.

Agreement.[652] The rejection was interpreted as a protest by the EP against the Commission and the Council because it was not consulted during the negotiations.[653] Also, the EP rejection reflected the significant power that the institution gained with the Treaty of Lisbon. The EP plays now an important role in the negotiation of international agreements.

The adoption of a second SWIFT agreement was imperative. In the months that followed there was no agreement in place so data transfers to the US were conducted through the existing EU-US MLA Agreement, as well as through the MLATs between member states and the US.[654] Yet, as seen earlier, this procedure is usually quite slow and inefficient.

The Council restarted negotiations with the US authorities for the new agreement during the spring of 2010.[655] Unsurprisingly, the EP played a predominant role during the negotiations. Yet, not all the changes proposed by this institution were finally fulfilled.[656] In any case, the EP voted in favour of that second agreement by 484 votes to 109,[657] and it was signed on 28 June 2010.

The second SWIFT agreement was based on Articles 87(2)(a) and 88(2) TFEU on police cooperation. It certainly introduced many of the EP suggestions such as i) the possibility of administrative and legal redress for EU citizens in the US (Article 18),[658] ii) the competence for Europol to approve the requests sent by the US Treasury Department (Article 4), iii) the introduction of an independent observer appointed by the Commission based in Washington D.C. (Article 12), iv) provisions on retention and deletion of data (Article 6), and v) plans for and equivalent TFTP in the EU (Article 11).

The EP's demands that were not included in the agreement referred particularly to the removal of bulk data and the pull system, as well as the establishment of a judicial oversight. Since these issues are important safeguards to be considered in any adequate data protection framework, some scholars believe that this second permanent agreement

---

[652] European Parliament, P7_TA(2010)0029, 10.02.2010.
[653] Cremona 2011, p. 16; Ripoll Servent A & MacKenzie A 2011, 'Is the EP still a data protection champion? The case of SWIFT', *Perspectives on European Politics and Society*, vol. 12, no. 4, p. 400.
[654] Cremona 2011, p. 18.
[655] Council of the European Union, 11575/10, 28.06.2010.
[656] Ripoll Servent & MacKenzie 2011, p. 401.
[657] European Parliament, A7-0224/2010, 05.07.2010.
[658] However, Ripoll Servent and MacKenzie argue that there is no judicial redress in the US in practice, see Ripoll Servent & MacKenzie 2012, 'The European Parliament as a 'Norm Taker'? EU-US Relations after the SWIFT Agreement', *European Foreign Affairs Review*, vol. 17, Special Issue, p. 81.

is not very different from the first interim agreement.[659] Other aspects subject to criticism in the new SWIFT agreement relate to the lack of necessity, the length of the retention period (five years),[660] and the vagueness of the US requests in order to collect SWIFT data.[661]

As will be analysed in Chapter 3, the new SWIFT agreement involves Europol in the transfer of financial data to the US. In this regard, the EP[662] raised concerns because Europol, which is in charge of verifying the US compliance of the agreement, did not initially provide any updated written information about the requests from the US Treasury Department and the compliance with the European data protection standards. A dispute on document secrecy between the Council and the EP ended up with a CJEU decision in favour of the EP in July 2014.[663] The Council argued that the disclosure of the US requests to the EP would have a '[negative] impact on the European Union's negotiating position'. However, the argument did not convince the Court because no evidence had been provided showing that the secrecy was necessary to prevent a 'risk of a threat to the public interest'. Thus, that CJEU decision reinforces EU transparency rules in the context of international agreements.[664]

### *2.1.4. EU-US agreements on air and maritime security partnership*

This study has already analysed one agreement between the EU and the US on air security: the EU-US PNR agreement. This is the most controversial legal instrument for transferring data collected regarding transatlantic flights, but it has not been the only air security measure. Other agreements have also been adopted since 9/11 in order to exchange information between the EU and the US related to air transport. Similarly, in the area of maritime transport, new security measures such as the Container Security Initiative (CSI) have been adopted. Transport security issues have become one of the main topics on both sides of the Atlantic. Also, regular dialogues, between the EU and the US on security has taken place since 2004.[665] Following the same contention as in

[659] Ripoll Servent & MacKenzie 2011, pp. 391 and 396.
[660] OJ C 355, 29.12.2010, p. 10.
[661] Archick 2013, p. 11.
[662] 'SWIFT implementation report: MEPs raise serious data protection concerns', Press Release Committee on Civil Liberties, Justice and Home Affairs, 01.03.2011.
[663] Council of the European Union v. Sophie in 't Veld, C-350/12 P, 3.7.2014.
[664] Fox B 2012, 'Commission pushes for document secrecy despite court judgement', *EUObserver*, 8 May. Available from http://euobserver.com [6 November 2014].
[665] See EU-US Policy Dialogue on Border and Transport Security (PDBTS).

the previous sections, I will demonstrate that the US transport security measures enacted after 9/11 have had a great influence on the EU rules relating to transport security matters.

I will look first at the EU security measures adopted within the scope of aviation – besides the already studied EU-US PNR agreement. In September and October 2001, EU Transport Ministers at the European Council organised several meetings for the adoption of new EU counter-terrorism measures.[666] A few days later, The Commission launched a proposal for a regulation on establishing common rules in the field of civil aviation security.[667] It was approved on 16 December 2002[668] and it consisted of preventative measures that ensured air transport security within the EU. Interestingly enough, the first recital justified the adoption of this regulation as though the EU had actually been threatened:

'The criminal acts committed in New York and Washington on 11 September 2001 show that terrorism is one of the greatest threats to the ideals of democracy and freedom and the values of peace, which are the very essence of the European Union.'

The regulation included minimum measures to be implemented by member states, such as surveillance activities, control access, pre-departure checks, security screening for passengers, or handling of checked-in baggage. These were specified in the annex of Commission Regulation (EC) 226/2003 and classified as secret.[669] The regulation on air security was amended in 2008.[670] The new text simplified and harmonised the measures that the member states had adopted, and it increased the levels of security in the field of civil aviation.

Simultaneously, the US introduced new security measures for passengers arriving by aircraft on the US territory. One of these measures consisted in tightening air transport entry requirements for passengers coming from countries included in the US Visa Waiver Program (VWP). The VWP allows citizens of certain countries to travel to the US territory without a prior visa as long as they do not stay for more than 90 days. After 9/11, the US ordered all countries benefiting from the VWP to start issuing computer-

[666] COM(2001) 575 final, 10.10.2001, p. 2.
[667] COM(2001) 575 final, 10.10.2001, p. 8.
[668] OJ L 355, 30.12.2002, pp. 1-21.
[669] OJ L 89, 05.04.2003, pp.9-10 and OJ L 221, 09.04.2008, pp. 8-22.
[670] OJ L 97, 09.04.2008, pp. 72-84.

coded passports, so that terrorists could not use fake passports to enter the US.[671] Accordingly, the Commission issued a decision in 2005 on the specifications for storing passport holder's facial images and two fingerprints in the chip of the passport.[672] This type of biometric data had to be present in passports of all VWP designated countries after 28 August 2006.[673]

Within the EU, twenty-two of the twenty-eight member states are VWP designated countries[674] (in contrast, the US has visa exemption in all member states).[675] Therefore, the EU and the US decided to start sharing information collected from the passports of passengers booking transatlantic fights, including biometric data. That information was not only useful for identifying passengers travelling across the Atlantic, but also for sharing information about any lost and stolen passports.[676]

Further requirements were introduced in 2007 for countries benefiting from the VWP: the US authorities established the web-based ESTA, by which since January 2009 all citizens from VWP designated countries flying to the US had to submit biographical information and answer a few questions,[677] at least two days before the fight. An ESTA application costs fourteen dollars but applying for it does not guarantee its approval.[678] If the citizen receives the authorisation, ESTA approval is valid for two years and covers multiple entries. However, approved citizens will still need to submit

---

[671] Shenon P 2003, 'Two years later: The borders; new passport rules to fight terrorism are put off for a wear', *New York Times*, 9 September. Available from www.nytimes.com [22 November 2014].
[672] OJ L 385, 29.12.2004, pp. 1-6.
[673] Faull & Soreca 2008, p. 400.
[674] The complete list is available in http://travel.state.gov/content/visas/english/visit/visa-waiver-program.html [22 November 2014].
[675] Annex II of OJ L 81, 21.03.2001 and OJ L 141, 04.06.2005, pp. 3-5.
[676] OJ L 27, 29.01.2005, p. 61.
[677] The questions are: 1) Do you have a communicable disease; physical or mental disorder, or are you a drug abuser or addict? 2) Have you ever been arrested or convicted for an offense or crime involving moral turpitude or a violation related to a controlled substance; or have been arrested or convicted for two or more offenses for which the aggregate sentence to confinement was five years or more; or have been a controlled substance trafficker; or are you seeking entry to engage in criminal or immoral activities? 3) Have you ever been or are you now involved in espionage or sabotage; or in terrorist activities; or genocide; or between 1933 and 1945 were you involved, in any way, in persecutions associated with Nazi Germany or its allies? 4) Are you seeking to work in the U.S.; or have you ever been excluded and deported; or been previously removed from the United States or procured or attempted to procure a visa or entry into the U.S. by fraud or misrepresentation? 5) Have you ever detained, retained or withheld custody of a child from a U.S. citizen granted custody of the child? 6) Have you ever been denied a U.S. visa or entry into the U.S. or had a U.S. visa cancelled? 7) Have you ever asserted immunity from prosecution?
[678] There is some confusion between the ESTA programme and the Advance Passenger Information (API) system. The former requires selected travellers to obtain formal authorisation from competent state authorities; the latter places an obligation on carriers to collect specific information from travellers. See Bigo B, Carrera C, Hayes H, Hernanz N & Jeandesboz J 2012, 'Justice and Home Affairs databases and a smart borders system at EU External borders. An evaluation of current and forthcoming proposals', *CEPS Paper in Liberty and Security in Europe*, no. 52, Brussels, p. 27.

biometric identifiers (including fingerprints and photographs) upon arrival every time they fly to the US. Citizens whose ESTA application is denied will need a US visa to enter the country.

Not only have EU passengers flying to the US been closely monitored over the last decade, but also cargo security of air transport was strengthened after the attacks. Today, the totality of cargo on passenger planes is screened in the EU following the Implementing Recommendations of the 9/11 Commission Act of 2007.[679] On 29 October 2010 the effectiveness of this counter-terrorism measure was proven, when an improvised explosive device was found within the cargo of two aircrafts arriving from Yemen.[680] That incident triggered the release of a European Action Plan in December 2010 for the harmonisation of security controls within the EU for cargo coming from non-EU countries.[681] Recently, the EU has adopted new legislation to enhance the security of cargo on aircrafts entering the EU[682] and, at the same time, it has concluded an EU-US agreement on air cargo security partnership, through which both parties establish mutual recognition of air cargo security frameworks.[683]

*Figure 2.1.*


Transportation Security Administration

NOTICE OF BAGGAGE INSPECTION

To protect you and your fellow passengers, the Transportation Security Administration (TSA) is required by law* to inspect all checked baggage. As part of this process, some bags are opened and physically inspected. Your bag was among those selected for physical inspection.

During the inspection, your bag and its contents may have been searched for prohibited items. At the completion of the inspection, the contents were returned to your bag.

If the TSA security officer was unable to open your bag for inspection because it was locked, the officer may have been forced to break the locks on your bag. TSA sincerely regrets having to do this, however TSA is not liable for damage to your locks resulting from this necessary security precaution.

For packing tips and suggestions on how to secure your baggage during your next trip, please visit:

www.tsa.gov

We appreciate your understanding and cooperation. If you have questions, comments, or concerns, please feel free to contact the TSA Contact Center:

Toll-free telephone: 1.866.289.9673
Direct telephone: 571.227.2900 (U.S.)
E-mail: TSA-ContactCenter@dhs.gov

* Section 110(b) of the Aviation and Transportation Security Act of 2001, 49 U.S.C. 44901(c)-(e)

TSA-repo form 1000 (Rev. 1-13-2010)

Smart Security Saves Time

*This leaflet might be found in your checked suitcase if your baggage has been inspected by the TSA.*

[679] Archick 2013, p. 18.
[680] Council of the European Union, 8161/11, 24.03.2011, p. 2.
[681] 'A European action plan to strengthen air cargo security', *European Commission Press Release*, IP/10/1651, 02.12.2010.
[682] Council of the European Union, 18928/11, 21.12.2011, p. 6.
[683] 'EU-US security agreement allows cheaper and faster air cargo operations', *European Commission Press Release*, 01.06.2012.

Besides the information exchanged between the EU and the US regarding passengers and cargo entering the US by air, maritime cargo screening between the EU and the US has likewise been reinforced. Within the EU territory alone there are more than 1,200 seaports and about 4,000 port facilities.[684] At the time the 9/11 attacks occurred, only 2% of the 12,000 million containers shipped every year to the US territory were being inspected.[685]

For the US-bound containers coming from the EU, the US launched the so-called Container Security Initiative (CSI) in mid-2002. It initially applied to eight ports in Europe.[686] The US then sought to increase the number of ports participating with the CSI and it started bilateral negotiations on container security with several member states (particularly, Belgium, France, Germany, the Netherlands, the United Kingdom, Italy, Spain and Sweden). The US main objective was to reinforce the security of maritime transport by installing US custom officers at European ports where they could examine high-risk containers before they reach the US.[687] These officers submitted containers to X-ray and radiation scanners and sent a report with the results twenty-four hours before the arrival of the container to the US territory.[688]

However, shortly after the system was operational, it was found that it infringed the EU laws, particularly the EU-US customs cooperation and mutual assistance accord of 1997.[689] According to these agreements, the former European Communities were the only competent authority in customs matters,[690] so member states could not adopt any independent agreement with the US on these issues.

The US threatened the EU with restricting its market access if the required security measures were not in place,[691] so the EU decided to adopt an agreement on EU-US maritime transport security.[692] In parallel, the EU passed legislation on enhancing ship and port facility security in 2004 and 2005.[693]

The EU-US agreement for intensifying and broadening customs and container

---

[684] COM(2006) 431 final, 01.08.2006, p. 3.
[685] MacKenzie 2012, p. 104.
[686] Antwerp, Bremerhaven, Felixstowe, Genoa, Hamburg, La Spezia, Le Havre, Rotterdam.
[687] 'EU Member States by-pass Commission to give US access to containers at ports', *Statewatch News Online,* 27.05.2003. Available at www.statewatch.org [22 November 2014].
[688] MacKenzie 2012, p. 105.
[689] OJ L 222, 12.08.1997, pp. 17-24.
[690] Faull & Soreca 2008, p. 409.
[691] Ripoll Servent & MacKenzie 2012, p. 77.
[692] COM(2003)229 final, 02.05.2003, p. 20.
[693] OJ L 129, 29.04.2004, pp. 6-88; OJ L 310, 25.11.2005, pp. 28-39.

security cooperation was in force in 2004.[694] That agreement gave the US a solid legal basis to extend the number of stations in EU ports where the US was able to pre-screen maritime cargo containers. However, the establishment of US officers in EU ports needed the express consent of the member states.[695] Today, ten member states participate in the CSI,[696] and the initiative covers more than the 86% of all maritime containerised cargo destined for the US.[697]

Therefore, the influence of the US over EU maritime security measures is unquestionable. In particular, the EU adopted a directive enhancing port security in 2005,[698] and a Commission regulation laying down revised procedures for conducting inspections in the field of maritime security entered into force in 2008.[699] In addition, a communication[700] with a road map[701] was launched by the Commission in 2009 seeking to integrate maritime surveillance and exchange of information among member states, and also with third countries.[702] Regarding the EU-US cooperation in this field, since May 2012, both countries have established mutual recognition of their shipper programmes by designating specific companies as 'trusted traders'.[703] Moreover, they cooperate closely in the sharing of intelligence about particular threats through the Container Security Advanced Information Networking (CONTAIN).

## 2.2. Issues of concern in the agreements

### *2.2.1. Legal basis implications*

Before Lisbon, the EU divided its policies in three pillars: the first on Community policies, the second on Common Foreign and Security Policy (CFSP), and the third on Police and Judicial Cooperation in Criminal Matters. This structural division had significant legal implications since the role of the EU (formerly, the European

[694] OJ L 304, 30.09.2004, pp. 34-37.
[695] Suda 2013, p. 777.
[696] Updated list available from http://www.dhs.gov/container-security-initiative-ports [22 November 2014].
[697] MacKenzie 2012, p. 105.
[698] OJ L 310, 25.11.2005, pp. 28-39.
[699] OJ L 98, 10.04.2008, pp. 5-10.
[700] COM(2009) 538 final, 15.10.2009.
[701] COM(2010) 584 final, 20.10.2010.
[702] COM(2009) 538 final, 15.10.2009, pp. 6-7.
[703] US Customs-Trade partnership Against Terrorism (C-TPAT) program and the EU's Authorised Economic Operators (AEO) regime.

Communities) was greater for policies under the scope of the first pillar than in the other two intergovernmental pillars. The legislative procedure under the first pillar required qualified-majority voting (QMV) in the Council and simple majority in the EP. In contrast, for second and third-pillar decisions there was no participation of the EP and any country could block a proposal in the Council because it required unanimity of its members.

Questions about the adequacy of the legal basis were raised regarding those measures that intertwined different policy areas. The process was known as cross-pillarisation and the choice of legal basis ultimately depended on the preferences of member states and EU actors. For example, there were cases in which member states preferred to conclude an international agreement under the former third pillar to get more control in the decision-making and implementation process. For instance, as mentioned above, an international agreement in the third pillar was only adopted if all member states voted in favour: once approved, the Commission lacked the competence to force any member state to comply with it.

Thus, the choice of the legal basis of any legislative act depends on the main objective that such law seeks to achieve. It is quite common that an EU instrument pursues more than one goal. For example, a law can protect the environment and criminalise a particular behaviour at the same time. If that law establishes that the protection of the environment is the main objective, then the proper legal basis falls under the former first pillar (ex Article 174 TEC). Yet, if the law mainly focuses on sanctioning individuals and companies that conduct non-environmentally friendly activities, then a third-pillar legal basis should apply.

As regards the first/third pillar dichotomy, a debate arose because former European Communities adopted several EC acts that involved internal security matters.[704] That was the case of first EU-US PNR Agreement. Airline companies initially collected PNR data for commercial reasons, and only later law enforcement authorities started to request them for security purposes. The fact that the processing of data was based on two purposes allowed a margin of discretion as for the most 'adequate' legal basis for the measure. The first EU-US PNR agreement in 2004 used ex Article 95 TEC as legal basis (first pillar), while subsequent EU-US PNR agreements of 2006, 2007 and 2012

[704] Randazzo V 2009, 'EU security policies and the pillar structure: A legal analysis', *Perspectives on European Politics and Society*, vol. 10, no. 4, p. 507.

were based on third-pillar provisions.[705]

The choice of different PNR legal bases had enormous implications. The first PNR agreement was adopted under the scope of the first pillar and, therefore, it involved both the Council and the EP in the decision-making process. According to ex Article 300(7) TEC, it also bound all member states without any room for exceptions. One of the reasons why member states and EU institutions decided to resort to a first-pillar instrument was because they wanted to gain more control in the way they executed sensitive security-related problems.[706] Also, by choosing a first-pillar legal basis for the first EU-US PNR Agreement, they ensured that it would comply with Directive 95/46/EC. In contrast, the 2006 and 2007 PNR agreements were subject to other decision-making rules. They were intergovernmental instruments so they needed unanimous consent in the Council, with no approval by the EP. As for the data protection safeguards, Directive 95/46/EC was no longer applicable. Member states (and not the European Communities) were the main competent authorities to control the data protection 'adequacy' of the transfers.

The Treaty of Lisbon kept the legal basis in the 'third pillar' for the 2012 EU-US PNR Agreement, but here the EP participated in the negotiations. Regarding the data protection standards, the agreement includes provisions regulating the protection of personal information, but it falls outside the scope of the general EU data protection legal framework. These provisions are carefully examined in section 3.2.1 of this chapter.

Besides the confusing first/third pillar division, another recent legal debate has referred to the ambiguous separation between second- and third-pillar measures. It was not always clear when a measure fell under the scope of CFSP, and when it was an AFSJ instrument. The reason for this confusion is that there is no specific provision in the EU treaties indicating the objectives of AFSJ external actions: Article 67 TFEU enumerates the general purposes of the AFSJ, but nothing is said about its external dimension. Likewise, Article 21 TEU lists the EU overall security objectives to be fulfilled through the EU external policies but it does not concretise which policy conducts what. In that regard, the AG Bot stated in the case C-658/11:

[705] In particular, articles 24 and 38 TEU before Lisbon, and articles 81(1)(d) and 87(2)(a) TFEU.
[706] Randazzo 2009, p. 509.

'The distinction between these two Union policies [the CFSP and the AFSJ] is made difficult because they are both connected to the imperative of security. The objectives of safeguarding the security of the Union and strengthening international security are assigned to the Union as objectives of the Union's external action under Article 21(2)(a) and (c) TEU. At the same time, ensuring a high level of security is also an objective of the AFSJ in accordance with Article 67(3) TFEU.'[707]

Precisely because of this lack of specific rules, the EU has made use of its implied powers to adopt international agreements within the scope of the external dimension of the AFSJ.

The Council has had some political discretion for deciding whether a measure falls under the scope of the CFSP or under the AFSJ (former second/third-pillar division).[708] This appreciation is ultimately subject to interpretation by the CJEU in the terms of Article 40 TEU. Interestingly, the Council has usually chosen to adopt data-sharing security measures under the scope of the external dimension of the AFSJ instead of using a CFSP provision. For instance, agreements on security procedures for the exchange of classified information, the 2006 and 2007 EU-US PNR agreements and the first temporary SWIFT agreement were all adopted under the basis of ex Articles 24 and 38 TEU. However, as seen above, intelligence gathered by organisations like the European Union Military Staff (EUMS) and IntCen would fall under the scope of the former second pillar.

My theory, after a careful examination of this CFSP/AFSJ division, is as follows: The choice of pillar on security issues depends on two factors: a) the specific purpose of the law and b) the actors involved.

Following the argument of AG Bot in the Mauritius case, if the the main purpose of the measure is the internal security of the EU then it should be adopted on an AFSJ legal basis; whereas if the main purpose is preserving the international security, then the CFSP should be used (eg the Mauritius case). However, the difficulty here is in deciding when the security objective is really internal or international.

As regards the subjects involved, two main categories of actors can process information for security purposes: law enforcement authorities and intelligence services. If data is gathered by the diplomatic or intelligence services, then the legal basis for

[707] Opinion of the Advocate General Bot on the case C-658/11, 30.01.2014, para. 107.
[708] Randazzo 2009, p. 516.

data-sharing agreements falls under the scope of the second pillar. In contrast, agreements on data processed by law enforcement authorities fall under the third-pillar framework.

As in the first/third-pillar discussion, the choice of legal basis under the second or the third pillars has legal implications. Agreements adopted under a third-pillar legal basis need the approval from both the EP and the Council, and they can be challenged before the CJEU. Contrary to this, second-pillar measures require unanimous consent by the Council, no participation of the EP and no control by the CJEU. Member states are here the only competent authorities to control the 'adequacy' of data processing; at least until the scope of Article 39 TEU is finally determined.

### *2.2.2. Public-private partnership*

During the investigation of a crime, law enforcement authorities often require information that has been originally collected by private companies. The privatisation of security gained importance during the nineties,[709] and it increased significantly after the 9/11 attacks. The public-private partnerships (PPPs) are present in all member states and they work both ways: law enforcement agencies are able to access information collected by private parties, and these companies can also access some police databases (see, for instance, the TIDE database).[710]

This section focuses only on the access that the law enforcement sector has to data collected by private companies. The phenomenon is seen with regard to passenger data collected by airline companies through PNR systems, financial records collected by banks and other similar institutions like SWIFT and, above all, data stored by telecommunication service providers (TSP).

A great number of TSPs are located in the US and, therefore, they are bound by US laws. This is the case of Google Inc., Yahoo Inc., Twitter, Facebook, LinkedIn, Dropbox and Whatsapp, to name a few. Despite having their headquarters in the US, these companies process personal data from users around the world. Such valuable

[709] Ortiz C 2013, 'Security partnerships, intelligence and the recasting of the UK monopoly of violence in the 21st Century' in *Counter-terrorism and Intelligence in Europe,* eds. Kaunert C & Leonard S, Palgrave Macmiltan, Hampshire, p. 216.
[710] The Terrorist Identities Datamart Environment (TIDE) is a US classified database where names of suspects of terrorists are registered. Ortiz 2013, p. 221.

information has not only caught the attention of publicity and marketing companies, but also of police and judicial authorities within and beyond the US borders.

Companies like Google, Twitter, Facebook, LinkedIn, Dropbox and Apple publish transparency reports every six months (or yearly, in the case of Dropbox) with the aim of keeping users informed about governments' requests for access or suppression of their data.[711] The number of requests varies from country to country. In the EU, Germany, France and the UK are leading the lists of data requests, as shown in a recent comparative study conducted by the NGO Silk.[712]

It has been seen above that MLA procedures are normally used by law enforcement authorities in the EU to request information located in the US, and vice versa. For instance, if Spanish authorities as Facebook to disclose an inbox message of a Spanish user, they will need to follow the procedure established in the MLA concluded between the US and Spain. The procedure consists of a request to the Office of International Affairs of the United States Department of Justice, which will then be reviewed by the Counter-terrorism Department and, finally, submitted to a federal court, which will issue the court order that authorises the data transfer.[713]

In principle, the provider (e.g. Facebook) will not send the records directly to the requesting country, but this is not always the case. Besides the formal MLA procedure, US companies can decide to provide law enforcement authorities with information through an alternative informal process. In fact, employees of big tech companies do not always understand the functioning of the MLA procedure when they receive a government request.[714] Therefore, they often choose the informal approach over the formal MLA, because they simply find it is easier.

Informal contact can be established directly with the TSP or by sending an application to the Federal Bureau of Investigation. For instance, as mentioned in Chapter 1, Twitter replies to requests made by governmental authorities of member states only if these are emergency requests. In contrast, for the rest of cases, requests should be issued via US courts by a letter rogatory, or through MLATs.[715] Likewise,

---

[711] Transparency reports available from www.dropbox/transparency; www.facebook/about/government_requests; www.google.com/transparencyreport; www.linkedin.com/legal/transparency [22 November 2014].
[712] Comparative study available from https://transparency-reports.silk.co [22 November 2014].
[713] The use of the Internet for terrorist purposes', United Nations Office on Drugs and Crime, September 2012, New York, pp. 90-91. Available from http://www.unodc.org [22 November 2014].
[714] 'Law Enforcement Disclosure Report', *Vodafone*, June 2014, p. 65. Available from www.vodafone.com [22 November 2014].
[715] Blasi Casagran 2013, p. 423.

Facebook will informally provide information to law enforcement bodies if the company has strong reason to believe it is necessary in order to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; or to prevent death or imminent bodily harm.[716]

The situation is made much more complex when law enforcement agencies requesting information are located within the US and the data is stored in servers placed within the EU borders. In theory, the rules should be the same, but in practice the US police authorities barely use MLATs when data is in the EU. Even when the general rule is that US judicial authorities should send a MLA request to the EU judicial courts of the country where the information is stored, a recent judgment shows that it rarely occurs. In the *Microsoft* case,[717] the company was requested to hand over information stored in its Irish servers to the US authorities. The request was accompanied by a search warrant[718] but it did not use the MLA procedures. Search warrants need to prove probable cause but their effects are limited to the US territory. Even though the information was stored within the EU borders (particularly, in Ireland), on 25 April 2014, Judge James C. Francis obliged Microsoft to provide the data. The US judge concluded that no extraterritoriality principles would apply to the case, since Microsoft has no verification system checking every user who registers in the system. For that reason, the judge considered that denying search warrants in the EU would be advantageous to those individuals who are aware of this flaw and use the account for criminal purposes.

From the judgment it can be deduced that US judicial and police authorities see MLA procedures as slow and laborious and, consequently, they are constantly looking for other ways to circumvent such laws. Judge Francis was concerned about a clause included in most of the MLATs which allows the requested party to deny assistance if it deems that the request would be 'contrary to important public policy' or involves 'an offense of a political character'.[719] He also noted that any search using MLATs had to be

[716] Facebook data use policy, available from https://www.facebook.com/about/privacy/other [22 November 2014].
[717] 'In the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation', United States District Court, Southern District of New York, 13 Mag. 2814, p. 19. Available from http://www.nysd.uscourts.gov [22 November 2014].
[718] In the US, the Government has three formal ways to obtain information from an TSP: a subpoena (18 U.S.C. 2703(b)(1)(B)(i)), a court order (18 U.S.C. 2703(d)) and a warrant (18 U.S.C. 2703(a)).
[719] See for example Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-U.K., Jan. 6, 1994, S. Treaty Doc. No. 104–2 ('U.S.–U.K. MLAT'), Article 3(1)(a) and (c)(i).

executed in accordance with the laws of the requested party.[720] Since the US does not have MLATs with all countries, relying only on these procedures would, in his view, be extremely risky.[721]

Therefore, it can be concluded that non-MLA means of obtaining information from private entities are increasingly used by law enforcement authorities on both sides of the Atlantic, but especially by the US. The main concern from the privacy perspective is that police authorities do not always have a court order for accessing content data stored in TSPs, so this practice lacks external oversight.[722] Within this context, the former Vice-president of the European Commission Viviane Reding stated in that, as a general rule, data should only be exchanged via judicial authorities, and not directly through a citizen or company.[723] She added that 'asking the companies directly should only be possible under clearly defined, exceptional and judicially reviewable situations'.[724]

In contrast, the Review Group on Intelligence and Communications Technologies has been encouraging private companies to send records directly to the requesting country.[725] According to the group, this mechanism would shorten the length of time that the procedure takes on average (ten months).

### 3. The EU data protection legislation for international data transfers in the field of law enforcement

As seen in previous sections, EU citizens' data is not only exchanged among law enforcement authorities in the member states, but might also be transferred beyond the EU. One of the main debates on international data transfers concerns the applicable data protection standards. The EU has often been accused of applying double standards when conducting data transfers, depending on whether these are sent to third countries or are

[720] United States District Court, p. 20.
[721] The judgement gives as an example the recent rumours that Google is exploring the possibility to establish 'offshore' servers, beyond the territorial jurisdiction of any nation. See Watson SR 2011, 'Google sets sail: Ocean-based server farms and international law', *Connecticut Law Revie*w, vol. 43, no. 3, p. 709.
[722] For instance, Vodafone, which has its headquarters in the UK, admitted that it received numerous requests without warrant for accessing its users' data between 1 April 2013 and 31 March 2014. See 'Law Enforcement Disclosure Report', *Vodafone*, June 2014, p. 65. Available from www.vodafone.com [22 November 2014].
[723] Speech available from http://www.euractiv.com/video/eu-commissioner-reding-us-meetin-531789 [22 November 2014].
[724] 'European Commission calls on the U.S. to restore trust in EU-U.S. data flows', Press Release European Commission, 27.11.2013.
[725] Liberty and Security on a changing world. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, 12.12.2013, p. 228.

purely intra-European data flows. This section focuses on the data protection safeguards that apply to data transfers beyond the EU. It will be crucial for determining the feasibility of global data protection rules. If the EU already has a consistent data protection framework for data transferred to third countries, EU laws could be used as a model at the international level.

This analysis is divided into three parts. First, it examines the provisions on international data transfers included in Council Decision 2008/977/JHA as well as the draft Directive on Police and Criminal Justice Data Protection. The main goal of this analysis is to determine whether these provisions offer the same level of protection as the provisions applicable for internal EU data transfers. Second, it evaluates the data protection provisions included in the main international agreements between the EU and the US. Particularly, the EU-US PNR agreement, the SWIFT agreement, and the EU-US agreement on data security are examined. Lastly, the EU and the US data protection regimes are compared. This comparison starts by identifying the differences in the conception of the right to privacy, followed by an analysis of the current attempts to approximate the two legal frameworks in the field of privacy.

## 3.1. EU secondary law

### *3.1.1. International data transfers according to Council Decision 2008/977/JHA*

When the EU adopted the first data protection law in 1995, it included a provision for data exchanges beyond the EU borders. It specified the conditions that a third country had to comply with for sharing personal data with an EU country.[726] According to Article 25(1) of Directive 95/46/EC:

'The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures **an adequate level of protection**.' (Emphasis my own).

[726] Article 25 of Directive 95/46/EC.

The Art. 29 WP later clarified that the level of protection of a third country is considered 'adequate' if it complies with the following principles: i) purpose limitation principle, ii) data quality and proportionality, iii) transparency, iv) security principle, v) sensitive data, vi) the right of access, rectification and opposition, and vii) restrictions on onward transfers.[727]

However, Directive 95/46/EC does not cover data transfers to third countries for law enforcement purposes. Member states were initially the only competent authorities to adopt legislation regulating data transfers in the field of security. As a result, there were situations in which one Member State could consider data protection standards of a particular third country (e.g. Nigeria) to be adequate, whereas another Member State could prohibit any exportation of data to that same third country because its data protection standards were not deemed to be high enough.[728]

In 2001 an additional protocol of 108 CoE Data Protection Convention was adopted. This solved the problems of the disparity of rules regarding data were transferred to third countries for law enforcement purposes. According to Article 2 of the protocol, parties could send data to non-Contracting Parties *only* 'if that State or organisation ensures an adequate level of protection for the intended data transfer'. However, that article presented two main limitations. First, paragraph 2 included broad derogations of the adequacy requirement,[729] and second, the adequacy requirement for transborder flows did not apply if a Contracting Party had not ratified the protocol, and not all CoE members have ratified it.[730]

Eight years later, the Commission adopted Framework Decision 2008/977/JHA (FD 2008/977).[731] According to recitals 23 and 24, and Article 13(1)(d), data transfers to third countries could only take place if 'the third state or international body concerned ensures an adequate level of protection for the intended data processing'. Also, that provision establishes an equivalent adequacy mechanism to that of Article 25 of Directive 95/46/EC for international data transfers in the field of the common market. In both cases, the criteria taken into account for any data transfer operation are:

---

[727] 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive', WP 12, 24.07.1998.
[728] de Hert & de Schutter 2008, p. 337; de Hert & Papakonstantinou 2009, p. 412.
[729] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 08.11.2001, ETS no. 181.
[730] De Busser 2009, p. 122.
[731] OJ L 350, 30.12.2008, pp. 60-71.

'[T]he nature of the data, the purpose and duration of the proposed processing operation or operations, the State of origin and the State or international body of final destination of the data, the rules of law, both general and sectoral, in force in the third State or international body in question and the professional rules and security measures.'[732]

The main disappointment of Article 13 is that it includes the same broad and ambiguous derogations as the additional protocol of 108 CoE Data Protection Convention.[733] In this regard, a Member State can still send data to non-EU members without complying with the adequacy criteria if it is for a legitimate specific interest or a public interest. Moreover, in contrast to Directive 95/46/EC, the FD 2008/977 gives a broad margin to member states to decide on specific adequacy parameters. In other words, each Member State assesses the adequacy level according to its own discretion. We must not forget that it is still the competence of the member states, and not the EU, to regulate in the field of criminal matters.

It is worth highlighting here that council framework decisions do not have direct effects for individuals. In consequence, EU citizens whose domestic legislation opposes or does not fully comply with the EU instrument cannot invoke it directly. Another debate stems from recital 38 and Article 26 of FD 2008/977. These provisions state that this framework decision is:

'[W]ithout prejudice to any obligations and commitments incumbent upon Member States or upon the Union by virtue of bilateral and/or multilateral agreements with third States existing at the time of adoption of this Framework Decision.'

Hence, the 2007 EU-US PNR Agreement existing at that time fell outside of the scope of this law. In fact, every international data-sharing agreement has its own data protection provisions.

Therefore, it is can be concluded that there is today no common EU legal framework regulating data transfers in the field of law enforcement. This situation will probably remain the same in the coming years, considering that the proposal for a new EU data

[732] Article 13(4) of Framework Decision 2008/977/JHA, Article 25(2) of Directive 95/46/EC.
[733] De Busser 2009, p. 119.

protection law on crime-related data transfers does not include any change on that issue.

### *3.1.2. International data transfers according to the Proposal for a Police and Criminal Justice Data Protection Directive*

On 25 January 2012, the European Commission launched two proposals dealing with data protection matters: the General Data Protection Regulation[734] and the Police and Criminal Justice Data Protection Directive.[735] This section examines only the latter, which regulates the processing of personal data for law enforcement purposes.

The proposal for Police and Criminal Justice Data Protection Directive (hereinafter, the proposal or the proposed directive) will repeal the current Council Framework Decision 2008/977/JHA when it enters into force.[736] As seen in Chapter 1, the wording of the proposal is ambiguous. Although it states that it does not apply to data processing operations falling outside the scope of Union law,[737] Chapter V and recitals 45, 46, 48 and 49 regulate transfers of personal data to third countries and international organisations. Unfortunately, neither the current FD 2008/977 nor the proposal includes a definition of an 'international data transfer'. A proper definition of this term would clarify, for example, whether the countries that are part of the European Economic Area are considered third countries or not.[738]

Regarding the specific provisions dealing with international data transfers, Article 33 of the proposal establishes that transfers to third countries may only take place if they are necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Moreover, Articles 34 and 35 of the proposal establish that the Commission will be the institution in charge of deciding whether or not an international transfer is adequate in terms of data protection.[739] So it will no longer be the Member State deciding on the adequacy of data protection rules in the third country, but any international data transfer bill needs the consent of the

[734] COM(2012) 11 final, 25.01.2012.
[735] COM(2012) 10 final, 25.01.2012.
[736] Article 58 of the proposal.
[737] COM(2012) 10 final, p. 7.
[738] Guasch Portas V 2014, 'Las transferencias internacionales de datos en la normativa española y comunitaria', *Agencia Estatal Boletín Oficial del Estado*, Madrid, pp. 46-55.
[739] COM(2012) 10 final, recital 48.

Commission. Despite the criticism from some member states,[740] this new role of the Commission will approximate the proposal for the current adequacy procedure of Directive 95/46/EC.[741]

Finally, Article 36 of the proposal enables the derogation of appropriate data protection safeguards when: i) it is necessary to protect the vital or legitimate interests of the data subject, ii) it is essential for the prevention of an immediate and serious threat to the public security, iii) for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and iv) for the establishment, exercise or defence of legal claims.[742] From this provision it can be deduced that future clashes between data protection safeguards and counter-terrorism measures will be solved by derogating individual rights in the best interest of collective security.

Thirteen non-EU countries have adequate data protection systems to date.[743] It means that, in the remainder of third countries, derogations of data protection standards can be accepted as long as they are proved to be 'necessary'.[744] In Chapter 1, it has been shown that the scope and limits of the necessity principle are often ambiguous, and there is the risk that it is interpreted too broadly. In this sense, the EDPS has argued that 'any derogation used to justify a transfer needs to be interpreted restrictively and should not allow the frequent, massive and structural transfer of personal data'.[745]

Article 36 of the proposal does not guarantee that data transferred to third countries with no adequacy decision will not be misused. Given the recent decision from the CJEU considering the Data Retention Directive as contrary to the EU laws, Article 36 should be modified. The Court highlighted the importance of an independent overseer for data transfers to third countries. Yet, neither national DPAs nor the EDPS can control the use of the data once it is transferred to a third country with no adequate legal framework.[746]

A further obstacle is detected in the data protection principles of Article 4 of the

---

[740] The UK has no general opt-out from this proposal. See Hinarejos A, Spencer JR & Peers S 2012, 'Opting out of EU Criminal law: What is actually involved?', *CELS Working Paper*, New Series, no. 1, Cambridge, p. 4.
[741] Peers 2012, p. 4.
[742] COM(2012) 10 final, recital 48.
[743] These are Uruguay, Switzerland, Israel, Canada, Argentina, Guernsey, Isle of Man, Andorra, Australia, Faeroe Islands, Jersey, New Zealand and the U.S.
[744] WP 191, 23.03.2012, p. 31.
[745] European Supervisor of Data Protection, 'Opinion on the data protection reform package', 07.03.2012, p. 65.
[746] Boehm & Cole 2014, p. 84.

proposal. Although this provision lists the same data protection principles as those in Article 6 of Directive 95/46/EC, the proposed directive is more limited in terms of its scope. For instance, these principles will not apply for previous international agreements in the field of police and judicial cooperation. According to Article 60, previous international agreements (e.g. the EU-US MLA agreement) will remain unamended for the five years after the directive enters into force. Assuming that the proposal enters into force in 2016, they would not be amended until 2021.

Another limitation is found in those EU instruments that regulate the processing of data collected by private entities for commercial purposes and then transferred to law enforcement authorities. This is the case of PNR data. The proposed General Data Protection Regulation will deal with cross-border data flows resulting from the functioning of the internal market. In contrast, the proposed directive will address the processing of personal data for police and criminal matters. But what legal instrument will bind data processing operations combining both commercial and security purposes? As noted by the EDPS,[747] that might be a controversial issue in the future, since both legislative proposals do not have the same level of data protection. It might occur that, for the same operation, one country applies the regulation standards, whereas another Member State bases its laws on the proposed directive.[748]

In conclusion, neither the current FD 2008/977/JHA nor the future directive on data protection in the field of law enforcement offer a full-fledged legal framework when a Member State transfers personal data to law enforcement authorities beyond the EU. One of the obstacles mentioned in this section is that these instruments do not apply for data transfers that fall within the scope of a specific data-sharing agreement concluded between the EU and a third country. Therefore, it is now necessary to examine whether data protection provisions in the main international agreements are similar to those foreseen in the proposed directive.

[747] European Data Protection Supervisor, Opinion on the data protection reform package, 07.03.2012, pp. 7 and 51.
[748] WP 191, 23.03.2012, p. 26.

## 3.2. Data protection provisions in the main international agreements between the EU and the US

Many international agreements regarding the exchange of information for law enforcement purposes have been signed between the EU and the US to date. Each of these agreements includes their own data protection provisions. This section examines the data protection provisions of the main EU-US agreements based on the exchange of information for security reasons: the PNR agreement, the SWIFT agreement and the agreement on the security of classified information. No study is carried out on the CSI, because the maritime information that the EU transfers to the US does not contain personal data. Likewise, no analysis is conducted as regards the EU-US MLAT because the agreement does not include provisions on data protection, except for the purpose limitation rule in Article 9. This lack of data protection clauses in the MLAT is however corrected by the fact that the agreement is currently subject to the FD 2008/977.

This study seeks to unveil whether all these agreements have the same data protection provisions or not. If it is concluded that each agreement has it own provisions, it means that different levels of protection are applied to EU citizens' data depending on the particular instrument. It would ultimately complicate the establishment of global data protection rules in the field of security.

### *3.2.1. Data protection in the EU-US PNR agreement*

The current EU-US PNR Agreement was adopted in 2012. Before examining it, it is pertinent to observe what data protection provisions were included in the previous PNR agreements.

The first draft of the 2004 EU-US PNR Agreement collected 38 PNR categories of data. However, during the negotiations of the agreement, this dropped from 38 to 34.[749] Moreover, there was no possibility for EU citizens to access their data and to have judicial redress.[750] Two particular aspects of that first agreement are, however, positive. The first is that data was retained for only three years and six months.[751] The other is

[749] De Busser 2009, p. 373.
[750] Pawlak P 2012, 'Homeland security in the making American and European patterns of transformation', *European Homeland Security. A European strategy in the making?,* eds. Kaunert C, Leonard S & Pawlak P, Routledge, NYC, p. 18.
[751] De Busser 2009, p. 381.

that the CBP used a 'push-system', through which airlines retained control over their databases for the CBP requests. That system lowered the chances for abuses by law enforcement agencies.[752]

As seen earlier, the 2004 EU-US PNR Agreement was found to be in breach of EU laws. The ground used by the EP to challenge the agreement was mainly an infringement of the fundamental principles of Directive 95/46/EC. Yet, that issue was never properly examined by the CJEU, which focused its decision on the examination of the applicable legal basis. The CJEU ruling gave airline companies an escape route, as before the judgment they found themselves in a catch-22 situation because they could not comply with the conflicting US and Community obligations. As for the EU citizens, the court decision resulted in lower data protection safeguards: prior to the ruling, the agreement fitted under the scope of the internal market provision and, consequently, European institutions had competence to enforce citizens' fundamental rights and principles. In contrast, subsequent agreements of 2006[753] and 2007[754] fell outside the scope of the first pillar and, therefore, adequacy levels required by Directive 95/46/EC were no longer applicable. The Council became the only institution entitled to decide on the mandate of the agreement, and the EP had no formal say in the negotiations.

The 2007 EU-US PNR Agreement decreased the protection of personal data in the following issues: first, data was no longer processed through the push method, but through the pull method. This means that the subjects in charge of processing personal data changed from private actors (air carriers) to public entities (law enforcement agencies), and the US authorities were now competent to extract data from the airlines' databases. Second, data was to be kept for seven years from the moment of collection, and then moved to an inactive database for a further eight years. This meant a total retention period of fifteen years, in contrast to the three and a half years of the previous agreement. Third, the DHS, and not the CBP, was the competent authority for the processing of data. This change had negative implications, since it gave access to PNR data not only to that specific body, but also to all other US agencies with counter-terrorism functions. Fourth, information (including sensitive data)[755] received at the

[752] De Busser 2009, p. 371.
[753] OJ L 298, 27.10.2006, pp. 29-31.
[754] OJ L 204, 04.08.2007, pp. 18-25.
[755] Sensitive data can be defined as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or concerning the health or sex life of the individual. See Faull & Soreca 2008, p. 414.

DHS could be easily transferred to foreign authorities. Finally, PNR data was used to detect more criminal offences than the previous agreement.[756]

Notwithstanding the general decrease of data protection, a few positive aspects of the 2007 EU-US PNR Agreement need to be highlighted. The main one is the fact that the number of categories of PNR data collected was reduced from 34 to 19. However, many scholars have stated that the shorter list did not necessarily mean that less data were included. De Busser used the example of the number of bags. The 2007 agreement included a single category of 'all baggage information', whereas the 2004 agreement added the elements 'bag tag numbers', 'number of bags' and 'general remarks' regarding a passenger's luggage.[757] Another positive feature was that the 2007 EU-US PNR Agreement foresaw the conducting of periodical reviews to check the compliance with privacy measures.[758] That was not required in the 2004 agreement.

The current 2012 EU-US PNR Agreement[759] includes many improvements in terms of data protection in comparison with the previous agreements. With regard to the method used to transfer data, it prescribes the 'push method', a process by which airline companies collect PNR data in their databases and then transfer such data to the respective government authorities. The push system is a sign of progress, considering that 2007 EU-US PNR agreement used the 'pull method' for transferring data. Under the old pull method, the US authorities had access to all data in airline companies' databases. Consequently, data was collected and processed under US laws, preventing EU data protection laws from being enforced.

However, this 'push method' is not fully implemented in practice: in 2013 the Privacy Office found that the 68% of air carriers had already transitioned to that system, but the 'pull' method was still used by 15 air carriers.[760] In that sense, the Commission has asked airline companies to fully move to the 'push' method, since it is required by Article 15(4) of the agreement.[761]

---

[756] Archick 2013, p. 14.
[757] De Busser 2009, p. 374.
[758] In this sense, a Joint Review took place in the Autumn of 2008, and a second one was carried out in February 2010. See 'A report on the use and transfer of Passenger Name Records between the European Union and the United States', *U.S. Department of Homeland Security, Privacy Office*, 03.07.2013, p. 9; 'How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel', U.S. Department of Homeland Security, Privacy Office, 05.11.2011, p. 6.
[759] OJ L 215, 11.08.2012, p. 5-14.
[760] SEC(2013) 630 final, 27.11.2013, pp. 14-15; 'A report on the use…', U.S. Department of Homeland Security, Privacy Office, 03.07.2013, pp. 5 and 17.
[761] COM(2013) 844 final, 27.11.2013, p. 2.

Data retention periods are also improved in the current agreement. In fact, the DHS had to introduce changes to the technology of the ATS in order to adapt to the requirements of Article 8. Authorised ATS users have access to an active database up to five years. Yet, PNR data are depersonalised after six months.[762] That means that after that period, authorised ATS users can only see the record locator, the reservation system, the date record, and the itinerary.[763] Thus personal data are no longer visible. A repersonalisation is still possible, but it lasts for a maximum of twenty-four hours. In addition, it requires prior authorisation by a supervisory agent and proof that there is a specific threat or risk. After five years, data is moved to a dormant, non-operational database. Data transferred to this dormant database will be retained for ten years in cases of transnational crime information (five years less than under the previous 2007 EU-US PNR Agreement), and for fifteen years in cases of terrorism information. During that period, access will only be possible with the approval of a senior DHS official designated by the Secretary of Homeland Security. After ten or fifteen years, PNR data will be automatically deleted, and no repersonalisation will be possible.

As for the categories of data collected, the agreement keeps the same number of items as those in the 2007 agreement: air carriers will provide a maximum of nineteen data categories, which are the following:

*Table 2.1.*

| |
|---|
| 1. PNR record locator code |
| 2. Date of reservation/issue of ticket |
| 3. Date(s) of intended travel |
| 4. Name(s) |
| 5. Available frequent flier and benefit information (i.e., free tickets, upgrades) |
| 6. Other names on PNR, including number of travelers on PNR |
| 7. All available contact information (including originator of reservation) |
| 8. All available payment/billing information (e.g., credit card number) |
| 9. Travel itinerary for specific PNR |
| 10. Travel agency/travel agent |
| 11. Code share information (e.g., when one air carrier sells seats on another air carrier's flight) |

| |
|---|
| 12. Split/divided information (e.g., when one PNR contains a reference to another PNR) |
| 13. Travel status of passenger (including confirmations and check-in status) |
| 14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote (ATFQ) fields |
| 15. Baggage information |
| 16. Seat information, including seat number |
| 17. General remarks including Other Service Indicated (OSI), Special Service Indicated (SSI) and Supplemental Service Request (SSR) information |
| 18. Any collected APIS information (e.g., Advance Passenger Information (API)) that is initially captured by an air carrier within its PNR, such as passport number, date of birth and gender) |
| 19. All historical changes to the PNR listed in numbers 1 to 18 |

[762] The Commission has argued that the six months have to start to count from the moment the information is loaded in ATS, and not from the moment PNR data is updated in ATS. See COM(2013) 844 final, 27.11.2013, p. 3; SEC(2013) 630 final, 27.11.2013, p. 18.

[763] 'A report on the use and transfer of Passenger Name Records between the European Union and the United States', *U.S. Department of Homeland Security, Privacy Office*, 03.07.2013, p. 16.

As seen in the Table 2.1., there is no information on racial or ethnic origin, political views, religion, or sex life of the individual. However, if sensitive data is collected by an air carrier (e.g. concerning the health or dietary requirements of the passenger), it will be subject to special treatment. The ATS-P has programmed certain codes that detect and filter 'sensitive' information. These codes automatically mask the information to prevent routine viewing. If an authorised ATS user retrieves information classified as 'sensitive', that access will be emailed within twenty-four hours to the CBP management,[764] and the information will be deleted after thirty days.[765]

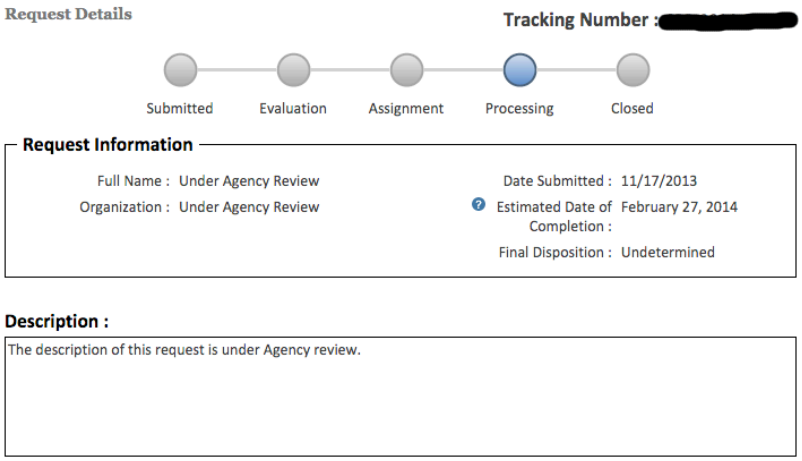
As for the individual rights included in the current EU-US PNR Agreement, any passenger of any nationality has in principle the right to access, rectify and delete the information that the CBP has processed about him/her. Data can be accessed by sending a Freedom of Information Act (FOIA) request. If the disclosure is rejected, there is an appeal procedure and the individual can go to the federal court as the last instance. In 2011 there were 220,000 FOIA requests,[766] and from July 2012 to March 2013, the CBP received a total of 21,606 requests, 27 of which were specifically on PNR (none of them was from EU citizens).[767] The majority of requests came from immigration and custom agencies,[768] and they were apparently processed within 38 days on average.[769]

For the purposes of this study, I followed the procedure of three data requests to the CBP from EU citizens (in particular, from France, Spain and Hungary) during the years 2013 and 2014. None of them was completed in 38 days. In fact, in 2015 none of the applicants has received the information yet. The only application that the CBP replied was to inform the applicant their request had been rejected. The other two remain unanswered by the US government.[770]

---

[764] 'A report on the use and transfer of Passenger Name Records between the European Union and the United States', U.S. Department of Homeland Security, Privacy Office, 03.07.2013, p. 16.
[765] European Commission, MEMO/13/1054, 27.11.2013, p. 2.
[766] Subcommittee Hearing: Intelligence Sharing and Terrorist Travel: How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel, 5.11.2011. Available from http://homeland.house.gov [19 December 2014].
[767] SEC(2013) 630 final, 27.11.2013, p. 12.
[768] Subcommittee Hearing: Intelligence Sharing and Terrorist Travel: How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel, 05.11.2011. Available from http://homeland.house.gov [19 December 2014].
[769] SEC(2013) 630 final, 27.11.2013, p. 12; 'A report on the use and transfer of Passenger Name Records between the European Union and the United States', U.S. Department of Homeland Security, Privacy Office, 03.07.2013, p. 18.
[770] See annex I of this thesis.

*Figure 2.2.*




*This is the permanent message that shows for the two unanswered applications*

Even if the CBP eventually sends the data, this delay of over one year must be viewed with disappointment, especially considering that a similar PNR data request sent to the Australian government was completed after only 15 days.[771]

Provisions on onward transfers are also found in the agreement. Data stored in ATS can be shared with non-DHS governmental agencies (within or beyond the US) after verifying that the requester has a need to know the information by the requester.

The use and disclosure of PNR data is regulated in the Customs and Border Protection Directive.[772] According to this law, requesters need to sign specific PNR disclosure forms in which they agree to treat the information provided as confidential and not to send it on other third parties without prior DHS authorisation.[773] The system logged 589 disclosures when the last PNR joint review took place in April 2013, and only one came from the EU.[774]

Data security measures are also present in the agreement. The DHS has noted that:

'[U]sers may only access PNR through ATS-P, which can only be accessed through a web-based user interface over the DHS infrastructure or remotely through secure-encrypted mobile devices for certain CBP officers in foreign locations and at

[771] See Annex II of this thesis.
[772] SEC(2013) 630 final, 27.11.2013, p. 3.
[773] 'A report on the use and transfer of Passenger Name Records between the European Union and the United States', *US Department of Homeland Security, Privacy Office*, 03.07.2013, p. 14. See also 5 U.S.C. 552a(b) of the Privacy Act.
[774] SEC(2013) 630 final, 27.11.2013, pp. 8 and 16.

Ports of Entry.'[775]

Thus, the CBP network can only be accessed by authorised users through secure encrypted devices requiring a password.[776] Any internal sharing is logged locally on hard copy, and data requests from non-DHS agencies are also retained and audited.

Regarding the overseeng of PNR transfers, audits of the use of ATS-P are carried out every six months by the CBP's Office of Internal Affairs. If the audits show that a user has conducted an unauthorised access or disclosure, it may result in criminal sanctions.[777] Therefore, all PNR users need to undergo privacy training and pass an examination before using ATS. Finally, independent supervision is conducted by the Chief Privacy Officer, the Department of Homeland Security Office of Inspector General, the US Government Accountability Office and the US Congress.[778] Also, since February 2012, a new Privacy Oversight Team has been incorporated in the DHS Privacy Office. It deals with privacy investigations, privacy complaint handlings and redress, among other tasks.[779]

The agreement explicitly states that decisions cannot be based solely on automated processed data. This provision aims to prevent illegal profiling.[780] This clause is particularly important considering the numerous errors that have been committed in the past due to the lack of investigation into hits of potential suspects of terrorism. The case of Maher Arar is an example. Arar is a dual citizen of Canada and Syria who was denied entry into US territory on 26 September 2002. The decision was taken after the Department of State's cross-matched passenger information from APIS and identified Arar as a 'special interest' alien who was suspected of terrorism and described as armed and dangerous. The inspectors of the Immigration and Naturalisation Service (INS) arrested him at the US airport and returned him to Syria, where he was subjected to

[775] SEC(2013) 630 final, 27.11.2013, p. 29.
[776] According to a recent Commission report, around 12,448 users have direct access to PNR. SEC(2013) 630 final, 27.11.2013, p. 10.
[777] 'A report on the use and transfer of Passenger Name Records between the European Union and the United States', *US Department of Homeland Security, Privacy Office*, 03.07.2013, p. 22.
[778] European Commission, MEMO/13/1054, 27.11.2013, p. 2.
[779] 'A report on the use and transfer of Passenger Name Records between the European Union and the United States', *US Department of Homeland Security, Privacy Office*, 03.07.2013, p. 6.
[780] European Commission, MEMO/13/1054, 27.11.2013, p. 2; Archick 2013, p. 14.

beatings and torture for over a year. Finally, he was found innocent and released to Canada.[781]

Even though the EU-US PNR Agreement incorporates several provisions that limit the collection, use and storage of EU citizens' data by the DHS, some rules may still be contrary to EU laws. The recent CJEU decision to annul the Data Retention Directive provided valuable guidance about what practices by which law enforcement authorities violate the right to data protection of EU citizens. In a study requested by the LIBE Committee, Boehm identified many provisions of the agreement that would contradict the CJEU judgment. Particularly, these are Article 4 on the purpose, Article 8 on the data retention, Article 14 on the oversight, Article 15(5) on the ad-hoc 'pull' method, Article 17(1) on the onward transfers and Article 21 on the rights of the data subject.[782] Therefore, after the judgment,[783] this agreement would need to be revised and adapted in accordance with the parameters established by the Court.

### *3.2.2. Data protection in the SWIFT Agreement*

From 2001 to 2009, the Belgian company SWIFT transferred financial data from EU citizens to the US authorities without any formal agreement. As mentioned earlier, SWIFT's headquarters were in Belgium and, consequently, Belgian Data Protection Law (which implemented Directive 96/46/EC) was applicable. On 30 November 2009 the EU and the US signed the first SWIFT Agreement, which authorised the transfer of financial data to the US Department of the Treasury for the prevention, investigation, detection, or prosecution of terrorism or terrorist financing. The agreement was vetoed by the EP in February 2010, on the basis that adequate data protection safeguards were lacking (see section 2.1.3 above). By mid-June 2010, the second and current SWIFT Agreement was adopted, this time approved by the EP.

Regarding the data protection provisions of the current SWIFT Agreement, some of them differ from those found in the EU-US PNR Agreement. For instance, data categories in SWIFT refer to the originator and/or recipient of a transaction, including

[781] For the details of Maher Arar's case, see 'The removal of a Canadian citizen to Syria', Department of Homeland Security, Office of Inspector General, OIG-08-18, March 2018. Available from http://www.oig.dhs.gov/assets/Mgmt/OIGr_08-18_Jun08.pdf [23 November 2014].
[782] Boehm & Cole 2014, pp. 58-65.
[783] CJEU, joined cases C-293/12 and C-594/12, *Commission* v. *Ireland* and *Digital Rights Ireland*, 8.04.2014

name, account number, address, and national identification number.[784] Once the data enters the database of the US Department of the Treasury, it is retained for 'no longer than necessary to combat terrorism or its financing', with five years being the maximum retention period.[785] This does not coincide with the provisions established in the EU-US PNR Agreement, which processes up to nineteen categories of data and permits passenger data to be retained for up to fifteen years.

Articles 12 and 13 of the SWIFT Agreement regulate the supervision of data transfers. It requires the establishment of independent overseers, one appointed by the Commission[786] and the other by the US Department of the Treasury. They perform regular checks on the TFTP database (or 'black box') to confirm that it complies with the extraction requirements.[787] In particular, overseers control that any extraction is based on the value of data for the investigation, prevention, detection, or prosecution of terrorism or its financing; the processing is necessary and proportional; and it includes adequate data security measures (Article 5 of the agreement). If any search or extraction appears to be in breach of the data protection safeguards of Article 5, overseers will then report and block that operation.[788]

Articles 14, 15, 16 and 18 of the agreement refer to the individual rights, namely, the rights to data access, right to rectification, erasure and blocking of inaccurate data, and non-discriminatory administrative and judicial redress. In the particular case of data access, any individual can request data that the US Department of the Treasury has control over via the national data protection authority (DPA). The DPA then sends the formal request to the US authorities.

During the current study, I myself sent a request for my own SWIFT data to the Spanish DPA. I requested access to my financial data in April 2014, and the Spanish DPA sent the request to the US Department of the Treasury. One year later, I received as a response that the US Department of the Treasury was 'unable to confirm or deny the existence of any responsive records'. The letter then added that the disclosure of such information could identify subjects of ongoing counterterrorism investigations or harm national security.[789] From this response, there are two possible conclusions: Either I have been particularly targeted as a suspect of a serious crime by the US authorities, or

[784] Article 5(7) of SWIFT Agreement.
[785] Article 6(4) of SWIFT Agreement.
[786] European Commission, MEMO/13/1060, 27.11.2013.
[787] De Busser 2009, p. 388.
[788] European Commission, MEMO/13/1060, 27.11.2013.
[789] See Annex III of this thesis.

the letter I recieved is a standarised answer for any data request. Either way, it is very worrisome. Therefore, in line with the recommendation made in an EP study about the TFTP, there is a real need for 'making the right to access, rectification, erasure, blocking and administrative and judicial redress a reality'.[790]

Some data protection provisions are the same in PNR and SWIFT agreements. For instance, data is extracted via the push method in both agreements. Article 4(6) of SWIFT Agreement establishes that it is the designated provider (i.e. SWIFT) that provides the data directly to the US Treasury Department. Moreover, SWIFT needs to keep a detailed log of all data transferred to the US.

Another similarity is found in the provision regulating onward transfers (Article 7 of the agreement). In line with the current PNR agreement, data can be shared with law enforcement, public security and counter-terrorism authorities in the United States; with member states; and with third countries. SWIFT also mentions Europol, as a possible receptor of the data. The narrow link between the US Department of the Treasury and Europol stems from the fact that the latter verifies that each request 'is tailored as narrowly as possible to minimise the amount of data requested'.[791] This practice is thoroughly examined in Chapter 3 of this thesis. Finally, the agreement also coincides with the current PNR agreement[792] in the obligation to obtain prior consent of the competent member states' authorities before EU citizens' data are shared.

It can therefore be concluded that, although there are some equivalences as regards the push method and the onward transfers in both the PNR and SWIFT data exchanges, we find many differences in the data protection provisions included in SWIFT and PNR agreements. Moreover, as with the EU-US PNR Agreement, the recent CJEU decision on the Data Retention Directive might have some implications for the SWIFT Agreement. In particular, the fact that SWIFT data is transferred in bulk, the lack of an independent administrative oversight and the absence of notification to the data subjects contradict the Court's core arguments.[793]

[790] Wesseling 2014, p. 33.
[791] European Commission, MEMO/13/1060, 27.11.2013.
[792] Article 17(4) of EU-US PNR Agreement.
[793] Boehm & Cole 2014, pp. 72-75.

*3.2.3. EU-US agreement on the security of classified information*

The protection of data is closely related to the establishment of data security. In fact, the implementation of data protection always requires the existence of data security measures. In this sense, Article 17(1) of Directive 95/46/EC states:

'Member States shall provide that the controller must *implement appropriate technical and organizational measures to protect personal data* against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.' (Emphasis my own)

Classified information routinely includes personal data. EU data security legislation was first adopted in 2001 through Council Decision 2001/264/EC,[794] which was later amended by Decision 2011/292/EU.[795] The EU also concluded an agreement with the US authorities on common standards for the security of classified information.[796] The agreement has lower data protection safeguards than the SWIFT and the PNR agreements. These only regulate the establishment of minimum standards of security (Article 4.1), the purpose limitation principle (Article 4.3), the prohibition of onward transfer without prior consent (Article 4.4), encryption measures (Article 9.2), and oversight rules (Article 12).

There are two other controversies as regards the data security agreement between the EU and the US. First, the security classification of Article 3 sets out different categories depending on the law enforcement authorities that have collected the information. EU authorities use a classification that distinguishes between: a) top secret, b) secret, c) confidential and d) restricted (Article 3(b)). Yet, when the information is sent by the US authorities, the classification is reduced to: a) top secret, b) secret, and c) confidential (Article 3(a)).

The level of classification is always marked by the data provider. This lack of consistency might lead to ambiguities on both sides of the Atlantic about what is considered 'classified information' and what is not. Particularly, the fact that a

[794] OJ L 101, 11.04.2001, p. 1.
[795] OJ L 141, 27.05.2011, pp. 17-65.
[796] OJ L 115, 03.05.2007, p. 29.

document labelled as 'restricted' is seen as classified information in the EU but not in the US might cause confusion about what parts of the document can actually be disclosed. In this sense, it could easily occur that restricted information is exposed to the public with no limitation once it is transferred to the US.

Second, Article 9 establishes that 'classified information shall be transmitted between the parties through mutually agreed channels'. This provision reflects the existing imprecision in the use of channels. The current discretion for the choice of channel could create problems of multiplicity of communication channels, and make it more difficult to implement common security measures for all data transfers.

Lastly, Article 19 states that '[n]othing in this Agreement shall alter existing agreements or arrangements between the Parties, nor agreements between the US and Member States of the European Union'. According to this provision, the agreement does not apply to other international agreements between the EU and the US such as PNR and SWIFT. This provision restricts enormously the scope of the agreement on classified information. Also, it does not solve the current discrepancies of data protection and security safeguards for specific transatlantic agreements.

Although the EU-US data security agreement is less problematic than data protection agreements,[797] this section has identified some data security controversies. We have to look at data protection and data security as intertwined synergies. Therefore, having different rules on data protection and data security legal frameworks on both sides of the Atlantic affects the consistency of transatlantic data exchanges in the field of law enforcement.

## 3.3. EU-US data protection regimes

### *3.3.1. Different conceptions of privacy in the US and the EU*

Although the EU and the US have made huge efforts to show to the world that they share common values, common interests and common responsibilities,[798] in practice many important divergences as regards their privacy laws are evident. This section focuses precisely on examining the differences between the EU and the US regarding

[797] O'Neill 2012, p. 180.
[798] See, for instance, Remarks by U.S. Ambassador to the EU, William E. Kennard, at Forum Europe's 3rd Annual European Data Protection and Privacy Conference. 04.12.2012; Available from http://useu.usmission.gov/data_privacy.html [23 November 2014].

the notion of privacy.

The main difference to be highlighted is that the EU considers 'privacy' as a human right, whereas the US tends to value it as a liberty over and against the state. This distinction has a historical explanation. The sensitivity that the EU has on privacy has its origins in the horror suffered by Jews during the Holocaust. The Nazis used public and church records to indentify Jewish people, so that they might be persecuted and ultimately be sent to concentration camps.[799] As a result of those abuses, the idea of human dignity, as well as the protection of one's identity have been significantly reinforced within the EU during the twentieth and twentieth-first centuries.[800]

Besides the idea that every individual has the right to enjoy a private life (Article 7 of the EU Charter of Fundamental Rights), the EU has taken a step further by establishing a 'right to data protection' (Article 8 of the Charter). In general terms, the main difference between the right to privacy and the right to data protection is that the latter is linked to the idea of self-determination, by which any individual should be able to decide how their data is processed. The right to data protection is thus connected to natural persons and it safeguards the human identity. In the US, laws only refer to the right to privacy, but EU laws treat these two concepts separately.[801]

The right to data protection constitutes a 'general principle of law' within the EU, and it is also regulated in Article 16 TFEU. This fundamental right has long been protected by many rulings issued by the highest European and Member State courts, including the ECtHR.[802] Likewise, the idea of data protection has been included in the constitutions of almost all member states.

In contrast, the US Constitution does not regulate the right to privacy against all circumstances, but only protects individuals against governmental action, and within the limits established by the US Fourth Amendment. The Fourth Amendment is the main

[799] Sullivan B 2006, ''La difference' is stark in the EU, US privacy laws', *NBC News*, 1 October. Available from www.nbcnews.com [23 November 2014].

[800] Hughes JT 2013, 'Bridging the EU-US privacy gap', *IAPP*, 22 April. Available from https://www.privacyassociation.org [23 November 2014].

[801] On the distinction between the terms 'privacy' and 'data protection', see González Fuster G 2014, 'The emergence of personal data protection as a fundamental right of the EU', *Springer*, London, pp. 257-262. Also, see Hondius F.W. 1983, 'A Decade of International Data Protection', *Netherlands International Law Review,* pp. 103-128.

[802] See, for instance, the case-law of the CJUE: C-450/00, Commission v. Luxembourg, 04.10.2001; C-465/00 and C-138/01, Rechnungshof v. Osterreichischer Rundfunk, 20.05.2003, C-101/01, Lindquist, 06.11.2003; C-524/06, Huber v. Germany, 16.12.2008; C-73/07, Tietosuojavaltuutettu [Finnish data protection ombudsman] v. Satakunnan Markkinaporssi Oy and Satamedia Oy, 16.12.2008; C-28/08, Commission v. Bavarian Lager Co., 29.06.2010; C-92/09 Volker und Markus Schecke GbR v. Land Hessen, and C-93/09, Eifert v. Land Hessen and Bundesanstalt fur Landwirtschaft und Ernahrung, 09.11.2010, among others.

binding provision as regards the right to privacy. That clause offers protection to the US citizens – or non-US citizens who are long-term residents in the US – as long as they have suffered an unreasonable search and seizure by the US government. Yet, the US Constitution does not protect individuals against violations committed by non-governmental actors. In such cases, the right to privacy can only be enforced through sectoral laws,[803] self-regulation[804] and privacy-enhancing technologies.[805]

The EU-US divergence is also seen in the fact that in the US privacy is associated with a governmental obligation to refrain from taking specific actions. In other words, it is linked to a negative duty. Instead, the EU perceives the right to privacy as a positive duty: the government must not only abstain from conducting certain activities, but it has to 'affirmatively protect privacy rights'.[806] Thus, according to the EU perspective, it is not sufficient that EU governments refrain from carrying out unreasonable searches, but they have an additional positive obligation to make sure that no individual is unlawfully monitored by a third person (either governmental or non-governmental).

At this point, one might ask: are privacy standards higher in the EU than in the US in the field of law enforcement? Although several academic studies conclude that privacy rights are similar on both sides of the Atlantic,[807] I believe they are not.

One of the main privacy flaws in the US (not present in the EU laws) relates to the great number of exemptions to the applicability of the purpose limitation principle. This principle is one of the core requirements of adequate data protection standards in the EU. However, it is not regulated in the US legal framework at all. In fact, since the adoption of the Patriot Act in 2001, the US government has been processing data that

---

[803] For instance, the 1986 Electronic Communications Privacy Act (ECPA), the 1974 Family Educational Rights and Privacy Act (FERPA), the 1994 Driver's Privacy Protection Act and the 1978 Right to Financial Privacy Act.

[804] Industries are expected to take responsibility for their own data protection safeguards.

[805] For instance, the use of encryption or smartcards systems to enhance the protection of personal data.

[806] Kuner C 2013, 'The transatlantic divide over data privacy rights', *IAPP*, 20 May. Available from www.privacyassociation.org [23 November 2014].

[807] In this sense, 'Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the European Union and the United States', *US State Department*, 04.12.2012, p. 2.; Bamberger K & Mulligan D 2013, 'Privacy on the ground: Governance choices and corporate practice in the U.S. and Europe', *George Washington Law Review*, vol. 81, no. 5, pp. 1529-1664; Tene O 2014, 'The U.S.-EU privacy debate: Conventional wisdom is wrong', *Privacy Perspectives*, 4 March. Available from https://privacyassociation.org [23 November 2014]; Bender D 2014, 'Why is the U.S. on the defensive?', *IAPP*, 14 March. Available from https://privacyassociation.org [23 November 2014]; Schwartz PM 2014, 'Differing privacy regimes: A mini-poll on mutual EU-US distrust', *IAPP*, 22 July. Available from https://privacyassociation.org [23 November 2014]; Rosenzweig R 2014, 'American privacy values vs. European perceptions', *The Business of General Technologies*, 8 August. Available from http://fcw.com/ [23 November 2014].

was originally collected for other purposes.[808] Particularly, Section 215 of Patriot Act increased the US government's control over all communications collected by TSPs. Under that provision, US law enforcement and intelligence authorities are able to collect phone metadata of any US citizen without prior warrant.[809]

Similarly, the EU adopted the Data Retention Directive. This law obliged European TSPs to store metadata for a period between six months and two years, depending on the Member State. The directive, however, was annulled by the CJEU in April 2014. As mentioned in Chapter 1 of this thesis, the grounds were the infringement of the purpose limitation, the proportionality and the necessity principles as stated in Directive 95/46/EC, as well as Articles 7 and 8 of the Charter.[810]

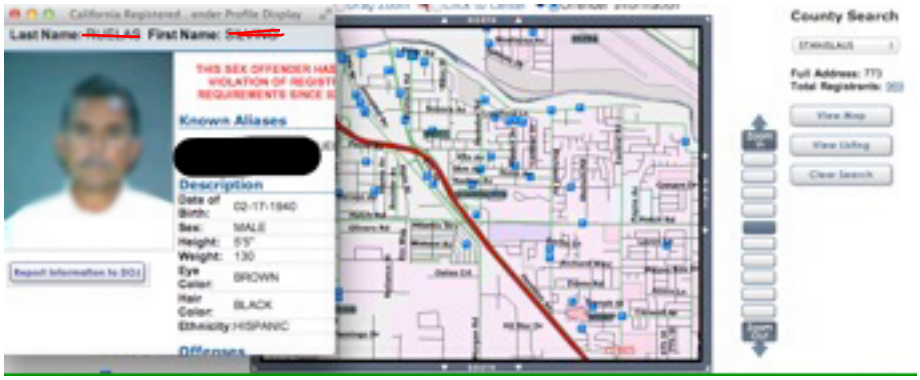
Another difference between the EU and the US concerns the retention periods. Precisely, the Data Retention Directive obliged phone companies to keep users' data for a period of between six month and two years. As mentioned above, the directive was annulled by the CJEU for violating EU fundamental rights. If we compare this ruling with the situation in the US, we notice that there are no US laws for retention periods. Each TSP decides for how long it wants to retain its users' data. For instance, *Verizon* keeps subscriber information from three to five years and call records for one year; whereas *Sprint* preserves subscriber information for an unlimited period, and keeps call details for approximately eighteen months.

Another privacy weakness that we find in the US and not in the EU concerns the publication of criminal records, and the subsequent difficulties of 'being forgotten' even after having served a sentence. One example is found in several US States with regard to the so-called 'Megan's Law'. Megan was a seven-year-old girl who was tragically raped and killed in 1994 by her neighbour in New Jersey. The murderer had been found guilty of committing several sex offences on other young girls before, but people living in his neighbourhood were not aware of this. Therefore, a month after the murder, New Jersey passed the first 'Megan's Law', by which any sex offender would be registered and publically identified on the Megan's law website of the State. The law had the

[808] See Smith J.C. 2003, 'The USA Patriot Act: Violating reasonable expectations of privacy protected by the fourth amendment without advancing national security' , *82 North Carolina Law Review*, pp. 412-455.
[809] This law is examined in Chapter 4 of this study.
[810] See Chapter 1 section 3.2.3 of this thesis.

purpose of informing other neighbours about the location of sex offenders, including the name, picture, address, nature of crime and the incarceration date.[811]

*Figure 2.3.*




*Open source: www.meganslaw.ca.gov (random search, face and name covered on my own)*

This example shows how in the US the freedom of expression, regulated in the US First Amendment, may often override the right to privacy if the purpose is justified, as in the case of sex offenders. No similar public database could ever exist in the EU. The right to freedom of speech is regulated differently in each Member State, and some give it higher importance than others. The EU courts have also been reluctant to keep criminal records indefinitely. In that sense, the ECtHR ruled in 2008 that DNA data of EU citizens arrested but never charged could not be retained permanently in police databases.[812] As for the publication of criminal records on the Internet, judgments of national courts (constitutional courts' rulings)[813] are excluded from the indexes of search engines through robots.txt. This is a measure that avoids linking police and judicial records to the name of a person via search engines. Likewise, the CJEU has demonstrated that someone can be formally 'forgotten' from the indexes of search engines, even if their name is linked to the website of a newspaper, as long as the information is no longer accurate and relevant to society.[814] In that particular case, the information to be removed revealed high social security debts that an individual had already paid off a long time ago. The CJEU argumentation for erasing information

[811] Megan's Law website in California: http://www.meganslaw.ca.gov
[812] S. and Marper v. the United Kingdom, [2008] ECHR 1581, 04.12.2008.
[813] Blasi Casagran C & Blasi Casagran E 2012, 'Spain makes Google remove personal information from index', *Privacy, Laws & Business, International Report*, no. 120, pp. 27-30.
[814] Case C-131/12, 13.05.2014.

could also be used to remove criminal data once the EU citizen has already served their sentence.

### *3.3.2. Attempts to approximate the EU and the US privacy legislations*

The EU and the US have launched many initiatives to approximate their privacy laws, basing them on global principles and conventions that they have both signed. They have also already adopted a few bilateral instruments that seek to establish common privacy rules.

As regards global principles subscribed to by the EU and the US, four main instruments can be distinguished: The OECD Privacy Guidelines, The APEC Privacy Framework, The Fair Information Practice Principles (FIPPs), and The Council of Europe Cybercrime Convention.

The OECD released recommendations concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines) in September 1980. The EU and the US are both members of the OECD. In fact, the OECD Privacy Principles are similar to those included in Directive 95/46/EC and member states' data protection legislations. Therefore, the OECD is a key organisation for the establishment of adequate data protection safeguards for EU-US data transfers in the field of law enforcement.

The US became a formal participant of the Asia-Pacific Economic Cooperation's APEC Cross-Border Privacy Rules (CBPR) framework on 25 July 2012. This framework creates privacy obligations for all APEC economies. With regard to the EU, it is not a formal member but the Art. 29 WP has produced a common referential[815] for the requirements of the CBPR system and the EU Binding Corporate Rules.[816] Therefore, this framework could also serve as the basis to get the two legal frameworks closer. However, the main problem with the APEC and the OECD privacy rules is that they constitute non-binding instruments. Consequently, the US has not always implemented the principles enshrined in the OECD Guidelines and the APEC Privacy Framework accurately. For instance, rules on data quality or purpose limitation (both

[815] Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents. See also WP 212, 24.02.2014.
[816] It is examined in Chapter 5 of this thesis.

well-defined by the conventions) have not been transposed in the US legislation.[817]

The US and the EU are also both subject to the Fair Information Practice Principles (FIPPs), released in 1973. These are core elements for all privacy laws around the world. In particular, they include principles such as transparency, individual participation, purpose limitation, data security, data usage, data access, auditing and accountability and redress. FIPPs were first embedded in the US Privacy Act of 1974, and they influenced later rules such as the aforementioned 1980 OECD privacy guidelines and Directive 95/46/EC. The FIPPs were created with the aim of harmonising privacy legislation applicable to any international data flow. Yet, as Wolf and Maxwell have pointed out, '[h]istorically, the EU and United States have taken divergent approaches to implementing the FIPPs'.[818] Similarly, De Busser concluded that the FIPPs have not been sufficient to make EU and US data protection systems fully compatible.[819] For data transfers in the field of law enforcement these principles have not been very helpful in approximating EU-US rules either. The US has often stated that all EU-US data-sharing agreements have been adopted in line with the FIPPs,[820] but these principles are so broad that they have not prevented different privacy provisions from existing in each of the current EU-US data-sharing agreements (see section 3.2 above).

The Council of Europe (CoE) Cybercrime Convention was signed by the US and all EU member states on 23 November 2001. It sets out a legal framework for police and judicial access to computer data. Among the safeguards guaranteed in the convention, there is the need for independent supervision (Article 15), and the use of mutual assistance requests in the absence of applicable international agreements (Article 27). Therefore, to some extent, the CoE Cybercrime Convention could provide a secure and effective EU-US framework for ensuring that electronic data is available to law enforcement authorities when needed for the investigation and prosecution of crimes. However, the scope of this convention is very specific, so it does not offer a complete data protection regime for the parties.

---

[817] De Busser 2009, p. 305.
[818] Wolf C & Maxwell W 2012, 'So close, yet so far apart: The EU and U.S. visions of a new privacy framework', *Antitrust,* vol. 26, no. 3, p. 8.
[819] De Busser 2009, p. 297.
[820] As regards the EU-US PNR Agreement, see the subcommittee Hearing: Intelligence Sharing and Terrorist Travel: How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel, 05.11.2011. Available from http://homeland.house.gov [23 November 2014]

Besides these multilateral instruments signed by the EU and the US, there are bilateral initiatives too. Two groups have been created with the purpose of bringing the two legal frameworks closer: the EU-US High Level Contact Group (HLCG) and the EU-US working group of data protection and privacy. The HLCG was established in 2006. It is composed of senior officers of both the EU[821] and the US[822] sides, who are in charge of discussing the exchange of data between both parties in the field of law enforcement. In the words of the Council of the EU:

'[T]he goal of the HLCG was to explore ways that would enable the EU and the US to work more closely and efficiently together in the exchange of law enforcement information while ensuring that the protection of personal data and privacy are guaranteed.'[823]

This group identifies common principles and definitions within the field of data processing for law enforcement. In particular, these are the purpose specification/purpose limitation; integrity/data quality; relevant and necessary/proportionality; information security; special categories of personal information (sensitive data); accountability; independent and effective oversight; individual access and rectification; transparency and notice; redress; automated individual decisions; and restrictions on onward transfers to third countries.[824]

The EU-US working group on data protection and privacy was set up in July 2013,[825] after the NSA scandal took place.[826] The goal was 'to establish the facts around U.S. surveillance programmes and their impact on personal data of EU citizens'.[827] On the one hand, it comprised members of the Commission, the Presidency of the Council of the EU, the European External Action Service, the EU Counter-Terrorism Co-ordinator, the Art. 29 WP and ten experts from EU member states. On the other hand, it involved the participation of the US Department of Justice, the US Office of the Director of

[821] They come from the European Commission and the EU Presidency (supported by the Council Secretariat).
[822] They come from the US Departments of Justice (DOJ), Homeland Security (DHS) and State (DOS).
[823] Council of the European Union, 9831/08, 28.05.2008.
[824] See Council of the European Union, 9831/08, 28.5.2008. On the principles, see also the Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection, 11.11.2008.
[825] European Commission, MEMO 13/1059, 27.11.2013.
[826] See chapter 4, section 3.
[827] European Commission, MEMO/13/1059, 23.11.2013, p. 8.

National Intelligence, the US State Department and the US Department of Homeland Security.[828] The Group organised three meetings in 2013[829] and issued an exhaustive report in which it clarified all the legal issues regarding the controversial Section 215 of Patriot Act and Section 207 of FISAA.[830] Yet, no new report has been published in 2014, and it is not fully clear what the input of this group is, apart from clarifying technical questions on the transatlantic exchanges of personal data.

Taking the above into account, we can conclude that none of the instruments seems to be sufficient for establishing a common data protection framework in the EU and the US, at least for the moment. It is precisely this need for a common regulatory system that triggered the negotiations for another legal instrument: the EU-US Data Protection Agreement, which is examined below.

### *3.3.3. Towards an umbrella EU-US Data Protection Agreement*

Parallel to the specific agreements on data transfers concluded between the EU and the US in the last ten years, many attempts have been made in order to reach a general framework on data protection.

The EP launched the first call for this Data Privacy and Protection Agreement (DPPA) in March 2009.[831] One year later, in May 2010, the Commission drafted a mandate on the negotiation terms,[832] which the Council authorised on 3 December 2010.[833] Negotiations officially commenced in March 2011.[834] Since then, several meetings have taken place between the Commission and the US authorities. Also, the DHS Chief Privacy Officer has participated in these discussions, giving valuable input on the current US privacy laws.[835] In November 2011, the EU and the US pledged in a

[828] European Commission, MEMO/13/1059, 23.11.2013, p. 9.
[829] One in Brussels on 22-23 July, one in Washington DC in 19-20 September and another in Brussels on 6 November.
[830] These provisions are examined in Chapter 4 Section 2. MEMO/13/1059, 23.11.2013, pp. 9-10; Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 27.11.2013.
[831] OJ C 117 E, 06.05.2010, pp. 198-206.
[832] European Commission, IP/10/609, 26.05.2010.
[833] Commission Press Release on http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1661.
[834] European Commission, MEMO/11/203, 29.03.2011.
[835] Homeland Security, Privacy Office 2013 Annual Report, 1.11.2013, p. 69.

joint statement to finalise negotiations on a comprehensive DPPA,[836] but as of February 2015 these are still ongoing.

The negotiations are advanced, and the EU and the US have already agreed on many provisions that the agreement will include.[837] First of all, the agreement will only cover data transfers between the EU and the US for the prevention, investigation, detection and prosecution of crimes. Moreover, it is now clear that the agreement will not be used as a specific legal basis for transatlantic exchanges, but rather will be a general mandate for particular data-sharing agreements. Thus, the current PNR and SWIFT agreements will have to conform to the provisions of the DPPA, but these might include stricter additional safeguards.

Regarding the substantive provisions of the agreement, the EU has moved forward to incorporate as many safeguards as possible. Although the US authorities were originally leading the negotiations on the content of the DPPA, the NSA revelations of 2013 brought a change of leadership. After the revelations, the US needed to rebuild trust within the EU and therefore, it gave greater consideration to the initial recommendations made by Commission.

The EU has achieved the inclusion of a provision on the need of prior consent of the original authority for onward transfers. Also, other stronger requirements will also be required if such onward transfer involves bulk data extracted from systems like PNR.[838] Other EU successes are the establishment of a non-discrimination clause between national and non-national data, the prohibition of basing decisions solely on the automatic processing of personal data (e.g. profiling systems), and provisions on data quality and integrity. Likewise, general provisions on access, modification and administrative redress will be available to any individual. Unfortunately, this might not be enough to stop the enormous delays that EU citizens encounter today when they request access to their PNR or SWIFT data.[839]

The US has also committed to establish oversight mechanisms similar to those conducted by DPAs within the EU. It is not clear what US supervisory authority will be in charge of the oversight, but it will probably be a combination of Chief Privacy

[836] European Commission, MEMO/11/842, 28.11.2012. The same idea was also recalled in European Commission, MEMO/12/192, 12.03.2012.
[837] The last document on the negotiations was leaked in April 2014, see Council of the European Union, 8761/14 RESTREINT UE/EU RESTRICTED, 09.04.2014.
[838] Council of the European Union, 8761/14 RESTREINT UE/EU RESTRICTED, 09.04.2014, p. 7.
[839] The author's own experiences in this regard are detailed in sections 3.2.1 and 3.2.2 of this chapter.

Officers, Inspector Generals and the Privacy and Civil Liberties Oversight Board.[840] The fact that a number of different supervisory authorities operate in the US could pose a problem. However, the US authority will need to be independent, in line with the EU DPAs characteristics. In addition, EU and US oversight authorities will cooperate and consult each other through national contact points.

For its part, the US has imposed its preferences in some of the provisions, especially in terms of data retention and data breach notification. As for data retention, the US has always resited setting specific data retention periods, suggesting that these should be decided in accordance to each party's domestic laws.[841] Therefore, the DPPA will not include specific periods of retention, but it will only state that data should not be kept 'for longer than necessary and appropriate'. The DPPA will also add that any specific data-sharing agreement will have to contain precise provisions on retention periods.[842] However, these retention periods will probably differ from one agreement to another, as is the case today with regard to the PNR and SWIFT agreements.

As for the provision on data breach notifications, the US has set some limits. A leaked document confirms that 'the incident would, *in principle,* be notified to both the provider of the data […] and […] the individual concerned'.[843] This ambiguity is the result of the US pressures that insisted on notifying only *serious* breaches. In contrast, the Commission was supporting the notification of data breaches in all cases, excluding certain exemptions.[844] In the end, there will be exceptions, but these will have to be exhaustively listed.

Three issues remain unresolved: i) the judicial redress – particularly the possibility for EU citizens to obtain redress in the US, ii) the purpose limitation principle, and iii) the processing of sensitive data. In addition, the US seems reluctant to transpose the HLCG's principle of *proportionality*[845] into the agreement, arguing that this term is undefined in the US laws and, therefore, it could cause uncertainty in the US.[846]

---

[840] Council of the European Union, 8761/14 RESTREINT UE/EU RESTRICTED, 09.04.2014, p. 14.
[841] European Commission, JUST/C3/MHB D(2011), 31.01.2012.
[842] Council of the European Union, 8761/14 RESTREINT UE/EU RESTRICTED, 09.04.2014, p. 6.
[843] Council of the European Union, 8761/14 RESTREINT UE/EU RESTRICTED, 09.04.2014, p. 9.
[844] European Commission, JUST/C3/MHB D(2011), 31.01.2012.
[845] About HLCG principles, see restricted document available from http://www.statewatch.org/news/2008/mar/eu-us-dp-principles.pdf [23 November 2014].
[846] European Commission, JUST/C3/MHB D(2011), 31.01.2012. For further information about the HLCG, see Callahan ME 2010, 'New international privacy principles for law enforcement and security", *The Privacy Advisor, The Official Newsletter of the International Association of Privacy Professionals (IAPP*), 1 January. Available from http://www.dhs.gov [23 November 2014].

As for the judicial redress, the Commission has been trying to enable EU citizens to obtain judicial redress in the US by establishing enforceable legal provisions in the agreement. The Commission has even requested that the US authorities amend the US Privacy Act of 1974 in order to include judicial redress for non-US citizens. However, the US Congress has been reluctant to do so. It has long maintained that EU citizens already have the possibility to use the US Freedom of Information Act (FOIA) to get judicial redress and, therefore, the amendment is unnecessary.[847] Yet, after the Snowden revelations,[848] the Attorney General of the US, Eric Holder, finally promised to take action in order to guarantee that Europeans who do not live in the US can also have judicial redress.[849] This is one of the issues that still need to be clarified for the future DPPA.

Another aspect to be noted is that the DPPA will not cover data transfers carried out by intelligence services (e.g. between the NSA and the British GCHQ). Hence, it seems that this future project is not as ambitious as it was initially presented to be, and it will only partially help to establish common minimal standards on data protection between the EU and US.

### *3.3.4. The norm-taking role of the EU*

Many studies have concluded that the US has shaped the EU's security policy.[850] This section will examine whether the EU has been a pure 'norm-taker'[851] of US counter-terrorism rules, or if it has also influenced the US in the negotiations of data-sharing agreements.

There is no doubt that, after the 9/11 attacks, the US strategy triggered the adoption of all the EU-US agreements described above. In 2001, the Bush administration called upon its allies (including the EU) to provide support and assistance to the US in order to combat terrorism. The US pushed the EU to change their national policies if necessary.

---

[847] Archick 2013, p. 16.
[848] It is examined in Chapter 4 of the present study.
[849] EU-U.S. Justice Ministerial in Athens: Vice-President Reding welcomes U.S. announcement on data protection umbrella agreement, European Commission - STATEMENT/14/208, 25.06.2014.
[850] Argomaniz 2009, pp. 119-121; de Hert P & Papakonstantinou V 2009, 'The PNR Agreement and transatlantic anti-terrorism co-operation: No firm human rights framework on either side of the Atlantic', *Common Market Law Review 46*, pp. 885-919; Hillebrand 2012, pp.127-128; and Trauner & Carrapiço 2012, p. 6; Quesada Gámez M & Mincheva E 2012, 'No data without protection? Re-thinking transatlantic information Exchange for law enforcement purposes after Lisbon' in *EU external relations law and policy in the post-Lisbon era*, ed. Cardwell PJ, Springer, Berlin, p. 292.
[851] The notions of 'norm-maker' and 'norm-taker' are used by Argomaniz 2009, p. 127.

The National Strategy for Combating Terrorism was clear on this point:

'When states prove reluctant or unwilling to meet their international obligations to deny support and sanctuary to terrorists, the United States, in cooperation with friends and allies, or if necessary, acting independently, will take appropriate steps to convince them to change their policies.'[852]

It has been confirmed by this study that when the EU adopted the SWIFT, PNR and CSI agreements, the negotiations were mainly led by the US needs. As for the PNR saga, the transfer of air passenger data to the US was not on the EU agenda as a counter-terrorism measure before the adoption of the first PNR agreement.[853] The US power over the EU legal framework was then seen in *Parliament v. Council*, ruled by the CJEU in 2006. The Court's reasoning on the applicable legal basis revealed the increasing influence of US counter-terrorism measures on the EU. The US has also shaped subsequent PNR agreements, softening their data protection provisions. In fact, the EU passed the agreements because it was afraid that a refusal would cause the removal of some member states from the VWP.[854]

With regard to the SWIFT agreement, this is another example of the EU becoming a 'norm-taker' of US interests, especially considering that the EP could not fulfil all its expectations regarding SWIFT II, after it rejected the first agreement.[855] SWIFT is up for renewal in 2015.[856] There is a possibility that the EU will propose some changes for the renewal, especially with regard to data protection, but for the moment it is mainly the US at the helm. Finally, the CSI was also established because the US wanted to have US officers at EU ports.

All these international agreements have brought changes to the EU's internal security policy. For instance, the future TFTS will mirror a similar US system,[857] and the EU PNR proposal resembles to a great extent the EU-US PNR agreement. In this sense, the preamble of the EU PNR proposal justifies its relevance by stating:

---

[852] 'The national strategy for combating terrorism', *Central Intelligence Agency*, 17.12.2003. Available from www.cia.gov [31 October 2014].
[853] Argomaniz 2009, p. 125.
[854] Suda 2013, p. 779.
[855] Kaunert, Léonard & MacKenzie 2012, pp.476, 487; Ripoll Servent & MacKenzie 2012, p. 73. However, de Goede argues that 'the resolution of the SWIFT affair tried to support and solidify the position of the EU as a global actor with normative appeal'. De Goede 2012, p. 216.
[856] Archick 2013, p. 9.
[857] Bigo et al. 2012, p. 5.

'On the basis of an exchange of information with…third countries, the EU has been able to assess the value of PNR data and to realise its potential for law enforcement purposes. The EU has further been able to learn from the experiences of such third countries in the use of PNR data.'[858]

The EU-US data-sharing agreements have also influenced international agreements between the EU and other third countries. Specially, PNR agreements between the EU and Australia or Canada show this tendency.

I will provide a brief outline of these two agreements. About the EU-Canada PNR Agreement, the Canadian government adopted a Customs Act requiring API and PNR data from all passengers arriving from outside the Canadian frontiers. As in the US, the Canada Border Services Agency (CBSA) threatened to fine all those airline companies that failed to comply with the mandate. However, the EU had a temporary derogation of such requirements since the EU law on data protection was seen as contrary to the Canadian measures. Hence, an EU agreement needed to be adopted. In 2005 the Commission launched a proposal for a Council decision on the conclusion of an agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API) and Passenger Name Record (PNR) data.[859] The proposed legislation had the purpose of preventing and combating terrorism and other serious crimes. Like the first EU-US PNR Agreement, it fell under the scope of the former Article 95 TEC. That international agreement was signed in 2006,[860] together with an adequacy decision.[861]

Nonetheless, at that time, the CJEU was reviewing the adequacy of the legal basis used for the EU-US PNR Agreement, so the EP adopted a legislative resolution[862] rejecting the Canadian proposal, as well as instructing the Council not to conclude the agreement until the CJEU had delivered a verdict on the pending judgment. As seen earlier, the CJEU finally annulled Council Decision 2004/496/EC and Commission Decision 2004/535/EC so, consequently, the proposed council decision on PNR between the Community and Canada was never adopted. The adequacy decision expired

[858] COM(2007) 654 final, 06.11.2007.
[859] COM(2005) 200 final, 19.05.2005.
[860] OJ L 82, 21.03.2006, pp. 15-19.
[861] OJ L 91, 29.03.2006, p. 49.
[862] OJ C 157 E, 06.07.2006, pp. 464-465.

in September 2009, and thus a new and permanent agreement was required by that time. In November 2010, the EP adopted a resolution encouraging the Commission to open new negotiations on behalf of the EU.[863] A new EU-Canada Agreement was signed on 26 June 2014,[864] but it is now awaiting the EP's consent.

Since the Lisbon Treaty, the EP can refer international agreements to the CJEU before voting if the institution has doubts on their legality. The EP has decided to make use of these new powers for the proposed EU-Canada PNR Agreement. Thus, using the arguments of the CJEU decision on the annulled Data Retention Directive, the EP has referred the proposal to the CJEU before it grants the approval.[865] According to the EP:

'[T]here is legal uncertainty as to whether the draft agreement is compatible with the provisions of the Treaties (Article 16) and the Charter of Fundamental Rights of the European Union (Articles 7, 8 and 52(1)) as regards the right of individuals to protection of personal data; questions, further, the choice of legal basis, i.e. Articles 82(1)(d) and 87(2)(a) TFEU (police and judicial cooperation) rather than Article 16 TFEU (data protection).'[866]

It remains to be seen whether the Court decides that the proposed EU-Canada PNR Agreement contradicts EU laws. If so, it could affect the validity of the current EU-US PNR Agreement as well as the EU-Australia PNR Agreement.

A few years after 9/11 the EU decided to sign a PNR agreement with Australia. It was concluded in June 2008 between the Australian Customs Service and the EU.[867] However, with the entry into force of the Treaty of Lisbon the EU found a need to amend that agreement. Negotiations for a new PNR agreement started on 2 December 2010 and, six months later, the Commission launched the proposal for the new EU-Australia PNR Agreement.[868] On 22 September 2011 the Council gave the agreement

[863] European Parliament, P7_TA-PROV(2010)0397, 11.11.2010.
[864] Council of the European Union, 'Signature of the EU-Canada Agreement on Passenger Name Records (PNR)', PRESSE 339, 26.06.2014.
[865] 'EU-Canada PNR scheme must have legality assessed by European Court', *EurActiv press release,* 25.11.2014. Available from http://pr.euractiv.com [25 November 2014].
[866] European Parliament, B8-0265/2014, 19.11.2014, p. 4.
[867] OJ L 213, 08.08.2008, p. 49.
[868] COM(2011) 281 final, 19.05.2011.

the green light[869] and it was successfully voted on by the EP on 27 October 2011. The EU-Australia PNR Agreement was adopted under the framework of the Treaty of Lisbon and, therefore, it required the EP's approval.[870]

The EU-Australia PNR Agreement clearly benefited from all the experience that the Commission had built up over many years during the negotiations of the EU-US PNR agreements. At the same time, the EU-Australia PNR Agreement[871] served as a reference for subsequent PNR agreements with the US (adopted in 2012) and Canada (still pending adoption). The three PNR agreements that the EU has with the US, Australia and Canada have several similarities. They have the same provisions on purpose, adequacy level, processing of sensitive data, data security measures, oversight, transparency, access and correction of individual data, judicial redress, decisions based on automated processing, retention of data (five years),[872] logging and documentation of data processing, transfers through the push method,[873] and the number of categories of collected data (nineteen).

However, it would be incorrect to say that all EU agreements for the exchange of data follow the US interests. It is today beyond a doubt that, like the US, the EU also has an enormous potential to influence third countries with respect to security policies. For example, in the SWIFT agreement, the EP promoted the elimination of bulk data transfers. Likewise, in the negotiations of the EU-US PNR agreement, the US originally sought to retain the data for fifty years.[874] Thanks to the EP this period was finally reduced to fifteen years. Similarly, the Parliament succeded in ensuring that the PNR transfers were carried out via the push method.

Moreover, the experience acquired by the Commission during the negotiations of the EU-US PNR agreements was of a great help for drafting other PNR agreements with third countries. The EU-Canada PNR Agreement is less intrusive than the EU-US PNR Agreement in terms of use of data (they will be used for offences punishable by at least four years in prison, versus the three years of imprisonment in the US agreement);

---

[869] Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, 10093/11, 13.09.2011

[870] OJ C 322, 05.11.2011.

[871] OJ L 186, 14.07.2012, pp. 4-16.

[872] Surprisingly, Australian Customs Service retains data for five and a half years, six months longer than the US and Canada.

[873] Canada applied a push method from the beginning, in its first PNR agreement in 2005; and even though Australia did not define it clearly in its first agreement of 2008, the push method is expressly stated in its current PNR agreement with the EU.

[874] Suda 2013, p. 780.

deletion of sensitive data (in Canada data has to be deleted after fifteen days, whereas in the US it is after thirty days), notification of the use of sensitive data (not existing in the US agreement), depersonalisation of data (after thirty days in Canada, and after six months in the US), disclosure of data (in Canada there is no onward transfer of data), and the frequency of transfers for a particular flight (there is no similar provision in the US agreement). Australia also applies these safeguards as for the scope of serious crime (the offences need to be of at least four years imprisonment) and the frequency of transfers.[875]

It can be thus concluded that, when security norms arrived from the US, the EU 'did not simply subordinate to the security rules that the United States unilaterally strengthened'.[876] The PNR schemes demonstrate that the EU has also contributed in establishing some limits to the US will. Recent improvements of data protection clauses are the result of years of negotiations and dialogue between the US authorities the EU institutions. These same data protection provisions are also found in the Australian and Canadian PNR agreements. Therefore, the EU also has an influence beyond the European borders on security issues, ensuring the compatibility if its international agreements with the EU data protection laws.

The number of PNR agreements concluded between the EU and third countries might increase in the coming years, including countries such as Japan, South Korea and the Kingdom of Saudi Arabia.[877] As Argomaniz points out, US norms in the field of counter-terrorism could easily become universal standards.[878] However, there is one issue in which the EU could contribute and export its model globally: the EU data protection framework. The Union has always been characterised for having strong data protection and privacy laws, which have had an impact on many third countries, including the US.

## 4. Concluding remarks

This analysis has demonstrated the increasing influence of the US authorities in shaping EU security measures consisting of transatlantic data exchanges. The EU emergence as

[875] Yet, Australia establishes stricter security measures than Canada and the US as regards the depersonalisation of PNR data, which is only conducted after three years, in contrast to the thirty days in Canada and six months in the US.
[876] Suda 2013, pp. 783-784.
[877] Hernanz N 2011, pp. 6-7.
[878] Argomaniz 2009, p. 132.

an international actor goes hand in hand with the US lead in the adoption of international agreements between the two within the counter-terrorism environment. In line with the argument of many scholars,[879] the EU's role as foreign and security policy actor appears to be quite weak in practice. This study has confirmed that the EU has often adopted the US's own approach in the trade-off between security and data protection.

Each of the current EU-US data-sharing agreements has different data protection provisions. They also differ from the sections dedicated to data transfers to third countries in the current FD 2008/977 and the EU Proposal for a Police and Criminal Justice Data Protection Directive. The lack of harmonisation among these laws complicates the future establishment of an umbrella EU-US data protection agreement, as well as global data protection standards in the field of law enforcement.

As for the question of whether the right to data protection is equally applicable when the data is only processed within the EU territory – rather than beyond the EU borders, the answer is partially negative. Although the general EU provisions of FD 2008/977 on international data transfers are very limited in scope, specific EU-US data-sharing agreements (and mainly, the PNR agreement) offer a complete data protection scheme for the exchange of information. The right to data protection is thus only weakened when the need for those data comes from beyond the EU territory and there is no specific international agreement in place. It has also been shown that, although the EU enjoys a specific legal basis on the right to data protection under Article 16 of the TFEU, the Treaty of Lisbon leaves the door open for the derogation of this provision if specific legislation is based on Article 39 TEU. This legal basis has never been used but it could eventually apply for CFSP measures.

Therefore, it can be concluded that external factors have played a fundamental role in the existing data protection legislation within the EU. The US, in particular, has exerted powerful external pressures in order to establish the right balance between security and data protection within the EU, even if it has entailed the weakening of the latter in certain circumstances. Following this same path, global data protection standards in the area of security might also come to be largely influenced by US needs in the future.

---

[879] Matlary JH 2009, 'European Union security dynamics. In the new national interest', *Palgrave Macmillan*, Basingstoke; Kaunert C & Zwolski K 2013, 'The EU as a global security actor: A comprenhensive analysis beyond CFSP and JHA', *Palgrave Studies in European Union Politics*, Basingstoke.

## Chapter 3: The role of Europol in the exchange of information within and beyond the EU

Within the EU Area of Freedom, Security and Justice (hereinafter, the AFSJ), Europol is the agency that stores the largest amount of information. Its scope covers any crime affecting a common interest within the EU, organised crime, terrorism and other forms of serious crimes involving two or more member states. As noted in the Stockholm Programme, Europol is a 'hub for information exchange between the law enforcement authorities of the Member States, a service provider and a platform for law enforcement services'.[880] Europol also processes information from non-EU countries, since third countries have been increasingly involving it in their criminal investigations.

The previous chapters have illustrated the challenges that the EU encounters in the exchange of crime-related information within and outside the European territory. After examining the main failures in the functioning of the EU data-sharing tools, this chapter will analyse whether the EU could enhance the use of Europol as a way to reduce the existing diversity of communication channels available for law enforcement authorities.

In addition, it will examine whether Europol's legal framework offers strong data protection rules that could inspire the future data protection legal framework at the international level. As concluded in the previous chapters, the EU cannot become a global regulator on data protection in the field of law enforcement without first achieving a coherent framework among its own member states. Neither member states nor the Commission have been capable of achieving that coherence so far, and the proposed Police and Criminal Justice Data Protection Directive does not seem to improve this situation either.

This chapter is divided into three parts. The first part will be an examination of whether Europol's data protection regime could be used as a reference for member states when processing data within the EU for law enforcement purposes. The second part of this chapter will look at the international actorness of Europol in the field of security. It will analyse to what extent Europol influences (and will continue to influence) third countries' data protection rules. I reserve the final section of this chapter for the analysis of the difficulties that currently exist with regard to the use of the agency's data protection and data security standards within and beyond the EU. In short,

[880] OJ C 115, 04.05.2010, p. 20.

this study will help conclude whether Europol's data protection system could be the solution for achieving an approximation of national data protection regimes for data transfers conducted within and beyond the EU borders.

## 1. The origins and aim of Europol

Europol was first regulated in the Treaty of Maastricht[881] as a way to contribute to a safer Europe.[882] It began functioning in 1994 as the Europol Drugs Unit (EDU), within the framework of TREVI III, which dealt with drug-trafficking and money-laundering cases. EDU had no competence to store personal data and the information collected could not be transferred to third countries or international bodies.[883]

Europol extended its competences in 1995, covering for the first time counter-terrorism investigations.[884] Rules governing that body were enclosed in the Europol Convention, which was ratified by all member states in 1999. From that moment, Europol became the European law enforcement organisation in charge of assisting 24/7 the competent authorities in member states and third countries for the prevention and combat of serious forms of crime. Yet, one of the main Europol's limitations is that its officers are not armed and they have no power to arrest. Europol is principally a hub of information, which interconnects national law enforcement activities within the EU, coordinates joint operations, and receives and distributes information.[885]

Since 9/11, several structural changes were implemented at Europol's headquarters. One of them was the establishment of a new unit, the so-called Counter-terrorism Task Force (CTTF), comprised of police agents and intelligence analysts from the member states. In 2003, the mandate of this unit was amended and taken over by the Serious Crime Unit.[886] The Commission encouraged member states to give enhanced operational competences to this unit.[887] However, even today numerous member states are reluctant to do this, so the unit maintains its original powers.

---

[881] The first legal basis for the establishment of Europol was Article K1(9) and K3 of the Maastricht Treaty.
[882] Council of the European Union, 10036/12, 24.05.2012, p. 13.
[883] Hillebrand 2012, p. 61.
[884] O'Neill 2012, pp. 71-72.
[885] *Data Protection at Europol*, Luxembourg: Publications Office of the European Union, 2010, p. 7.
[886] Bures & Ahern 2007, p. 199.
[887] 'European Commission Action Paper in Response to the Terrorist Attacks on Madrid', *European Commission*, MEMO/04/66, 18.03.2004, p. 8.

Europol's tasks have evolved since the moment the Europol Convention came into force. In fact, in Tampere (1999),[888] Hague (2004)[889] and Stockholm (2009)[890] the Commission suggested enhancing the role of Europol in cooperation with the member states and other EU bodies. The main amendment has been the replacement of the convention by a Council decision. The Europol Council Decision (hereinafter, ECD) was proposed by the Commission in late 2006[891] and finally adopted in April 2009.[892] It came into force in January 2010, when Europol became a full EU agency.

Today, Europol is the largest AFSJ agency. The list of crimes in which Europol can be involved is found in the annexes of the current ECD[893] and the proposed Europol Regulation.[894] The Treaty of Lisbon introduced significant changes with respect to Europol. First, the agency now has an explicit legal basis in Article 88 TFEU. This provision permits the amendment of Europol's laws without having to be ratified first by the twenty-eight member states. In fact, the existence or Article 88 has triggered a process to replace the current ECD with the above-mentioned Europol Regulation,[895] proposed by the Commission in 2013. Another important change since the Treaty of Lisbon is that Europol's activities are scrutinised by both the EP and the national parliaments. Moreover, Europol is now financed by the EU, and the agency is composed of EU staff.[896] All of these new issues bring the agency closer to the current EU institutions.

Europol is often involved in Joint Investigation Teams (JITs) to support member states in the preparation and coordination of criminal investigations. The JIT principle was first included in the Treaty of Amsterdam[897] and it was later reinforced after the 9/11 attacks.[898] Europol can participate in JITs under three conditions: a) the involvement must be expressly requested by a Member State; b) the JIT must include at least two member states; and c) the offence investigated must fall under the Europol's

[888] European Council. Tampere Conclusions, 15-16.10.1999.
[889] OJ C 53, 03.03.2005, pp. 1-14.
[890] OJ C 115, 04.05.2010, pp. 1-37.
[891] COM(2006) 817, 20.12.2006.
[892] OJ L 121, 15.05.2009, pp. 37-65.
[893] Annex of Council Decision of 6 April 2009 establishing the Europol Police Office, OJ L121, 15.5.2009, pp. 37-65.
[894] COM(2013) 173 final, 27.03.2013, Annex 1.
[895] Council of the European Union, Europol Work Programme 2012, 13516/11, 25.08.2012, pp.10.
[896] Boehm 2012b, p. 179.
[897] Ex Article 30(2)(a) TEU.
[898] OJ L 162, 20.06.2002, pp. 1-2.

mandate.[899] If these conditions are met, Europol can be part of an investigation team for a fixed period of time.

## 2. Europol's data exchanges within the EU

In addition Europol's general purpose of supporting and strengthening national law enforcement authorities' action in the prevention and combat of crimes,[900] Article 5 ECD lists a few other more specific tasks. One of these tasks is 'to collect, store, process, analyse and exchange information',[901] usually sent by member states. As a result, large amounts of personal data are currently stored in Europol's files. These are analysed by Europol officers and exchanged between its units, member states and even third parties.

Europol offers strong data protection and data security safeguards in the processing of data. In fact, the Joint Supervisory Body (JSB) has described Europol's data protection framework as one of the strongest in the world, because the agency has 'strict, tailor-made rules and efficient supervision arrangements'.[902] This section pays special attention to Europol's communication tool SIENA. It stands out for being a very secure system for data processing, and it also complies with the purpose limitation principle. Taking this as a premise, I scrutinise whether Europol's data protection regime could be used as a reference for member states. This analysis also includes a study of the proposed Europol Regulation too.

### 2.1. The increasing involvement of Europol in the data-sharing procedures within the EU

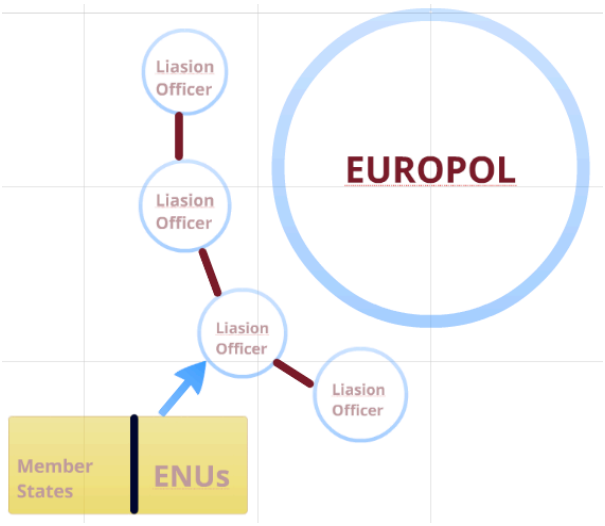
As noted above, Europol is currently the biggest AFSJ agency, covering any serious crime affecting two or more member states, or the EU itself. Europol provides a platform for the exchange of criminal intelligence and information,[903] processing a large

[899] de Buck B 2007, 'Joint Investigation Teams: The participation of Europol officials', *ERA Forum*, no. 8, p. 257.
[900] Article 3 ECD.
[901] Article 5(1)(a) ECD and Article 4(1)(a) of Europol Regulation.
[902] JSB Opinion 13/31 with respect to the proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol), 10.06.2013, p. 2.
[903] COM(2012) 735, 07.12.2012, p. 4.

amount of data every day. A considerable part of such data is first collected by national law enforcement authorities,[904] which follow the rules in the Council decision on the exchange of information and cooperation concerning terrorist offences.[905] This act sets out the conditions under which the information has to be sent to Europol.[906]

The common procedure for transferring information from a Member State to Europol is illustrated below.

*Figure 3.1.*




As perceived from Figure 3.1., the contact point between Europol and member states is usually through the so-called Europol National Units (ENUs),[907] although the proposed regulation allows establishing contact with any 'competent authority of a Member State'.[908] Thus, when it enters into force, Europol will be able to make direct contact with national law enforcement authorities without going through the national contact point.[909] By having direct contact with law enforcement authorities in the member states, Europol will also prevent clashing police operations among member states in cross-border investigations.

---

[904] Data might also come from another EU agency or EU information system, private entities, third countries and international organisations.
[905] OJ L 253, 29.09.2005, pp. 22-24.
[906] Article 2 of Council Decision 2005/671/JHA, and Europol, TE-SAT 2012, EU Terrorism Situation and Trend Report, p. 43.
[907] Article 8 ECD. See also Disley E, Irving B, Hughes W& Patruni B 2012, '*Evaluation of the implementation of the Europol Council Decision and of Europol's activities*', RandEurope, The Hague, p. 52.
[908] Article 7(5) of Europol Regulation.
[909] Recital 13 and Article 7(4) of Europol Regulation.

Each Member State has an ENU. They were introduced in 2010 with the adoption of the ECD. ENUs have access to the Europol Information System (EIS) when they need to search for information on individuals with factual indications or reasonable grounds to believe that they have committed (or will commit) criminal offences within the Europol's mandate. Before ENUs were established, such information was only accessible via Europol's liaison officers.

Although, as Chapter 1 of this thesis has shown, member states are free to choose the channel for exchanging information between them, ENUs are the only possible channel for exchanging information with Europol. ENUs are used in any case where Europol is involved, but they may also be used by member states to exchange information bilaterally for crimes outside Europol's mandate. ENUs can exchange information directly or through the so-called Europol Liaison Officers, who are part of an ENU but stationed at Europol's headquarters.[910] Each ENU seconds at least one liaison officer to Europol in the Europol Liaison Bureaux,[911] and there are currently a total of 160 liaison officers in The Hague.[912] They provide Europol with information of the particular member state 24/7, and they assist in the exchange of information. Regarding the data access that liaison officers have to the national law enforcement's databases, it varies from one country to another. For instance, in some member states such as Spain, liaison officers always need to contact the Spanish ENU in order to get access to Spanish police databases, whereas in Finland liaison officers have direct access to all Finnish databases.

Member states have no clear obligation to provide information to Europol under the ECD;[913] and the agency does not have, in principle, access to member states' national law enforcement databases. Member states are divided when it comes to transferring information to Europol for the prevention and investigation of crimes. Some of them are convinced of the added value of the agency and rely on the support that Europol can give to their own work.[914] They often request Europol's assistance during the investigation of a crime. Yet, other member states do not provide Europol with

[910] COM(2012) 735, 07.12.2012, pp. 5-6, and Article 8 of Europol Regulation. For an exhaustive study on Europol Liaison Officers, see den Boer & Block 2013.
[911] Articles 8 and 9 Council Decision 2009/371/JHA.
[912] Council of the European Union, 10426/14, 06.06.2014, p. 20.
[913] Disley et al. 2012, p. 47.
[914] Vermeulen & Wills 2011, p. 17.

sufficient information,[915] or they simply do not share information with Europol at all. This is mainly due to a lack of confidence and trust among such member states about the added value that the agency can provide.[916]

Law enforcement authorities of member states can decide not to involve Europol in a criminal investigation by using other communication channels such as the Swedish initiative[917] and Prüm decision.[918] As seen in Chapter 1 these are multilateral EU instruments for exchanging criminal information among member states. However, the use of the Swedish initiative and Prüm decision does not always exclude Europol. For instance, Europol is informed of a request made through Swedish initiative each time this falls within the agency's mandate.[919] Likewise, Europol officials can issue a request using the Swedish initiative, in accordance with Europol's laws.[920] In such a case, the channel used is either the liaison officers or the ENUs directly, and the information is transferred via SIENA. Also, specific handling codes in addition to the conditions established in the Swedish initiative have to be fulfilled for such requests.[921] After that, the information will be transmitted to the specific analysis work files (AWF), the Europol Information System, or the Europol Operational Centre.[922]

Europol also has a role in the use of Prüm decisions. In January 2012, Europol's Prüm Helpdesk and the Mobile Competence Team (MCT) were established. The purpose of both initiatives was to prepare a platform for experts, which would help member states implement and run Prüm systems.[923] The MCT, operational since 18 July 2011,[924] transferred all its activities to the Europol's Prüm Helpdesk in July 2013.[925] Hence, Europol is helping member states exchange DNA, fingerprint and vehicle registration data that might then be shared with the agency.

---

[915] Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, 31.05.2013, pp. 7-8.
[916] 'Europol: coordinating the fight against serious and organised crime. Report with evidence', House of Lords, European Union Committee, 29th Report of Session 2007-2008, HL Paper 183, p. 24; Bures O 2008, 'Europol's fledgling counterterrorism role', *Terrorism and Political Violence*, vol. 20 no. 4, p. 498.
[917] OJ L 386, 29.12.2006, pp. 89-100.
[918] OJ L 210, 06.08.2008, 1-11 and OJ L 210, 06.08.2008, pp. 12-72.
[919] Council of the European Union, 9512/1/10 REV 1, 17.12.2010, p. 8.
[920] Article 6(2) of Council Framework Decision 2006/960/JHA.
[921] Council of the European Union, 15278/11, 14.10.2011, p. 4.
[922] Council of the European Union, 9512/1/10 REV 1, 17.12.2010, p. 9.
[923] Council of the European Union, 10036/12, 24.05.2012, pp.31; COM(2012)732 final, 07.12.2012, p. 8.
[924] Council of the European Union, 17761/11, 05.12.2011, p. 3.
[925] COM(2012) 732 final, 07.12.2012, p. 8.

Likewise, Europol has access to data obtained through VIS,[926] SIS/SIS II,[927] CIS[928] and Eurodac.[929] This has raised concerns among numerous privacy experts, who have argued that it might undermine the EU fundamental principles of purpose limitation and non-discrimination.[930] However, in my view the main concern regards the national police authorities' data processing in the first place. Data processed by Europol goes through periodical auditing sessions, uses specific communication tools, and applies a common level of protection for all types of information. In contrast, national law enforcement authorities use diverse communication tools and standards when they exchange VIS, SIS, CIS and Eurodac data with each other. Therefore, member states could take Europol's infrastructures and systems as a model, as well as SIENA as default communication tool. This is examined in the next section.

## 2.2. The use of SIENA as default communication tool within the EU

### *2.2.1. Background*

Europol has its own communication tool, called the Secure Information Exchange Network (SIENA). It became operational in July 2009 and it is the backbone of Europol's infrastructure. It consists of a tailor-made messaging system, which carries no risk of interception due to its secure and user-friendly design.[931]

SIENA is not the first communication tool used by Europol. Before 2009, Europol used a system called Information Exchange System (InfoEx). It was established in 1996 under the Europol Convention. However, in November 2005, with the prospect of a forthcoming legislative amendment in Europol, the idea for replacing InfoEx with a new application was proposed. SIENA was first discussed during the first half of 2007, and after an exhaustive privacy assessment by the JSB, it was approved by the Europol Management Board in July 2007. The designing of the new-generation communication tool commenced in October 2007. It offered a range of innovative functionalities such as the availability of the tool to the users of ENUs, Liaison Officers and Europol staff.

[926] Article 7 of VIS Council Decision 2008/633/JHA, OJ L 218, 13.08.2008, pp. 129-136.
[927] Articles 41, 42 and 43 of SIS II Council Decision 2007/533/JHA, OJ L 205, 07.08.2007, pp. 63–84.
[928] Articles 11 (1) and 12 (1) of CIS Council Decision 2009/917, OJ L 323, 10.12.2009, pp. 20–30.
[929] Article 7 of Eurodac Regulation 603/2013, OJ L180, 29.06.2013, pp.1-30.
[930] See, for instance, Boehm 2012c, p. 342.
[931] Disley et al. 2012, p. 78.

It has been seen above that Europol usually contacts member states through ENUs.[932] ENUs use SIENA as the communication tool with Europol. Likewise, SIENA is used by: a) Member states' liaison officers, b) seconded national experts, c) Europol officials at Europol headquarters, d) some colleagues in other designated competent authorities besides ENUs, and e) some of the third parties with which Europol has concluded cooperation agreements.[933] On 1 July 2009 SIENA became technically available for all ENUs, but member states needed time for its implementation.

*2.2.2. SIENA phases*

SIENA has been evolving since July 2009. The first phase (SIENA v1.0, v1.1 and v1.2) was available until March 2010, at which time the second version of this tool (SIENA v2.0) was adopted. The new version introduced functionalities such as the extension to other designated authorities in member states, and the access for third parties that had operational agreements with Europol. By mid 2011, SIENA v2.1 enhanced the availability to third parties holding a strategic agreement with Europol.

SIENA v2.2 was operational for the period 2012-2013. It included new functionalities such as i) the integration with national systems;[934] ii) the capability to multitask; and iii) the establishment of EMPACT to set impact priority in the messages (e.g. messages referring to the Western Balkans).

SIENA v2.3 was implemented in the third quarter of 2013, and it introduced one major change: a Universal Message Format (UMF) Prüm form, through which a pdf form used for Prüm data exchanges was available within SIENA for member states. That provided a glimpse of the future link between Prüm and SIENA, enhancing its use in investigations in which Europol was not directly involved. That also solved the lack of a common communication channel following Prüm hits.[935]

SIENA v2.4 incorporated the UMF II format. That was the second phase of the EU-funded project led by Europol called the Universal Message Format. UMF is a structured data format in the SIENA messages that offers 'an additional service for those member states that wish to automate parts of the workflows of international law

[932] Article 8 ECD.
[933] Disley et al. 2012, p. 78.
[934] For the moment only Germany benefits from this functionality, being able to use its own national channel, the SIENA and Interpol channel all at once.
[935] Council of the European Union, 10303/14, 28.05.2014, p. 7.

enforcement cooperation'.[936] That phase of the UMF programme presented advantages in terms of cost savings, better use of resources, elimination of manual re-entry of data, and reduction of copying errors.[937]

In 2014, SIENA III was established. It enhanced interoperability between the national case management and the system by offering features such as faster searches and task assignment tools.[938] During 2015, the updated tool seeks to integrate the Europol Analysis System (EAS), convert the UMF to a human readable format, prepare the embedding of FIUs into SIENA, and explore the upgrade of the tool to carry confidential material, among other issues.[939]

Taking the above-mentioned into account, SIENA's evolution shows the clear intention of Europol to accommodate other EU channels like the Swedish initiative and Prüm in its own tailor-made communication tool. This tool brings national law enforcement authorities and Europol closer in the exchange of criminal information.

### *2.2.3. The scope of SIENA*

95% of Europol's information arrives through SIENA. It creates more than 38,000 SIENA messages per month.[940] The tool was originally developed for data exchanges between the agency and law enforcement agencies in the member states,[941] but a growing number of non-EU countries and third parties have been added to the system through the conclusion of cooperation agreements.[942]

Although in the majority of cases SIENA supports follow-up searches in the EIS, the tool can also be used for the exchange of information between member states outside Europol's mandate.[943] For instance, in 2012 member states used SIENA to exchange 222,000 messages;[944] but only in 53% of those was the information in the message shared with Europol.[945]

---

[936] Council of the European Union, Europol Work Programme 2012, 13516/11, 25.08.2012, p. 26.
[937] COM(2012) 735, 07.12.2012, p. 12.
[938] Council of the European Union, 6721/14, 20.02.2014, p. 2.
[939] Council of the European Union, Europol Work Programme 2015, 5250/15, 16.01.2015, p. 37.
[940] Council of the European Union, 10426/14, 06.06.2014, p. 13.
[941] European Commission, COM(2012) 735, 07.12.2012, pp.6.
[942] General Report on Europol's activities in 2011, Council of the European Union, 10036/12, 24.05.2012, pp. 20 and 23.
[943] Article 8(4) of Europol Regulation.
[944] In 2013, the number of SIENA messages rose up to 456,598. See Council of the European Union, 10426/14, 06.06.2014, p. 13.
[945] European Commission, COM(2012) 735, 07.12.2012, p. 6.

Europol, the Commission and the Council are now encouraging member states to use SIENA as the default system for exchanging crime-related information and intelligence.[946] In this sense, a Single Point of Contact (SPOC) will be established in every Member State, which will use all existing communication tools, including SIENA. An extended use of SIENA will not replace the use of other reliable channels for exchanging information among member states,[947] but it will integrate all of them into a single communication tool.

### *2.2.4. Advantages of using SIENA as EU default communication tool*

SIENA is mostly used for communications between law enforcement authorities and Europol, but it can also be extensively used for other data-processing systems in the future. In this sense, for instance, the Commission announced in January 2015 that the updated version of the EU PNR Directive will establish SIENA as the channel to exchange data among national Passenger Information Units (PIUs), and also with Europol.[948] In the same way, SIENA could be the tool for exchanging financial data according to the future TFTS, or even for exchanging data among intelligence services within the EU if they choose to use this tool.[949]

There are several advantages in using SIENA as the default communication tool by national law enforcement authorities. First, the system is in line with the privacy-by-design principle. As defined by the former EDPS Peter Hustinx, the principle of privacy-by-design means that 'controllers should be able to demonstrate that appropriate measures have been taken to ensure that privacy requirements have been met in the design of their systems'.[950] In fact, although this tool does not find any explicit legal basis in the ECD, the inclusion of the privacy-by-design principle and other data protection requirements have been present in SIENA since the very beginning. Throughout the different phases, SIENA has built a system that conforms to

---

[946] Council of the European Union, Europol Work Programme 2013, 17.07.2012, p. 24; COM(2012) 735, 07.12.2012, pp. 9; Council Conclusions 7-8 June 2012; Council of the European Union, 10303/14, 28.05.2014, pp. 2.
[947] Council of the European Union 9811/13, 24.05.2013, p. 7.
[948] European Commission, 'EU PNR – the way forward. Following the Orientation Debate of 21 January 2015 on the European Agenda on Security', p. 2. [Leaked on 28.01.2015].
[949] An exhaustive study of the intelligence services of the member states and their role at the EU level is conducted in Chapter 4 of this thesis.
[950] Hustinx P 2012, 'Ensuring stronger, more effective and more consistent protection of personal data in the EU', *NewEurope*, 2 February. Available from <http://www.neurope.eu> [5 December 2014].

Europol's data protection and data security standards. For example, it only allows authorised staff to access the tool; and it processes specific categories of data in accordance to the purpose limitation principle. When a new SIENA request is launched by one of the authorised actors (e.g. if the Spanish ENU contacts the French Liaison Office for a child pornography investigation), a number of data categories need to be filled in. It includes the cybercrime area, EMPACT, crime-related content, handling codes,[951] reliability (e.g. A1), priority (high, normal, low), and the deadline (e.g. 7 days).

Second, the increasing use of SIENA among member states reduces the processing of mass data (e.g. bulk passenger lists) as a preventive measure. In Europol, mass data is only retained in very specific cases, and for a short period of time. Moreover, names included in mass lists are only disclosed after a positive hit. In contrast, if member states use other communication tools such as regular email, there is no tracking of the amount of data processed, nor the period of time it will be stored in the particular server.

Third, SIENA is a multilingual interface, which permits operators at ENUs to communicate in their own national language.[952] This makes the system very efficient, since it does not require any translation of the messages, which might slow down a criminal investigation.

Notwithstanding the above-mentioned positive aspects, there would a few shortcomings if SIENA was established as the default communication tool within the EU. First, neither the current ECD nor the proposed Regulation[953] contains any mention of SIENA. This is a missed opportunity to regulate and enhance the use of the tool. Second, a problem encountered in the use of SIENA is that some member states might prefer other channels instead. Some Member States do not see sufficient added value in Europol's tasks and findings,[954] so they do not provide Europol with all the necessary information to fight serious cross-border crimes. These member states prefer to use other channels like Interpol, because it is more flexible and it includes the possibility for transferring judicial information (not only police information). Third, some member states have not fully implemented the SIENA data protection features,[955] and this

[951] There are currently three handling codes available with the following description: H1: Not to be used as evidence in a judicial procedure without permission; H2: No dissemination of the information without permission; and H3: any other restriction.
[952] Council of the European Union, 10303/14, 28.05.2014, p. 5.
[953] The ECD does not include any explicit provision of SIENA either. Even though it could have been included in the provision on AWFs, but this did not occur.
[954] SWD(2013) 99 final, 27.03.2013, pp. 2-3.
[955] See Joint Supervisory Body, Opinion 13/31, p. 4.

technical obstacle impedes their use of the tool. Fourth, SIENA only exchanges information classified up to EU Restricted. It excludes any information filed as Secret or Top Secret – which makes it less likely to be used by intelligence/ security services. In this sense, the Council has recommended increasing the SIENA confidentiality level in order to extend its use.[956] Lastly, another flaw of SIENA is that this tool offers a standardised channel to be utilised by all law enforcement agencies in the EU, but it excludes any information exchanged by intelligence services.

### 2.3. Europol's data protection regime

The compliance of SIENA with the privacy-by-design approach shows the significance that the right of data protection and privacy have for Europol. The agency claims to have one of the strongest data protection regimes in the world,[957] with higher standards than those found in the majority of member states. This section focuses on the examination of three main data protection safeguards in Europol: the compliance with the purpose limitation principle; the right of access, correction and deletion of data; and the external supervision by an independent body.

#### *2.3.1. Purpose limitation principle*

The current ECD processes personal data through two different systems: the Europol Information System (EIS) and the analysis work files (AWF). The former processes data introduced by member states – and Europol itself in the case of third country data – and it is used for cross-checking purposes. According to the last Europol General Report, information from nearly 71,000 people is held in the EIS.[958] The purpose limitation principle applies here, since the data processed belongs only and exclusively to either criminals or suspects of a criminal offence. The objective is to provide member states with relevant information for future investigations involving such criminals or suspects of a crime.

Regarding the AWFs, they have a completely different *raison d'être*. It is a system that provides information within a specific criminal investigation, and supports either

[956] Council of the European Union, 10303/14, 28.05.2014, p. 8.
[957] 'Data protection at Europol', Publications Office of the European Union, 2012, pp. 4 and 11.
[958] Council of the European Union, 10426/14, 06.06.2014, p. 17.

strategic analysis or operational cases. AWFs process information not only from criminals and suspects of a crime, but also from victims, witnesses and other relevant contacts. Yet, the AWFs are also structured in a way that it complies with the purpose limitation principle too.

There are currently two AWFs: the AWF for data on serious and organised crimes (SOC) and the AWF on counter-terrorism (CT) data. Each of these work files include different focal points or target groups separated by their crime area, as seen in the tables below.

*Table 3.1.*

| **AWF SOC** | | |
|---|---|---|
| FP[959] MTIC | FP SUSTRANS | FP MONITOR |
| FP CANNABIS | FP PHOENIX | FP TWINS |
| FP COPPER | FP TERMINAL | FP CYBORG |
| FP HEROIN | FP CHECK POINT | FP COPY |
| FP SMOKE | FP EEOC | FP GNST |

| **AWF CT** | | | | |
|---|---|---|---|---|
| FP HYDRA | FP DOLPHIN | FP TFTP | FP CHECK THE WEB | FP PIRACY |

Today there are twenty-five different focal points,[960] many of which include target groups. Each focal point stores different types of data complying with the purpose limitation principle. The annex of each focal point regulation, developed by the Europol analysts themselves, details what types of data can be processed. For instance, in the focal point HEROIN, dealing with investigations related to heroin dealers and heroin trafficking, any data concerning an alleged victim is hardly justified as necessary for such investigations. In the same way, any sensitive data relating to the sexual orientation of a drug dealer is also considered unnecessary and, therefore, not processed. In contrast, for the focal point TWINS, which deals with child pornography cases,

[959] Abbreviation for 'focal point'.
[960] Until 2011 there were twenty-three AWFs. Then they were reduced to two, and the concept of focal point and target groups was introduced. That new structure permitted an extended use of the Index Function, which is now able to search data among the different focal points in a common AWF.

information about victims or the sexual orientation of the offender might be relevant for the investigation and, hence, processed.

Europol analysts working in focal points tend to follow the list of categories of data that they normally need to process during an ongoing investigation. Moreover, regular audits conducted by the Europol DPO take place to supervise the adequacy of the data processed. One of the tasks of the DPO is drafting the audit plan for the coming year. It then scrutinises the selected focal point and verifies that the information processed is in line with the purpose limitation, proportionality and necessity principles.

Another mechanism – not foreseen in the legislation – which reinforces the compliance with the purpose limitation principle in both the EIS and the AWFs is the use of the so-called 'handling codes' for any information up to EU Restricted.[961] Every time a piece of information is sent by a Member State to Europol, an opening order is filled in, and the Member State has the competence to decide the restriction level applied for that particular information. This is possible through the handling codes. There are currently four handling codes available: a) The H0 or no-handling code, which permits the distribution to all member states as long as it is necessary for the purpose of preventing and combating crimes, b) H1, which prevents the information to be disclosed in judicial proceedings without the permission of the provider, c) H2, by which cross-matched information cannot be disseminated without the permission of the provider, and d) H3, which allows free text for other restrictions (e.g. only accessible for a specific target group).

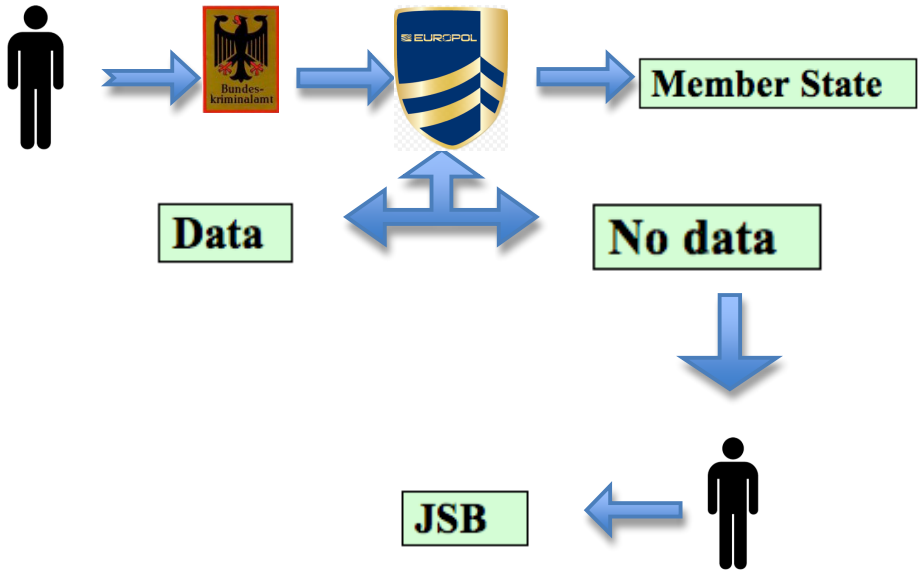
The Member State originally providing the information to Europol is also in charge of deciding the level of classification – public, restricted, secret, top secret. That Member State has discretion in making that decision, and Europol cannot modify it without prior consent from the country.[962] Data access by Europol officials will depend on the level of security: officials with higher data security clearance will gain access to more classified information than those with low or no clearance.

[961] There is currently a Europol initiative to allow handling codes up to Confidential.
[962] Abazi V 2013, 'Unveiling the power over Europol's secrets', *Amsterdam Centre for Law and Governance*, Working Paper Series 4, Amsterdam, p. 14

*2.3.2. Right of access, correction and deletion of data*

The right of access is established in Article 30 ECD. According to this provision, individuals who want to access data that Europol stores about them need to contact the competent national authorities, normally the national data protection authority (DPA) or a special police department. The procedure can be explained through the following hipotetical situation:

*Figure 3.2.*




A German man, whose name is Paul, wants to access data about him held on Europol's databases. First, he needs to issue the request to the Bundeskriminalamt in Germany. He will be required to send a copy of his ID or passport and a letter with the data request by post. The Bundeskriminalamt will then notify Europol of the particular query within one month.[963] The agency will check all systems and databases, and respond to Paul directly within the period of three months. If there is no hit, the agency sends a message to Paul explaining that there is no information held about him in the systems. If, on the contrary, there is a hit, Europol contacts the Member State that owns the information, which ultimately authorises the data disclosure. It might occur that there is an ongoing investigation in relation to Paul or that, by releasing it, national security is jeopardised. In such cases, the information is not revealed. Hence, Paul will

[963] Some individuals contact Europol through their solicitor instead. This is also possible as long as the individual has signed a letter authorising it.

only get access to his data if there is no objection by the country originally owning the data.

In case of a refusal, Paul can still appeal to the JSB, which will conduct an inspection at the Europol's premises, making sure that the request has been properly addressed.[964] It is worth noting that the responsibility is always from Europol, even if the agency has only followed orders from a Member State. If the JSB finds that Europol has failed to comply with the right of access, Paul may receive compensation for the damage.

Articles 31 and 32 ECD address the right to correct and delete information. The same procedure as in the right of access applies here. For instance, it could occur that Paul already knows that Europol has information about him, and has asked for the deletion of that information because it is not accurate. In this case, Europol will contact the Member State owning the information to determine whether it can be deleted. If the answer is positive, Europol will proceed to remove Paul's data from its databases. As in the right of access, the right to correct and delete information provide the possibility to appeal before the JSB. Yet, one of the problems detected is that, even once the information is corrected or removed from Europol databases, there is no efficient mechanism to certify that it has also been modified in the particular Member State.

### *2.3.3. Europol's oversight*

Europol has a model supervisory scheme composed of two bodies: the Europol Data Protection Officer (DPO)[965] and the Joint Supervisory Body (JSB).[966] Despite the existing complementarity between them, they play different roles in the protection of the data processed by Europol, as examined below.

The DPO is part of the agency's staff and, therefore, carries out an internal form of supervision, which according to Article 28 ECD is independent from the rest of Europol's activities.[967] The DPO has many mechanisms at its disposal to ensure that Europol complies with the data protection rules. In this sense, Article 28(4) ECD establishes that:

[964] The JSB publishes the decisions in its website: http://europoljsb.consilium.europa.eu/about.aspx [7 December 2014].
[965] Article 28 ECD and Article 10 of Council Decision 2009/936/JHA.
[966] Article 34 ECD.
[967] Disley et al. 2012, p. 5.

'If the Data Protection Officer considers that the provisions of this Decision concerning the processing of personal data have not been complied with, he or she shall inform the Director, requiring him or her to resolve the non-compliance within a specified time.'

However, the position of the DPO is at times a difficult one. Despite its formal independence, the office's funds come directly from Europol's budget. Therefore, the DPO has a dual role. One the one hand, it must ensure compliance of the agency, working hand in hand with the analysts responsible for the processing of personal data, and advising them on the spot (rather than ex-post). On the other hand, the DPO must offer loyalty to the agency.

Besides the DPO, Europol has another oversight mechanism via the Joint Supervisory Body. Although some scholars have criticised the JSB for its lack of objectivity,[968] this body is composed of representatives from national DPAs and is, therefore, completely independent from Europol. The JSB, operational since 1998, aims at reviewing that the processing of personal data from Europol to other parties is carried out according to the agency's data protection principles.[969]

The JSB carries out periodic inspections and external audits with the purpose of verifying whether Europol has properly implemented the data protection rules. It is not a judicial body, so it cannot impose sanctions in case Europol infringes a rule. However, its reports have always had a great political influence. In case of a violation, the JSB will require the Director of Europol to address the issue.[970] The JSB is also the only body entitled to decide whether a recommendation has been adequately fulfilled.[971], Furthermore, it submits periodical reports to the European Parliament (EP) and the Council,[972] and carries out appeal functions for data access requests.

[968] Especially when it approved the first Europol-US agreement. See Hillebrand 2012, p. 175.
[969] Disley et al. 2012, p. 96.
[970] Article 34(4) ECD.
[971] This could at times be an obstacle since Europol is not always capable of implementing the JSB recommendations, sometimes for budget reasons, sometimes for the lack of resources needed.
[972] Scherrer, Jeandesboz & Guittet 2011, p. 49. Unfortunately, JSB reports on data protection aspects are not public.

## 2.4. Main features in the proposed Europol regulation

On 27 March 2013 the Commission launched a proposal for a Europol regulation, which will replace the current Europol Council Decision.[973] One of the goals of the proposal is to increase the flow of information on crime to Europol.[974] Although this enhancement has raised concerns among member states and scholars, the proposal should be perceived as a positive development for the following reasons: first, Europol has gradually built a coordinated and efficient infrastructure which connects all member states in the prevention and investigation of crimes. Second, the agency offers high standards in terms of data security, mainly through the SIENA tool. Finally, Europol's data protection safeguards are robust and strong, and the guarantees it offers to individuals are often higher than those in the national legal frameworks. Yet, the proposed regulation also introduces some issues of debate, which will be addressed in this section.

### *2.4.1. Enhanced powers of Europol*

The Treaty of Lisbon has introduced significant changes with respect to Europol. The agency now has an explicit legal basis in Article 88 TFEU, whose first paragraph is also found in the proposed Europol regulation.[975] Two new main functions of Europol are: a) it coordinates investigations, and b) it has broader powers to retrieve and process information.

The coordination role was given to Europol in December 2009, with the entry into force of the Treaty of Lisbon. Article 88(2) TFEU states that Europol has competence to coordinate criminal investigations together with the member states. Keeping the same wording, the proposed Europol regulation establishes that Europol has the duty to 'coordinate, organise and implement investigative and operational action' in Article 4(1)(c). Yet, the regulation does not establish particular rules on how Europol and the member states should distribute their competences when they work together in an investigation.[976]

[973] European Commission, COM(2013) 173 final, 27.03.2013.
[974] Council of the European Union, 10213/13, 29.05.2013, p. 3.
[975] Moreover, Article 88 para. 2(b) TFEU is reproduced in Article 4 of the proposed regulation.
[976] Joint Supervisory Body, Opinion 13/31, p. 6.

The possibility for Europol to participate in joint investigative teams (JITs) is kept in Article 4(1)(d) and 5 of the proposed regulation, with a clearer wording than that found in the current ECD. JITs allow participants to access information stored in Europol's databases and, at the same time, Europol can obtain new information and add it in its systems. Another new feature is that there is no longer a need for prior arrangement if Europol wants to participate in JITs. This will facilitate the involvement of Europol in the investigations. In addition, Article 5(3) states that Europol will 'take measures to assist [Member States] in setting up the joint investigation team'. Althought this paragraph is somewhat symbolic, it enhances the role of Europol and is necessary for Europol in relation to the JITs.

Europol's coordination role is found in several other provisions of the proposal. For instance, Article 4(1)(g) permits Europol to 'develop, share and promote specialist knowledge of crime prevention methods, investigative procedures and technical and forensic methods, and to provide advice to Member States'. Likewise, Article 4(1)(h) allows Europol to provide technical and financial support to Member States; and Article 4(1)(l) empowers the agency to develop centres of specialised expertise for combating certain types of crime (e.g. the current EC3 or the office for counterfeiting). Article 6 on Europol's requests to initiate criminal investigations does not present many changes from the wording in the current ECD. The only new issue is the need to inform Eurojust in some cases (Articles 6(1) and (5)) and the one-month deadline for the member states to initiate the investigation (Article 6(4)).

The proposal also enhances Europol's access to crime-related information. It is particularly foreseen in Article 7 of the proposed regulation. Article 7(5) introduces an obligation for member states to provide the agency with information. Yet, the ownership remains with the member states, so it will ultimately have to authorise such data access.

Within this context, Article 23(3) of the proposed regulation states that 'Europol may retrieve and process information, including personal data, from information systems, of a national, Union or international nature'. Under the current legal framework, the agency can only access information that national authorities have introduced to Europol's databases.[977] However, the practice shows that several Europol Liaison Officers do have access to national police databases in their own countries, according to

[977] This is also foreseen in Article 7(5) of the proposed regulation.

their security clearance. Therefore, and despite the EDPS opposition to such provision,[978] it seems reasonable that the Commission adds a legal basis for this, underlining that it will be possible 'in so far as authorised by Union, international or national legal instruments'.

### *2.4.2. Data protection*

Although the JSB has argued that the draft regulation might result in a weaker Europol's data protection regime,[979] data protection rules will not necessarily lose strength under this new act. One of the amendments to be highlighted is that, for the first time, data protection rules are all in one single instrument. Following the previous structure, this section examines whether the new regulation will comply with the purpose limitation principle; the right of access, correction and deletion of data; and the external supervision by an independent body.

#### *a. The purpose limitation principle*

The proposal introduces a more flexible system for the processing of personal data, which does not require specific data systems as in the current Europol Council Decision. Data processing will depend on dataset levels. According to the explanatory memorandum on the proposal, the reason for this change is 'to better establish links between data already in its possession and subsequently analysing them'.[980] However, in line with the JSB argument, the reduction from 23 to 2 AWFs in May 2012 was created for this same purpose,[981] and therefore the Commission's argument is out of date.[982] Particularly, Article 24 (1) establishes that:

'Europol shall process data, including personal data only for the purposes of: a) cross-checking aimed at identifying connections between information, b) analyses of a strategic or thematic nature, c) operational analyses in specific cases.'

---

[978] Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, 31.05.2013, p. 24.
[979] Joint Supervisory Body, Opinion 13/31, p. 2.
[980] Explanatory Memorandum of the proposed regulation, p. 7.
[981] See also recital 20 of of the proposed regulation.
[982] Joint Supervisory Body, Opinion 13/31, p. 8.

From Article 24 it is deduced that the new data processing structure will consist of a single depository with different data set levels of processing. It will be only capable to store data for three specific purposes, namely, cross-checking, strategic analyses, and operational analyses. The first debate encountered on this issue is that it is hard to see how the future single 'Europol Information System' is going to function. The regulation does not include any indication on this issue other than stating that privacy-by-design will be introduced.[983] Considering that the current ECD also complies with the privacy-by-design principle, the only difference in the proposed regulation is that the system will no longer apply as a large-scale tool, but rather in a small-scale manner.

The Commission has justified the introduction of this new approach by stressing that the technical separation between the EIS and the AWFs is inefficient, since 'data must be stored at least twice (or three times) with duplicated obligations for the data owner as well as for Europol to maintain (update, delete) the data'.[984] For this reason, the Commission has decided that data protection rules in the future Europol regulation will no longer be 'database-oriented', but data protection safeguards will be rather attached to each piece and type of data.[985]

Although there is a significant chance that the current Europol systems are replaced by a single depository, the agency might maintain the existing structure in the future. In fact, oversight bodies such as the JSB and the EDPS have recognised the compliance of the existing AWFs and the EIS with the purpose limitation principle.[986] They have also expressed doubts about a future new structure, since Article 24 is presented in a very broad and ambiguous way, and it needs to be concretised.[987] Specifically, the JSB has highlighted its opposition to this more flexible IT structure, stressing that the purpose limitation and the necessity principles are already applied in the current ECD through the flexibility clause.[988]

The second debate refers to the scope of Article 24, which limits the data processing to purposes of cross-checking, strategic analyses, and operational analyses. In the current ECD there is a flexibility clause allowing the creation of new information systems other than those expressly foreseen in the law – however these must be

[983] Joint Supervisory Body, Opinion 13/31, p. 9.
[984] SWD(2013) 99 final, 27.03.2013, p. 3.
[985] SWD(2013) 99 final, 27.03.2013, p. 5.
[986] European Data Protection Supervisor, Opinion of 31.05.2013, p. 10.
[987] See European Data Protection Supervisor, Opinion of 31.05.2013, pp. 12-13.
[988] Joint Supervisory Body, Opinion 13/31, pp. 2-3.

authorised by the Management Board, the Director and the JSB.[989] The fact that this clause has never been used to date confirms that the current system is sufficiently flexible.[990]

A similar flexibility clause is not found in the proposed regulation. Many Europol officials argue that this limitation of purposes for data processing will be a step backwards for the agency, which seeks to enhance its competences and become more operational in the future.[991] For instance, under the future regulation, Europol will never be able to create a public portal for 'most wanted people' (similar to that found on the FBI website). Such a portal does not correspond to any of the three purposes listed in Article 24(1), so it would never be possible under the proposed regulation.

Therefore, the Council has suggested an amendment that would include a fourth purpose allowing Europol to process information for 'facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations'.[992] If accepted by the Commission and the EP, it would maintain the current existing possibilities under Article 10 ECD.

Article 25 refers to the purpose limitation principle too. This provision tackles the need for member states, EU bodies, third countries or international organisations to decide for what purpose the information is processed. If they fail to do so, Europol will take the decision. The EDPS has expressed its opposition to leaving the decision in the hands of Europol.[993] However, this is already occurring under the current system: information introduced mainly by member states arrives at the department O1 by default. Department O1 decides whether the information is relevant and, if so, it is distributed to the other departments (e.g. AWF FP TWINS). If not, the information is deleted from the pool within a period of six months.

*b. Right of access, correction and deletion of data*

Any individual whose data is stored in the Europol database has, as in the current ECD, the right to access,[994] correct, delete and block data,[995] the right to a judicial remedy,[996]

[989] Article 10(2) ECD.
[990] Joint Supervisory Body, Opinion 13/31, p. 9.
[991] Council of the European Union, 6517/10, 22.02.2010.
[992] Council of the European Union, 8596/14, 07.04.2014, Article 24(1d).
[993] European Data Protection Supervisor, Opinion of 31.05.2013, p. 25.
[994] Recital 37 and Article 39 of Europol Regulation. See particularly the possibility for the data subject to lodge a complaint to the EDPS in Article 39(6). Currently, Article 30 ECD.

and the right to compensation for damages or unlawful data processing.[997] The only difference from the current legal framework is that, in the proposed regulation, the appellate body will be the EDPS instead of the JSB.

For the rest, there are no changes on this issue. The only criticism on individual rights has been raised by the EDPS, which has suggested modifying the wording of Article 39 for a more plain language.[998] In my view, however, this provision does not present complexities as it is drafted. In fact, the practice shows that the data access procedure is working well at Europol. The DPO responds to all data requests in a clear and efficient manner, despite the high number of queries lately. In seven years the number of data requests received by Europol has increased from 10 to 600 hundred, but each of these requests has been properly examined on a case-by-case basis.

*c. External supervision of Europol's data processing*

Europol's supervisory body will be modified under the proposed regulation. According to the proposal, the supervision of Europol's data processing will be conducted by the EDPS,[999] replacing the current JSB. The main reason for this change is that Europol became a full EU agency in 2009. Before Lisbon, Europol was a third-pillar organisation subject to an intergovernmental convention ratified by all member states in 1998. Therefore, its activities were supervised by an independent body, the JSB, in accordance with the convention and within the scope of the former third pillar.

The EDPS is today in charge of supervising the EU institutions and bodies' compliance with data protection rules – including AFSJ agencies such as Frontex and the new eu-LISA.[1000] The only agencies that still have their own supervisory bodies are Europol and Eurojust. Therefore, the proposed Europol regulation (and also the

[995] Article 31 ECD, and recital 37 and Article 40 of Europol Regulation.
[996] Article 32 ECD, and recital 45 and Article 41 of Europol Regulation. The current ECD only allows the judicial redress for access, not for correction or deletion, see Boehm 2012, p. 198. In the proposed regulation any processing activity can be challenged to the EDPS and appealed to the CJEU. See Articles 49 and 50 of Europol Regulation.
[997] Article 52(1) ECD, and articles 51-52 of Europol Regulation.
[998] European Data Protection Supervisor, Opinion of 31.05.2013, p. 28.
[999] Recital 39 and Article 46 of Europol Regulation.
[1000] Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.01.2001, pp. 1-22.

proposed Eurojust regulation) will align the supervisory mechanisms of all agencies and bodies of the EU.[1001]

The EDPS has participated actively in the drafting of the proposal, and has expressed satisfaction with the new Article 46.[1002] On the contrary, the director of Europol and many powerful countries such as the UK, Germany and Sweden have stressed their discontent about the replacement of the current JSB with the EDPS. The JSB has also highlighted its objection to giving the EDPS the sole responsibility for Europol's supervision. Instead, it suggests creating an independent structure with equal participation of each national DPA, the EDPS and the Europol DPO.[1003]

The EDPS's supervisory role will consist of carrying out prior checks,[1004] consultations, complaint handling,[1005] visits, and inspections.[1006] In addition, the body will authorise automated processing of sensitive personal data,[1007] investigate complaints lodged by data subjects,[1008] and carry out 'joint supervisions' with national supervisory authorities in some cases.[1009] Finally, the EDPS will be informed if Europol stores data for more than five years.[1010]

The EDPS will have powers to rectify, block, erase, or destroy data; to refer a matter to the CJEU, and even to impose temporary or definitive bans for data processing.[1011] This last new power has been received with criticism among member states and Europol, and, therefore, the body has clarified that it will be, in any circumstance, a very exceptional remedy.[1012] Articles 47 and 49(2) of the proposal refer to the national authorities' cooperation with the EDPS. These provisions are particularly relevant considering the EDPS's lack of experience in auditing and inspecting Europol. The fact that the legislator has foreseen the possibility for national experts (for instance, the

[1001] The EDPS today supervises more than sixty institutions and bodies.
[1002] European Data Protection Supervisor, Opinion of 31.05.2013, p. 2.
[1003] Joint Supervisory Body, Opinion 13/31, pp. 3 and 10.
[1004] Article 42 of Europol Regulation. The EDPS has issued more than 600 opinions on prior checks to date.
[1005] The EDPS has received more than 650 complaints to date.
[1006] European Data Protection Supervisor, Opinion of 31.05.2013, p. 15.
[1007] Preamble of Europol Regulation, p. 8.
[1008] Recital 44 of Europol Regulation.
[1009] Preamble of Europol Regulation, p. 9.
[1010] Article 37(3) of Europol Regulation.
[1011] Article 46(3)(f) of Europol Regulation.
[1012] European Data Protection Supervisor, Opinion of 31.05.2013, p. 16.

current JSB members) to participate in these EDPS audits is thus seen as a positive development.[1013]

The proposed regulation also gives the EP stronger supervisory powers.[1014] This new role has its origins in Article 88(2) TFEU and Article 218(6) TFEU. Since the Treaty of Lisbon, the EP has been co-legislator in the AFSJ, which means that the EP plays an important role in 'ensuring that these agencies fulfil their mandates effectively'.[1015] Since the current ECD was adopted before the Treaty of Lisbon, these new EP compentences are not regulated.[1016] Therefore, Europol's draft regulation incorporates several provisions promoting the cooperation between the EP competencesand the national parliaments (NPs) in the scrutiny of Europol.

Under the current ECD, the EP only controls Europol's policies, administration and financial aspects.[1017] These competences are enlarged in the future Europol regulation.[1018] The proposal adds the following new tasks for the EP: a) the Management Board will have to consult the EP (and the national parliaments) on the annual programme,[1019] b) the EP (and the national parliaments) will receive strategic analysis, non-confidential threats, situation studies and evaluations, and working arrangements from Europol,[1020] c) the EP will be able to make requests for classified and sensitive non-classified information,[1021] d) the EP will receive all activity reports from Europol, e) the Director of Europol will send reports to the EP,[1022] and f) the EP will appoint the Europol's Executive Director.[1023]

It is yet unclear how the EP will actually adapt its infrastructures according to these new tasks. Some scholars state that the EP will create an oversight sub-committee of LIBE called 'Parliamentary Scrutiny Unit, which will have access to privileged

---

[1013] However, the EDPS has suggested clarifying the provision and the specific scope of cooperation. See European Data Protection Supervisor, Opinion of 31.05.2013, p. 17. See also Letter from EDPS to Mr. Juan Fernando López Aguilar, PH/HH/mk C 2013-0879D(2013) 0430, 13.11.2013.
[1014] Articles 53-54 of Europol Regulation.
[1015] Vermeulen & Wills 2011, p. 19.
[1016] COM (2010) 776 final, 17.12.2010; Hillebrand C 2013, 'Guarding EU-wide counter-terrorism policing: The struggle for sound parliamentary scrutiny of Europol' in *European Security, Terrorism and Intelligence. Tackling New Security Challenges in Europe*, eds. Kaunert C & Léonard S, Palgrave Macmillan, pp. 96-124.
[1017] Preamble of Europol Regulation, p. 6.
[1018] Article 62(2) and 53(1) of Europol Regulation.
[1019] Article 15(4) of Europol Regulation.
[1020] Article 53(3) of Europol Regulation.
[1021] Article 54 of Europol Regulation. It is expected that both institutions will conclude a working arrangement on that issue in the future. See Preamble Europol Regulation, p. 6.
[1022] The Council has suggested that the appearance of the Executive Director before the EP will only be to discuss non-operational matters. See Council of the European Union, 8596/14, 07.04.2014, Article 53(1).
[1023] Article 56(2) of Europol Regulation.

information.[1024] However, as Abazi points out, it might clash with the principle of originator control.[1025] According to this principle, member states originally sharing confidential information with Europol will retain the powers to decide whether the information can be accessed by the EP or not. Therefore, the new EP scrutiny competence might be *de facto* limited.

Finally, when the proposed regulation enters into force, the agency will fall under the CJEU's full jurisdiction. It conforms to Protocol 36 attached to the Treaty of Lisbon. Article 10(2) of that protocol specifically states that the amendment of an act adopted before the treaty will entail the applicability of new powers by the Commission – which will have competence to launch an infringement procedure – and the CJEU.

### 2.5. Comparison with data protection standards in the member states

After examining the data protection rules in the current ECD and the future Europol regulation, this section compares Europol's provisions with data protection rules in some Member States. The particular member states chosen for this study are Bulgaria, Finland, Greece, Poland, and Spain.[1026]

*Table 3.2.*

| | **Communication channel** | **Purpose limitation principle** | **Retention period** | **Independent oversight body** | **Audits** | **Right of access, modification, deletion** |
|---|---|---|---|---|---|---|
| Europol | SIENA | Yes | -As long as necessary<br>-Reviews after 3years | -Europol DPO<br>-JSB | Yes | Yes |
| Bulgaria | -Email<br>-Special encrypted channel | Yes | As long as necessary | No | Yes, annually | No |
| Finland | -Email<br>-Telephone<br>-Fax<br>-Intelligence blogs<br>-SIENA | No | It depends on the seriousness of the crime. Automated deletion | -National Police Board<br>-Parliamentary ombudsman | Yes, annually | Yes, once a year free of charge |

[1024] Vermeulen and Wills 2011; Abazi V 2014, 'The future of Europol's parliamentary oversight: A great leap forward?', *German Law Journal*, vol. 15 no. 6, p. 1132.
[1025] Abazi 2014.
[1026] This choice is based on the interviews that the author conducted during 2013 and 2014 with several police officers of these member states.

| | | | | | | |
|---|---|---|---|---|---|---|
| Greece | -Closed secure network<br>-Hard copies of documents<br>-Telephone | No | Unlimited | No | Unknown | Unknown |
| Poland | -Email<br>-Fax<br>-Cryptofax<br>-Special mail for secret information<br>-SIENA/Interpol/ Sirene channels | Yes | -As long as necessary<br>-10 years for intelligence | Data protection department | Yes, annually | Yes |
| Spain | -Sistema de información policial (SIP)<br>-Radio conference<br>-Telephone<br>-SIENA/Interpol/ Sirene | No | As long as necessary | No | Yes, every two years | Yes |

As shown in Table 3.2., law enforcement authorities of the member states often use regular email or the telephone to communicate with each other during a criminal investigation. Some departments also have encrypted channels of communication, but not all of them. The problem with not having secured communication tools is that crime-related data can easily be intercepted or accessed by third persons.

One of the data protection principles ensured by Europol is the purpose limitation principle. According to this rule, personal data collected and processed for one purpose may not be used later for other unrelated purposes. Law enforcement authorities in the member states do not always comply with the principle. In several countries, if a piece of data is introduced in the database, it remains in the system for 'as long as necessary'. Normally, police officers have different levels of clearance. Officers with high levels of clearance are able to access any data in the system relevant to their investigation, and use them for any 'necessary' purpose within the scope of their duties.

Only two of the countries examined in this study have data protection departments in charge of overseeing that information stored in the law enforcement database is adequately processed. The majority of countries do not have independent bodies that control data processed by law enforcement authorities. Annual audits are conducted, but it is not always clear by whom and how police databases are scrutinised. An example of adequate data protection audits is found in Finland. Finnish law enforcement authorities are subject to annual audit plans that define the amount, targets and the themes. Audits are carried out by the National Police Board Audit Unit. This unit conducts a comprehensive inspection, which includes an in-depth examination of data protection

issues. Besides this, Finnish police offices have other type of audits, conducted by a specific police unit. Finally, the collection of intelligence is controlled by the Finnish parliamentary ombudsman.

Most of the member states offer citizens the possibility to access their personal data. However, the procedure is subject to broad limitations and it varies from one country to the other. In Spain, for instance, police officers have one month to respond from the moment they receive the request.[1027] Yet, according to the Spanish law, data controllers (police) can deny the access, modification and suppression of data if it jeopardises national security, the freedoms and rights of a third person, or any ongoing investigation.[1028]

For all said above it can be concluded that, in the processing of information, both the current ECD and the proposed Europol regulation offer higher data protection standards than the majority of safeguards applied within the member states. Therefore, in principle, the Europol data protection framework could be taken as a model for member states in the future.

### 3. Europol's data exchanges beyond the EU

It is well known that 9/11 set in motion the creation of a global security infrastructure. The goal was to create a global system that would connect law enforcement authorities in different countries for the prevention of similar terrorist attacks. At the EU level, measures on issues related to criminal law and external relations fell under the scope of the intergovernmental competence – former second and third pillars. Yet, due to the increasing number of cross-border crimes and the fear of global terrorism, EU institutions started to propose initiatives within the scope of the external dimension of the Justice and Home Affairs (JHA) pillar. In this regard, on 21 September 2001, the European Council expressed its determination to elevate Europol to 'an effective information and intelligence exchange medium'.[1029] One of the EU goals was to achieve a coherent external relations' framework between Europol and third parties, as part of the overall EU external action.[1030]

[1027] Article 15 LOPD, articles 27, 28 and 29 RLOPD.
[1028] Article 23 LOPD.
[1029] Bures & Ahern 2007, p. 196.
[1030] Council of the European Union, 14366/3/05, 30.11.2005; and Disley et al. 2012, p. 107.

Today, Europol is not only the EU agency dealing with the largest amount of information within the EU, but it also has an important role with respect to the exchange of data outside the European territory. The agency exchanges more than 20,000 messages a year with third parties, retrieving personal as well as non-personal data.[1031] Consequently, external activities of Europol have not only led to the strengthening of the internal security architecture within the EU member states, but they have also had an influence on the EU's external security decisions.[1032]

The impact of Europol on external matters tackles both the CFSP and the AFSJ. Regarding the CFSP, Europol exchanges information with military agents within the context of EU's civilian CSDP missions.[1033] On the external dimension of the AFSJ, Europol has numerous cooperation agreements with third countries. These cooperation agreements will be precisely the focus of this section. Europol's cooperation agreements are separated from the international agreements signed between the EU as a whole and third countries. Yet, Europol's agreements have often positioned the EU security policy as a reference for third countries, since such third countries had to implement Europol's data protection standards as a condition for the agreement. Because of this, I will examine whether Europol is becoming a normative actor within the area of the EU external relations.

This section will first look at the current legal instruments used by Europol for the exchange of data with third parties, focusing on Europol's cooperation agreements. After that, it will analyse the special relationship existing between Europol and the United States (US). These parties have two cooperation agreements, one supplementing the other, signed in 2001 and 2002 respectively. In addition, Europol has developed a relevant role in transfers of financial data taking place between the European company 'SWIFT' and the US Department of Homeland Security. Finally, the last part of the section will discuss the proposed Europol Regulation and the changes it introduces with regard to Europol's data transfers to third countries.

---

[1031] Submission by Europol, House of Lords, Select Committee on European Union. Call for Evidence. File no. 3100-174, 28.04.2008, section 6.1, pp. 20-21.
[1032] Mounier G 2009, 'Europol: A new player in the EU external policy field?', *Perspectives on European Politics and Society,* vol. 10, no. 4, pp. 593 and 597.
[1033] For instance, on the EU missions in the Western Balkans, see Europol, 'Europol experiences of cooperation in the Western Balkans', EDOC 416612, 01.09.2009.

### 3.1. Europol cooperation agreements with third parties

Europol is not only in charge of giving support to the member states in the prevention, combat or investigation of crimes, but it also has a legal personality to negotiate and conclude cooperation agreements with third parties as part of its external relations.[1034]

The Council of Ministers is the European institution in charge of laying down rules governing Europol's external relations. In line with Article 42 of the former Europol Convention, the Council adopted on 3 November 1998 an act on the rules governing Europol's external relations with third states and non-European Union related bodies.[1035] That act established the following main features: a) the possibility to incorporate liaison officers at Europol's headquarters,[1036] b) the opportunity to organise missions by Europol staff to the relevant third states or non-European Union related bodies,[1037] and c) the possibility to establish regular meetings between Europol and third parties.[1038]

The act also regulated the participation of the Council of Ministers during the negotiations and adoption of cooperation agreements.[1039] Particularly, the Council is first entitled to draft a list with the third states and international organisations accepted for starting negotiations with Europol.[1040] Then, the Council has to authorise Europol's Director to enter into negotiations with the specific third country.[1041] After the negotiations, which take around two years on average,[1042] the Council will also authorise the conclusion of the agreement. In that sense, current Article 23(2) ECD[1043] adds that cooperation agreements with third states may be concluded 'only after the approval by the Council […] and, as far as it concerns the exchange of personal data, obtained the opinion of the Joint Supervisory Body via the Management Board'.

---

[1034] Mounier 2009, p. 586.
[1035] OJ C 26/19, 30.01.1999, pp. 19-20.
[1036] Article 3 of Council Act of 3 November 1998 laying down rules governing Europol's external relations with third States and non-European Union related bodies.
[1037] Article 4 of Council Act of 3 November 1998 laying down rules governing Europol's external relations with third States and non-European Union related bodies. See also 'Plans emerge for the collection of personal data outside European borders to obtain 'comprehensive situational awareness and intelligence support', *Statewatch*, 30.10.2012. Available from www.statewatch.org [10 December 2014].
[1038] Article 5 of Council Act of 3 November 1998 laying down rules governing Europol's external relations with third States and non-European Union related bodies.
[1039] Article 2 of Council Act of 3 November 1998 laying down rules governing Europol's external relations with third States and non-European Union related bodies.
[1040] Article 23(2) and 26(2)(a) ECD.
[1041] This was first established by Council of 27 March 2000, OJ C106, 13.4.2000, pp. 1-2, but the list of third countries has been updated since then.
[1042] For instance, negotiations between Europol and Colombia took around two years. See also Mounier 2009, pp. 588-589.
[1043] OJ L 121, 15.05.2009, pp. 37-66. See also O'Neill 2012, pp. 172-173.

Europol cooperates externally with eighteen non-EU countries to date: Albania, Australia, Bosnia & Herzegovina, Canada, Colombia, Former Yugoslav Republic of Macedonia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Republic of Serbia, Russia, Switzerland, Turkey, Ukraine, and the United States of America.[1044] As will be examined below, some of these countries have concluded an operational agreement with Europol, whereas others have only a strategic agreement in force.

The agency has also concluded agreements with nine EU bodies and agencies, as well as with three international organisations, including Interpol. It is also worth mentioning that Europol hosts liaison officers from nine non-EU countries and organisations, which are Albania, Australia, Canada, Colombia, Iceland, Norway, Switzerland, Interpol and some United States' law enforcement agencies. Regarding the future cooperation agreements with Europol, negotiations have recently started in Brazil, Mexico, Georgia and the United Arab Emirates.[1045]

As for the exchange of information between Europol and a third party, the Council did not adopt specific rules on this issue until 2009, exactly one day before the Treaty of Lisbon entered into force. Particularly, Council Decision 2009/934/JHA establishes the implementing rules on Europol's exchange of personal data and non-personal data with third parties, including a list of third states and organisations with which Europol can conclude agreements.[1046]

Article 23(2) ECD states that 'such agreements may concern the exchange of operational, strategic or technical information, including personal data and classified information, if transmitted via a designated contact point'. There are thus two types of cooperation agreements that Europol can conclude with third countries and international organisations: i) strategic agreements, which do not exchange personal data,[1047] and ii) operational agreements, which do allow the transfer of personal data.[1048] For exceptional situations, the ECD establishes the possibility to share information with

[1044] Council of the European Union, 10036/12, 24.05.2012, p. 105
[1045] 'The spider's web: Europol goes global in the hunt for intelligence and analysis', *Statewatch*, 5.3.2013. Available from www.statewatch.org [10 December 2014].
[1046] OJ L 325, 11.12.2009, pp. 6-11.
[1047] Article 1(g) of Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information.
[1048] Article 1(h) of Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information.

third states without a cooperation agreement, in the terms of Articles 23(8) and (9) of the ECD.

### *3.1.1. Strategic agreements*

Europol currently has strategic agreements with the following third countries: Albania, Australia, Bosnia Herzegovina, Canada, Colombia, Iceland, Macedonia, Moldova, Montenegro, Norway, Serbia, Switzerland, Liechtenstein, the US, Turkey and Ukraine.[1049] A strategic agreement between Europol and a third state, as the name indicates, only allows the exchange of strategic and technical information. Strategic information includes, for instance, enforcement actions to suppress offences, trends in the methods used to commit them, and threat assessments. Similarly, technical information deals with any data about investigative procedures, crime intelligence analytical methods, and forensic police methods, to name a few.[1050] Any transmission of data related to an identified or identifiable person falls outside of the scope of these agreements.

Strategic agreements permit the designation of the National Bureau of Europol in the police directorate of the third country. This bureau acts as a national contact point and participates regularly in high-level meetings with Europol. It is also in charge of the majority of information exchanges between both parties. Interestingly, liaison officers of a third country can be appointed even if there is no operational agreement between Europol and the third country. For instance, this was the case of Colombia and Albania before 2013. Both countries had only strategic agreements with the agency but they had liaison officers at Europol's premises – yet, they did not process personal data.

Two other observations need to be made with regard to strategic agreements. First, these agreements normally include a provision prohibiting the onward transfer of the information shared to other third countries, unless there is prior consent by the providing party.[1051] Second, each contracting party will be responsible for the choice of

[1049] In addition, Europol has strategic agreements concluded with CEPOL, FRONTEX, ECB, EU, ECDC, UNODC, OLAF, ENISA, World Customs Organisation, European Monitoring Centre of Drugs and Drug Addiction. Information available from https://www.europol.europa.eu/content/page/external-cooperation-31 [5 December 2014].
[1050] Article 2 of the Agreement on Strategic Co-operation between Montenegro and the European Police Office.
[1051] Article 6(7) of the Agreement on Strategic Co-operation between Montenegro and the European Police Office.

the appropriate classification level of information as regards data security standards. In this sense, there is always a table of equivalences between the third country and Europol.

### *3.1.2. Operational agreements*

It is usual that a third country first signs a strategic agreement with Europol and, a few years later, it concludes the operational and strategic agreement. By doing that, the third country makes sure that it has enough time to build an adequate data protection framework before operational relations with Europol start. Europol has concluded operation agreements with Albania, Australia, Canada, Colombia, Iceland, Monaco, Norway, Serbia, Switzerland, the US, Macedonia and Liechtenstein to date.[1052] This type of agreements exchange information, including personal data, in the form of specialist knowledge, results of strategic analyses and crime prevention methods[1053] that can add value for investigations.[1054]

As in strategic agreements, operational agreements require the appointment of a national contact point in the third country. This contact point participates in high-level meetings with the agency, and ensures the exchange of information between both parties on a 24-hour basis.[1055] In addition, both parties agree on appointing one or more liaison officers,[1056] who will be located at the Europol's headquarters. Third countries and organisations with an operational agreement with Europol are also capable of accessing analysis work files (AWFs) and focal points.[1057] Therefore, these third countries are required to have adequate data protection standards before concluding an operational agreement with Europol.

---

[1052] Europol has also operational agreements with Interpol and Eurojust. Information available from https://www.europol.europa.eu/content/page/external-cooperation-31 [5 December 2014].
[1053] See Article 4 of Agreement on Operational and Strategic Cooperation between Australia and the European Police Office.
[1054] Mounier argues that only operational agreements 'have a real added value for investigations because the strategic agreement merely allows the exchange of threat assessments and analytical reports'. See Mounier 2009, p. 587.
[1055] Article 7(2) of Agreement on Operational and Strategic Cooperation between Australia and the European Police Office.
[1056] Article 14 of Agreement on Operational and Strategic Cooperation between Australia and the European Police Office.
[1057] Mounier 2009, p. 589.

In this sense, a provision extinguishing personal data transfers if the adequacy is no longer in place is included in these agreements.[1058] Clauses on accuracy and the purpose limitation principle integrate the agreements, too. When a third country sends information to Europol, it specifies its purpose and access restrictions. Europol will then check whether the data is necessary for Europol's tasks and, if not (or no decision is taken within six months), it will be deleted.[1059]

Data protection rules included in operational agreements are similar to those in strategic agreements. For instance, operational agreements establish limits on the information sent to third countries. Moreover, they include clauses on individual rights. Any person has the right to access information collected by the government of the third country and transferred to Europol, but the agency needs prior consent from the supplying party before the release.[1060] Regarding data security issues, third countries need to ensure that personal data received from Europol is protected through technical and organisational measures.[1061] Lastly, as in strategic agreements, the supplying party is in charge of choosing the classification level of such information.[1062]

Europol can also sign working arrangements on a particular focal point with those third countries that have operational agreements with the agency. In this regard, Article 14(8) ECD allows Europol, under certain conditions, to invite experts from third countries or international organisations to be associated with the activities of an analysis group. For instance, Switzerland and Australia have recently joined the focal point 'Check-the-web'. These countries already have operational agreements with Europol, so the level of data protection in these countries is adequate. Finally, third countries accessing a focal point need to provide analysis data that justifies the necessity of such access, and all members of the particular focal point have to agree unanimously on it.

[1058] See Article 7(8) of Agreement on Operational and Strategic Cooperation between Australia and the European Police Office.
[1059] Articles 8 and 9 of Agreement on Operational and Strategic Cooperation between Australia and the European Police Office.
[1060] Article 7(7) of Agreement on Operational and Strategic Cooperation between Australia and the European Police Office.
[1061] Articles 9(3) and 12 of Agreement on Operational and Strategic Cooperation between Australia and the European Police Office.
[1062] Article 13 of Agreement on Operational and Strategic Cooperation between Australia and the European Police Office.

*3.1.3. Data exchanges between Europol and private parties*

Europol can exchanges data with private companies too. However, the agency does not have agreements or other arrangements with private entities. Therefore, the general rule is that information exchanged between the agency and private companies needs to be transferred via Europol National Units (ENU), never directly.

If the private company is not established within the territory of a Member State, the third state's regime will apply. For instance, Europol often needs to contact the credit card company Visa, located in the US. When that occurs, Visa sends the requested data to Europol via the US competent authorities.[1063]

As mentioned above, if the third country has a cooperation agreement with Europol, information from the private organisation is transmitted to Europol via the contact point of that state. However, if there is no agreement between Europol and the home (third) country of the private company, Europol can process data only if the organisation is on a list approved by Europol's Management Board. In addition, a memorandum of understanding and an opinion of the Joint Supervisory Body (JSB) are required.[1064]

## 3.2. Europol's receipt of information from third parties without an agreement

Europol does not need to conclude a cooperation agreement with a third party if the agency only wants to receive information from that country. It is regulated in Article 10(4) ECD, and Articles 19 and 20 of Council Decision 2009/934/JHA.[1065] These provisions state that when Europol only seeks to receive information from a third parties, it can do it, even if there is not a cooperation agreement in place. The only condition is the flow of information has to be one-way only. If Europol does not only receive but also sends information to that third country, a cooperation agreement with that third country will be required.

This procedure permits Europol to receive information from any third country rapidly. It is an advantatge in comparison to the two years on average that it takes for the conclusion of a cooperation agreement with third countries.

[1063] Disley et al. 2012, p. 117.
[1064] Disley et al. 2012, p. 116.
[1065] OJ L 325, 11.12.2009, pp. 6-11.

The following requirements take place for every receipt of information: a) the assessment of the reliability of the source;[1066] b) the communication of any deleted or modified information to Europol;[1067] c) the communication of the receipt to the Europol's data protection officer (DPO), the Director and the JSB; and finally d) the deletion of any information that has been obtained in violation of human rights.

It is worth adding that Europol's receipt of information from a third partner without an agreement has to be addressed on a case-by-case basis. Therefore, if Europol receives regular information from a particular third partner, Europol will require the conclusion of an agreement with that partner.

### 3.3. Data protection rules for data transfers to third parties

One of the current debates regarding Europol's external relations refers to whether Europol data transfers to third countries comply with the same data protection standards as data transfers within the EU.[1068] This section will answer that question, and it will also examine Europol's influence on data protection laws of those third countries with which the agency has cooperation agreements in force.

Some scholars have raised doubts about the adequacy of data protection rules when Europol transfers data to third countries.[1069] Indeed, this is the impression given by Article 23 ECD. The provision regulates the relations of Europol with third states and bodies, but it does not include specific rules on data protection for Europol cooperation agreements.

Detailed rules on the transmission of personal data by Europol to third states and bodies are found in Council Decision 2009/934/JHA.[1070] It requires the establishment of an independent authority responsible for data protection matters in the third country (Article 5(4)); an agreement on confidentiality for transmitting classified information

[1066] Article 19 of Council Decision 2009/934/JHA.
[1067] Article 20 of Council Decision 2009/934/JHA.
[1068] Ruthig J 2008, 'Rechtliche Rahmenbedingungen der Tätigkeit von Europol – Bestandaufnahme Ausblick', *Alternativenentwurf Europol und europäischer Datenschutz*, eds. Wolter J, Schenke WR, Hilger H, Ruthig J & Zoller MA, C.F.Müller Wissenschaft, p. 112.
[1069] Gless S 2008, 'Zusammenarbeit von Europol mit Drittenstaaten und Drittenstellen', *Alternativenentwurf Europol und europäischer Datenschutz*, eds. Wolter J, Schenke WR, Hilger H, Ruthig J & Zoller MA, C.F. Müller Wissenschaft, p. 346; Kaunert C 2010, 'Europol and EU Counterterrorism: International security actorness in the external dimension', *Studies in Conflict & Terrorism*, no. 33, pp. 661-662; Boehm 2012a, p. 210.
[1070] It derogates Council Act of 12 March 1999, OJ C 88, 30.3.1999, pp. 1-3, amended in 2002 by OJ C 76, 27.03.2002, pp. 1-2.

(Article 6(2));[1071] the need for concrete provisions on the recipient of the data, the type of data to be transmitted and the purposes (Article 15); a limitation of transmission to the competent authorities (Article 17); and the obligation to include a clause for correcting and deleting data (Article 16). Besides it, any data exchange between Europol and a third country has to comply with the principles of the Organisation for Economic Co-operation and Development (OECD)[1072] and the Council of Europe (CoE).[1073]

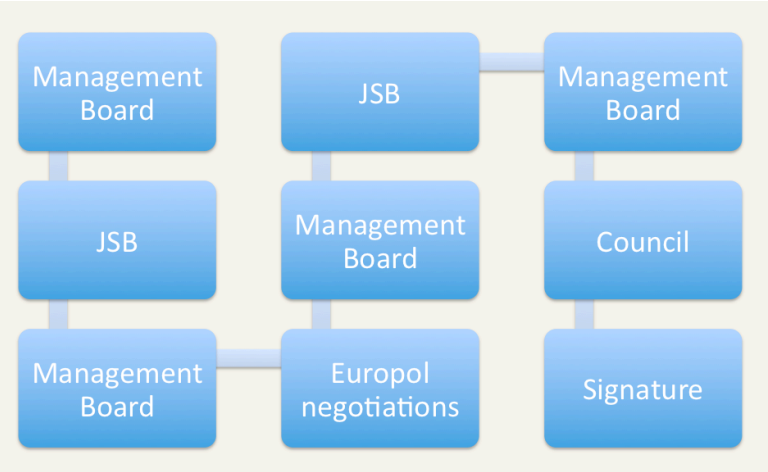
From Council Decision 2009/934/JHA it is inferred that Europol data transfers to third countries are only allowed when i) there is an adequacy decision on the level of data protection, b) there is an existing agreement between them or, c) exceptionally, to protect the fundamental interests of a country, or to avoid an imminent threat.[1074] Therefore, the general rule is that Europol's data transfers will not take place in countries without an adequate data protection regime.

As seen above, there are two types of cooperation agreements: strategic and operational. For operational agreements, an adequate level of data protection is required (unless it is a 'ticking bomb' situation).[1075] Europol has to examine the data protection regime in countries and organisations outside the EU before it concludes the operational agreement.[1076] In order to do so, the agency observes the nature of the data, the purpose for which the data is intended, the duration of the data processing, the general/specific data protection provisions, and other specific conditions.[1077] The steps to carry out this assessment are the following:

First, a data protection questionnaire is sent to the third country. If the Europol DPO is not convinced by the answers to the questionnaire, a data protection study visit is arranged. This is usually a one-week visit at the institutions of the third country that will carry out the data transfers, as well as the data protection authority (DPA) of the country. After that, the Europol's DPO drafts a report about the study visit.

[1071] This is also regulated in Article 23(7) ECD.
[1072] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23.09.1980.
[1073] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, 28.01.1981.
[1074] Ruthig 2008, p. 112.
[1075] Article 23(8) ECD. See also *Data Protection at Europol*, Luxembourg: Publications Office of the European Union, 2010, p. 23.
[1076] Disley et al. 2012, p. 112.
[1077] Article 23(9) ECD.

*Figure 3.2*




As illustrated in the table above, the study visit report is sent to the Management Board (MB), which forwards it to the JSB. Then, the JSB provides an opinion to the MB on the study visit report. The JSB opinion will allow the MB to adopt its own report. If the MB report is favourable, Europol enters into actual negotiations. Once the negotiations are finalised, Europol submits the resulting draft agreement to the MB. The draft is then forwarded to the JSB, which sends a second opinion to the MB. Finally, the MB forwards the draft, together with the JSB opinion, to the Council for approval.[1078] The conclusion of operational agreements can take years. Yet, Article 23(8) and (9) provides a possibility for derogation from the general provision. Although the derogation has only been used once to date, it allows Europol to exceptionally transmit personal data to third parties without an operational agreement in urgent or exceptional cases.

The general procedure for Europol to conclude operational agreements is similar to that for international data transfers originating in a Member State. According to Article 31(2) of Directive 95/46/EC, the proof that a third country has an adequate level of protection starts with a Commission proposal, and it is then followed by opinions from the Art. 29 WP and the Art. 31 Committee.[1079] After that, the EP can undertake a thirty-day scrutiny and, finally, a decision is taken by the Commission.

[1078] Disley et al. 2012, p. 113.
[1079] The Committee is established in Article 31 of Directive 95/46/EC and it is composed of representatives of every Member State who decide on matters like the adequacy decisions for third countries.

In the terms of this procedure, the impact of Europol's data protection framework on third countries and international organisations has been notorious. Europol has become a key actor for exporting the European model and, particularly, the EU data protection standards. The reason for that is that Europol's external strategy presents less political pressure than the overall EU external strategy, so it becomes easier to negotiate with third countries. As a result, Europol has developed a role as normative actor. Third countries have often changed their domestic laws, adapting them to the European standards, in order to gain access to the agency's data.[1080]

In conclusion, this section has demonstrated that Europol has been a norm exporter, influencing many third countries' data protection laws and principles. This influence has taken place during the Europol's visits to the country, through guidelines sent by the agency to the third country, or by organising internships and training sessions at the Europol headquarters.

### 3.4. Special relationship with the United States

The importance of a strong cooperation between the US and Europol is unquestionable. On several occasions Europol has participated in US operations that have resulted in the successful detention of criminals.[1081] This section will analyse the existing agreements between both parties, signed after the terrorist attacks that occurred on 11 September 2001. It will explore whether the US is also recognising Europol's actorness, and whether Europol's data protection rules have had an impact on the US legal framework.

#### *3.4.1. Cooperation agreements between the US and Europol*

Europol has concluded a strategic and a supplemental operational agreement with the US. After the 9/11 attacks, Europol decided to make use of the emergency clause to share information with the US without having any agreement in force.[1082] However, the

[1080] Mounier 2009, pp. 589-593.
[1081] See, for instance, the operation Joint Hammer, which included the involvement of USPIS, ICE and the FBI. Europol was in charge with the analysis of the seized material, and it was coordinated by the US Department of Justice. It was a success, resulting in 240 suspects identified, 61 child sex offenders arrested, and 11 child victims identified.
[1082] Current Articles 23(8) and (9) ECD.

abusive use of the clause was strongly criticised and, therefore, the agency decided to formalise a data-sharing agreement with the US.[1083]

The strategic agreement entered into force on 6 December 2001.[1084] It was negotiated with very little time due to the urgency of the matter.[1085] That agreement was not seen as controversial since it did not allow the exchange of personal data. However, one year later a supplemental agreement was concluded between Europol and the US for the exchange of personal data.[1086] On 16 October 2001, the former US President George W. Bush sent a letter to the ex-president of the Commission Romano Prodi requiring access to all of Europol's information, including information on individuals.[1087]

The supplemental agreement was concluded without first assessing the US level of data protection.[1088] Consequently, the provisions of the agreement do not correspond with the majority of operational agreements later adopted by Europol. For instance, in the US agreement the purpose limitation principle can be circumvented if there is prior consent from the providing part,[1089] and onward transmissions of information are also possible.[1090] Moreover, there is no clear time limit for the data retention period, and individuals have no right to correct or delete their data. The negotiations for this operational agreement were tense. They raised strong criticism because of the low data protection standards, as well as the exclusion of the EP, national parliaments and NGOs from the negotiations.[1091] Privacy experts feared that it could establish a precedent for other future cooperation agreements.[1092] However, as will be seen below, it did not become the model for subsequent agreements.

There are several liaison officers established between the agency and the US.[1093] Although the US removed its officials from the Europol headquarters at first, contact

---

[1083] Hillebrand 2012, p. 143.
[1084] Agreement between the United States of America and the European Police Office, 06.12.2001, File nº 3710-60r2.
[1085] On this issue, see Opinion 01/38 of the JSB in respect to the data protection level in the United States of America, 26.11.2001.
[1086] Supplemental Agreement between the Europol Police Office and the United States of America on the Exchange of Personal Data and related Information, 20.12.2002.
[1087] Letter available from http://www.statewatch.org/news/2001/nov/06Ausalet.htm [10 December 2014].
[1088] De Busser 2009, pp. 335; de Busser E 2010, 'EU data protection in transatlantic cooperation in criminal matters. Will the EU be serving its citizens an American meal?', *Utrecht Law Review*, vol. 6, no. 1, p. 96.
[1089] Article 5(1) of 2002 Europol-US Agreement.
[1090] Article 7(3) of 2002 Europol-US Agreement.
[1091] Hillebrand 2012, pp. 145 and 183.
[1092] Mounier 2009, p. 588.
[1093] Article 8 of 2001 Europol-US Agreement.

points were re-established in 2007.[1094] These come from the following US law enforcement agencies: Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Drug Enforcement Administration (DEA); Secret Service (USSS); Federal Bureau of Investigation (FBI); Immigration and Customs Enforcement (ICE); Internal Revenue Service (IRS); and US Postal Inspection Service (USPIS). In addition, Europol has two liaison officers seconded at Washington D.C. (and one at Interpol's headquarters in Lyon).[1095]

Therefore, Europol and the US authorities have been cooperating closely since 2001. They participate together in diverse joint projects,[1096] developing trainings and information sharing.[1097] SIENA is progressively becoming the tool of choice for exchanging operational information between both parties.[1098] In particular, the US has become a key partner for Europol on issues related to terrorist financing,[1099] as examined in the section below.

### *3.4.2. The role of Europol in the TFTP*

In June 2010 the EU and the US signed the second Terrorist Financing Tracking Program (hereinafter, TFTP) on the processing of financial data held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Europol has three main activities as regards the TFTP. The first is defined in Article 9 of the agreement and it consists of allowing the US Department of the Treasury 'to spontaneously provide to Europol […] the results of their processing of the data'.[1100] The second is established in Article 10 and it allows the agency to request searches of data obtained by the US authorities. The TFTP Unit (or O9), located at the Europol's premises, is in charge of

[1094] Hillebrand 2012, p. 120.
[1095] Council of the European Union, 10036/12, 24.05.2012, p. 19.
[1096] See, for instance, the joint project on countering violent extremism, where cooperate the EU member states, Europol and the US Department of Homeland Security (DHS). Council of the European Union, 10036/12, 24.05.2012, p. 111.
[1097] For example, in January 2013 Europol signed a letter of intent between U.S. Immigration and Customs Enforcement (ICE) and the agency in which the two agencies committed to developing ongoing, cooperative efforts through support, training, and information sharing on cybercrime, cyber fraud and online child sexual exploitation. Available from http://www.ice.gov/news/releases/1301/130111thehague.htm [10 December 2014].
[1098] This has been recently promoted by the Council. See Council of the European Union, 13516/11, 25.08.2012, p. 19.
[1099] Council of the European Union, 12667/12, 17.07.2012, p. 17.
[1100] Europol Activities in Relation to the TFTP Agreement Information Note to the European Parliament 1 August 2010 – 1 April 2011, File no. 2566-566, 08.04.2011, p. 2.

these two tasks. It is composed of three qualified staff members, and it has its own focal points to process data sent by the US.[1101]

The third and most controversial activity is described in Article 4 of the agreement. It regulates Europol's verification process and consists of reviewing that requests specify the categories of data, their time limits, the geographical scope, and the compliance with the necessity principle. Each request has fifty pages on average and, in most cases, they do not contain personal data.[1102] The verification process is carried out by the operational officer, the Legal Affairs Unit and the DPO.[1103] Only if Europol authorises it will the designated provider (*i.e.* the SWIFT company) have the green light to send the information, in an encrypted format, to the US Treasury Department. In this sense, the EDPS has complained that Europol is not a judiciary authority and therefore it should not be entitled to decide on the adequacy of the US requests.[1104]

Europol has no access to the amount of data transferred to the US. The agency can only verify the request by taking into account other documents provided by the US. In addition, TFTP documents kept at Europol HQ cannot be inspected by external supervisors like the European Ombudsman without prior consent of the US authorities.[1105] The role of Europol as supervisory body is, therefore, very limited. In this regard, Ripoll Servent and MacKenzie have questioned the neutrality of Europol in the verification process. They state that 'Europol will almost certainly be pressured to maintain good relations with the US in order to successfully obtain TFTP leads, compromising its effective review'.[1106] Even if it is certain, Europol must still apply data protection safeguards during the verification process, concretised in Articles 5, 6, 7, 8, 12, 15, and 16 of the agreement.

The TFTP agreement also includes data security provisions. For instance, the US requests under Article 4 are classified as 'SECRET UE/EU SECRET' due to their high operational sensitivity and, therefore, highly secured. The majority of data exchanged

---

[1101] Europol Activities in Relation to the TFTP Agreement Information Note to the European Parliament 1 August 2010 – 1 April 2011, File no. 2566-566, 08.04.2011, p. 5.
[1102] Except for in particular investigations, for instance some requests with general references to Osama Bin Laden.
[1103] Europol Activities in Relation to the TFTP Agreement Information Note to the European Parliament 1 August 2010 – 1 April 2011, File no. 2566-566, 08.04.2011, pp-4-5 and 7.
[1104] European Data Protection Supervisor Opinion on the proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II), 22.06.2010, pp. 5-6.
[1105] This has been critisised by the European Ombudsman. See Emily O'Reilly letter to the Chair of LIBE Committee, 27.02.2015, at http://www.statewatch.org/news/2015/mar/eu-ombuds-europol-letter.pdf
[1106] Ripoll Servent & MacKenzie 2011, p. 397.

between Europol and the US is channelled through the secure tool SIENA, which offers the possibility for additional future encryption measures.[1107] Unfortunately, a secure communication channel between Europol and the designated provider has yet to be established.

The JSB and the Commission oversee the implementation of the TFTP agreement in the EU.[1108] In 2011 and 2012 both bodies found that the US had to issue more specific requests under Article 4 TFTP, and that the information had to be provided in writing.[1109] The US implemented these recommendations successfully.[1110] In the US, the oversight comes from two EU independent supervisory authorities. They are in charge of checking that the information is processed according to the agreement. In order to do that, they can access data, review searches, and monitor the data protection rules, similarly to the role of the JSB within the EU.

The role of Europol in the TFTP agreement demonstrates that the agency can also take part in EU international agreements for the exchange of data with third countries. The role of Europol for the control of TFTP data requests is particularly relevant, since it could lead the agency to participate in other future international agreements. For all that, it must be concluded that Europol plays a key role in data exchanges between the EU and the US.

### 3.5. Data transfers to third partners in the proposed Europol Regulation

As mentioned earlier, on 27 March 2013 the Commission launched the proposal for a Europol regulation,[1111] which will repeal the current ECD. The proposed regulation includes new provisions on data transfers to third countries, the receipt of data from third countries, as well as the adoption and supervision of the cooperation agreements.

---

[1107] Europol Activities in Relation to the TFTP Agreement Information Note to the European Parliament 1 August 2010 – 1 April 2011, File no. 2566-566, 08.04.2011, pp. 6 and 13-14.

[1108] However, documents on the TFTP implementation are not always public, as can be seen in the recent case between Europol and the EU Ombudsman. See Decision of the European Ombudsman closing the inquiry into complaint 1148/2013/TN against the European Police Office (Europol), 02.09.2014.

[1109] See Report on the inspection of Europol's implementation of the TFTP Agreement, conducted in November 2010 by the Europol Joint Supervisory Body, Report nr. 11/07, 01.03.2011, pp. 5-6; and Europol JSB inspects for the second year the implementation of TFTP Agreement, Public Statement, 14.03.2012, p. 3.

[1110] Implementation of the TFTP Agreement: assessment of the follow-up of the JSB recommendations, Ref. 13/01, 18.03.2013.

[1111] European Commission, COM(2013) 173 final, 27.03.2013.

*3.5.1. Transfer of personal data to third countries*

Data transfers to third countries or international organisations are regulated in Chapter VI of the proposal. The general rule is that 'Europol may directly exchange all information, with the exception of personal data',[1112] unless it is expressly restricted in the sense of Article 25(2) of the proposal. In other words, transfers of personal data to third countries will be generally prohibited. Yet, in very exceptional cases and to the extent it is necessary for the accomplishment of its tasks, Europol will be able to transfer those personal data beyond the EU borders on a case-by-case basis.[1113]

In line with the current legal framework, Article 31 of the proposed regulation establishes three possible scenarios under which data can be exchanged between Europol and a third country. The first possibility is the existence of an adequacy decision,[1114] similar to that foreseen in Article 25 of Directive 95/46/EC for member states' transfers to third countries. It will require a proposal by the Commission, in conjunction with an EDPS study on the national data protection standards. The EDPS will apply the same procedure as that established in Article 9 of Regulation 45/2001 for EU institutions and bodies not subject to Directive 95/46/EC.[1115] The Art. 29 WP, which will be named European Data Protection Board, will also release an opinion on the agreement. After that, the EP will carry out a thirty-day scrutiny, which will result in a recommendation. Finally, the Commission will adopt the decision. The average time for this procedure will be one and a half years.

A second option that will enable Europol to transmit personal information to a third country is the adoption of an agreement between the agency and the particular country pursuant to Article 218 TFEU. As established by Article 31(1)(b) of the proposed regulation, the international agreement needs to include adequate data protection safeguards. The conclusion of the agreements between Europol and third parties will be in the hands of Europol, as it is today. In line with the procedure in other EU bodies, the Commission will be the institution in charge of the conclusion of the international agreements between Europol and a third country.

---

[1112] Article 29(2) of Europol Regulation.
[1113] Article 31 and recital 27-28 of Europol Regulation.
[1114] Article 31(1)(a) of Europol Regulation.
[1115] For a detailed analysis on the procedure, see 'The transfer of personal data to third countries and international organisations by EU institutions and bodies', European Data Protection Supervisor Position Paper, 14.07.2014.

The involvement of the Commission in Europol's activities is enhanced in the proposed regulation. Besides the new task of concluding international agreements, the presence of this institution at Europol's headquarters will be enhanced. Article 13 of the proposal includes the establishment of two members of the Commission in Europol's Management Board, which will be able to vote on Europol's future decisions. The Commission has already pointed out that it will still require the technical support of Europol on aspects relating to law enforcement, and that pre-existing international agreements will continue to be valid.[1116] It is, however, not fully clear how Europol will be involved in the procedure of Article 218 TFEU. In this regard, the JSB has argued that a legal basis for that should be included in the proposed regulation, ensuring that such additional tasks are in accordance with Europol objectives.[1117] Also, the EDPS has claimed that the new procedure should require an EDPS report during the negotiations of an international agreement between the EU and third countries or international organisations.[1118]

Finally, it will be possible to transfer personal data to a third country if it has a prior cooperation agreement with Europol.[1119] The EDPS has asked for a transitional clause for this option, so that such existing agreements will be reviewed and aligned with the proposal within a maximum period of two years from the adoption of the regulation.[1120] If this clause is finally introduced, the US-Europol agreements will probably be revised. As stated above, such agreements do not fully comply with adequate data protection standards. Since many current cooperation agreements already include a mechanism to amend the scope of application of the agreements according to Europol's new mandate,[1121] the revision of existing Europol agreements in the future is highly probable.

Notwithstanding the three possible ways for transferring personal data to a third country, there is a carve-out clause for emergency situations in the proposed Europol regulation.[1122] If the proposal is adopted, it will derogate Article 31 ECD, requiring no formal assessment of data protection safeguards, either for cases of one single transfer, or for transfers of a set of data. If it is a single transfer, the derogation will take place

[1116] COM(2013) 535 final, 17.07.2013, p. 6.
[1117] Joint Supervisory Body, Opinion 13/31, p. 8.
[1118] European Data Protection Supervisor, Opinion of 30.5.2013, p. 20.
[1119] Recital 29 and Article 31(1)(c) of Europol Regulation.
[1120] European Data Protection Supervisor, Opinion of 30.05.2013, p. 21.
[1121] See, for instance, Article 3(3) of the Agreement on Strategic Co-operation between Montenegro and the European Police Office, or Article 3(3) of the Agreement on Operational and Strategic Cooperation between Australia and the European Police Office.
[1122] Article 31(2) of Europol Regulation.

after Europol's Executive Director authorises such transfers on a case-by-case basis. The data transfer will be authorised if: a) it is absolutely necessary to safeguard the essential interests, b) it is absolutely necessary to prevent imminent danger, c) it is required on important public interest grounds, and d) it is necessary to protect the vital interests of the data subject.[1123] Yet, despite the derogation, the Executive Director will not abstain from examining the data protection standards of the third country, informing also the Management Board.

If instead of a single transfer a set of data is transferred to the third country for an emergency situation,[1124] the derogation can only apply for one year maximum, and it will require an additional authorisation from the MB and the EDPS.

In order to implement a cooperation agreement or an adequacy decision, Europol will be able to sign a working arrangement with the third country.[1125] As it is today, working arrangements need an existing agreement between Europol and the third country. However, the regulation fails to define in what cases a working arrangement will not be allowed. It is thus unclear in what specific situations the adoption of these arrangements will and will not be pertinent.

One of the new uses for these working arrangements will refer to the EP data access to the EU Classified Information and sensitive non-classified information processed by or through Europol.[1126] Another new task of the EP will consist in scrutinising the adoption of such working arrangements.[1127] The next section discerns future EP tasks relating to Europol's external relations.

### *3.5.2. The enhanced role of the European Parliament*

Before Lisbon, the EP had a limited role in the adoption of agreements between the EU and third countries. That institution was consulted but its recommendations were not binding. In that sense, neither the former Europol Convention nor the current ECD conferred decisive powers to the EP. Article 26 ECD states that the EP should be

[1123] The EDPS has argued that the terms 'essential interests' and 'important public interests grounds' are too vague, and he has suggested requiring at least 'that this public interest is recognised in Union law or in national law of a Member State of the European Union'. See European Data Protection Supervisor Opinion, 30.5.2013, pp.21.
[1124] The EDPS has proposed to replace the term 'transfer of sets of data' by 'occasional transfers'. See European Data Protection Supervisor, Opinion of 30.05.2013, pp. 22.
[1125] Article 31(1) of Europol Regulation
[1126] Preamble of Europol Regulation, p. 6.
[1127] Article 53(3)(b) of Europol Regulation.

consulted for the determination of the list of third countries with which the agency can conclude agreements.[1128] It is not a coincidence that both Council Decision 2009/934/JHA on Europol's data exchanges with third parties and the first SWIFT agreement were adopted exactly one day before the Treaty of Lisbon came into force. The reason was to avoid the participation of the EP in the decision-making processes.

Since the Treaty of Lisbon entered into force the EP is no longer a mere consultative body. This institution now has competence to participate in the decision-making process for the conclusion of international agreements. For instance, in October 2012, Europol's Management Board proposed that Mexico, Brazil, Georgia and the United Arab Emirates be added to the Council's list, and the Council amended the list accordingly.[1129] Negotiations for operational agreements started with Mexico and Brazil in 2013.[1130] However, the EP voted against these initiatives arguing that the proposals for these agreements did not conform to EU laws.[1131] The EP asked Europol's director and the Management Board to reconsider the proposal, and the negotiations were not started.

In addition to these new powers, when the proposed Europol regulation enter into force, the EP will have access to classified information[1132] processed by or through Europol. Especially interesting will be the EP role as regards the TFTP agreement. One of the past controversies regarding this agreement referred to Europol's refusal to send the TFTP inspection reports to the EP.[1133] The constant dispute on document secrecy between Europol and the EP[1134] led to a CJEU decision on 4 May 2012 in favour of the EP document requests.[1135] The Council argument that it would 'negatively impact on the European Union's negotiating position' did not convince the Court, which found that the Council had 'not established the risk of a threat to the public interest'.[1136]

---

[1128] Wesser, Marin & Matera 2011, p. 295.
[1129] Council of the European Union, 15951/12, 12.11.2012.
[1130] 'The spider's web: Europol goes global in the hunt for intelligence and analysis', *Statewatch*, 14.03.2013. Available from www.statewatch.org [02 December 2014].
[1131] EP report on the draft Council decision amending Decision 2009/935/JHA as regards the list of third States and organisations with which Europol shall conclude agreements, European Parliament, A7-0351/2013, 23.10.2013.
[1132] Article 54 of Europol Regulation.
[1133] Nielsen N 2012, 'EU hands personal data to US authorities on daily basis', *EUobserver*, 22 June. Available from http://euobserver.com/22/116719 [10 December 2014]; Commission, 'SWIFT implementation report: MEPs raise serious data protection concerns', Press release, Committee on Civil Liberties, Justice and Home Affairs, March 2011.
[1134] Nielsen 2012.
[1135] Case T-529/09 - In 't Veld v Council, 04.05.2012.
[1136] Fox 2012.

Although the new regulation will broaden the EP tasks relating to Europol, it is not clear yet whether these will also apply to the existing international agreements or only to those adopted after the regulation enters into force.

### *3.5.3. The lack of a SIENA provision*

The tailor-made communication tool SIENA represents one of most secure measures created by Europol in order to exchange personal and non-personal data. Besides its use for data transfers between Europol and member states, as well as among member states themselves, there are today several third countries connected to SIENA. According to the last Europol General Report, forty-two third parties are connected to SIENA (thirteen directly and twenty-nine indirectly).[1137]

When a third country uses SIENA as a communication tool, a message can be exchanged directly between the following actors: a) Member states and Europol, b) operational or strategic third parties and Europol, and c) among operational or strategic third parties among themselves.

Norway and Australia were the first two third countries directly connected to the system, on 18 January and 7 April 2011 respectively. Ghana, Croatia and Iceland also joined the system that year. In 2012, eight other third countries connected to SIENA: the US, Switzerland, Serbia, Montenegro, Bosnia & Herzegovina, Albania, Turkey, Monaco and Canada. The tool is expanding its borders year by year.

Moreover, its use is no longer limited to third countries having operational agreements with Europol, but it is also offered to third parties with strategic agreements. Specifically, Bosnia & Herzegovina, Montenegro and Turkey are strategic partners of Europol and they use SIENA. Also, many US agencies are connected to SIENA.[1138] The problem is that, although each of these agencies has a liaison officer at Europol, there is no contact point in the US territory.

The JSB has often underlined the necessity to regulate the use of SIENA as a messaging system between third parties.[1139] The body has also reiterated that SIENA is an adequate tool for exchanging information in terms of data protection and data security, including those communications sent beyond the EU borders.

---

[1137] Council of the European Union, 10426/14, 06.06.2014, p. 13.
[1138] Particularly these are the ATF, DAA, FBI, ICE, NCIS and USSS.
[1139] Joint Supervisory Body, Opinion 13/31, 10.06.2013, p. 8.

However, there is no regulation of SIENA in the proposal. The absence of a SIENA provision in the proposed Europol regulation is particularly disappointing, since there are no rules to date about the exchange of data through this tool. Moreover, the inclusion of a SIENA clause in the proposal could have engaged other third countries to join it.

It has been seen above that a disparity currently exists within and beyond the EU regarding the channels and tools to exchange crime-related data. This could be minimised by establishing SIENA as the common default communication tool. The proposal underlines the importance of introducing privacy-by-design systems in Europol. SIENA definitely complies with the requirements to be considered a privacy-by-design tool. Yet, the proposal, which was the perfect context for it, has missed the opportunity to introduce specific rules on this tool.

### *3.5.4. Processing of data from third countries to Europol*

As in the current legal framework, Europol will not need a cooperation agreement for receiving information from a third country. Nonetheless, the proposal includes a few new rules in this respect. First, it expressly establishes the possibility to receive information from a private party in a third country.[1140] This will be feasible as long as one of the following conditions is met: a) it is through a contact point of a third country with which Europol has concluded a cooperation agreement in accordance with Article 23 of Decision 2009/371/JHA, or b) it is through an authority of a third country or an international organisation with which the EU has concluded an international agreement pursuant to Article 218 TFEU.

Second, the proposed regulation explicitly states that Europol will not process 'any information which has clearly been obtained by a third country or international organisation in violation of human rights'.[1141] This new provision seeks to regulate what has been Europol's praxis for many years. For instance, negotiations with Russia for a cooperation agreement took a very long time due to the several violations of human rights by that country. Europol suggested many institutional and political changes as the conditions *sine qua non* for the adoption of a cooperation agreement with Russia. Today, the agreement has been concluded, but it still needs to be implemented. Lastly,

[1140] Article 32(1) and 33(1) of Europol Regulation.
[1141] Recital 31 of Europol Regulation.

the proposed regulation introduces specific evaluation codes on accuracy and reliability in Article 35, which will also apply for the information received from a third country or international organisation.[1142]

A related debate emerging from new Articles 24 and 25 needs to be highlighted. In the proposed Europol regulation, Article 24 makes a distinction between operational and strategic analyses. However, then Article 25(1) states that:

'[A] Member State, a Union body, a third country or an international organisation providing information to Europol determines the purpose for which it shall be processed as referred to in Article 24.'

Thus, a third country can discretionarily decide to send a piece of information to one or several member states, but exclude Europol. Europol has no voice in deciding if certain information from a third country is necessary for its investigations, since the main objective of the agency is to support member states in the prevention, combat and investigation of crimes, but it does not include the support of third parties. Therefore, any petition from Europol to be included in data exchanges between third countries and member states is beyond the agency's mandate.

Finally, the Council has suggested including a paragraph in the proposed regulation that would allow the receiving of data sent by private parties in a third country with no cooperation agreement. The only limitation that the Council sets for that procedure is that Europol forwards the information to the member state that has concluded an agreement with the third country.[1143] Similarly, if Council's amendments are approved, Europol will be able to share data with private parties as long as the data subject has presumably consented to it, or if it is necessary for the prevention of an imminent threat.[1144]

## 4. Shortcomings and limitations of Europol's data protection rules

As revealed in this study, Europol has become a comprehensive EU police actor due to its robust data protection framework. Europol's data protection rules are stronger than

[1142] Article 35(5) of Europol Regulation.
[1143] Council of the European Union, 8596/14, 07.04.2014, Article 32(1b).
[1144] Council of the European Union, 8596/14, 07.04.2014, Article 32(3a).

those applied in the majority of member states and third countries. However, there are several issues today that impede such a scheme from becoming a reference for EU and non-EU countries. These are listed in the following paragraphs.

First of all, there is a lack of will from member states and third countries have to share information with the agency. National law enforcement authorities often prefer to share information bilaterally rather than multilaterally.[1145] They are reluctant to send data to Europol for several reasons. Sometimes these countries follow a rather 'national-minded' approach,[1146] and sometimes they simply do not trust the agency.[1147] Another reason is that some member states do not believe that the agency offers any 'added value' to their national investigations. In this sense, many scholars refer to an inherent 'chicken-egg dilemma': Europol is not granted executive powers by the member states; but it is precisely this limitation that causes the agency's lack of 'added value'.[1148] As a result, Europol does not make full use of all its capabilities and loses effectiveness as a EU police agency.

Second, Europol has no enforcing powers. This means that the agency has a very limited power over national law enforcement agencies' actions. An example of this is found in the paragraph proposed by the Council for the proposed Europol regulation. The Council suggests in Article 41 that 'if Europol becomes aware that personal data […] are factually incorrect or have been unlawfully stored, it shall inform the provider of that data accordingly'. This is what currently occurs for data that Europol identifies as incorrect or out-of-date. Even if Europol modifies its database accordingly, there is no way to certify that the originating Member State has also amended the data.

Third, data processed by intelligence agencies is out of the scope of Europol. As examined in Chapter 4 of this thesis, a large part of the information processed for security reasons is collected by intelligence services of the member states. For instance, in some countries police agencies are in charge of counter-terrorism policies, whereas in

---

[1145] Bures & Ahern 2007, pp. 222; Kaunert 2010, p. 656.
[1146] Occhipinti JD 2013, 'Availability by Stealth? EU information-sharing in transatlantic perspective', *European Security, Terrorism and Intelligence. Tackling New Security Challenges in Europe*, eds. Kaunert C & Leonard S, Palgrave Macmillan, Hampshire, p. 160.
[1147] Rozée S, Kaunert C & Léonard S 2013, 'Is Europol a Comprehensive Policing Actor?', *Perspectives on European Politics and Society*, vol. 14 no. 3, pp. 372-387.
[1148] Bures 2008, p. 513; Bures 2011, pp. 85-109; Leonard S & Kaunert C 2013, 'Introduction - Beyond EU Counter-terrorism Cooperation: European Security, Terrorism and Intelligence', *European Security, Terrorism and Intelligence. Tackling New Security Challenges in Europe*, eds. Leonard S & Kaunert C, *Palgrave Macmillan*, Hampshire, p. 9; Bures O 2013, 'Europol's counter-terrorism role: A chicken-egg dilemma', *European Security, Terrorism and Intelligence. Tackling New Security Challenges in Europe*, eds. Kaunert C & Léonard S, Palgrave Macmillan, pp. 65-93.

others these fall under the scope of the intelligence services' tasks.[1149] Data collected by intelligence services is rarely shared with Europol, since the EU has its own supranational intelligence body called IntCen. Although IntCen and Europol have a cooperation agreement in force, Europol only assesses trends on a general level and it cannot conduct intelligence analysis outside the EU borders.[1150] Therefore, the participation of Europol in police investigations is constrained by the lack of access to information collected by intelligence services.

Finally, there is a lack of convergence between some provision in the proposal for the Police and Criminal Justice Data Protection Directive and those in the future Europol regulation. A confluence in the wording of both instruments is crucial to have a consistent EU data protection framework in the field of law enforcement. The proposed Directive, despite excluding Europol from its scope, impacts directly on the future Europol legislation. The necessity to align both instruments is in fact mentioned in recital 32 of the proposed Europol regulation:

'Europol should be autonomous and aligned with […] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [to *be replaced by the relevant Directive in force at the moment of adoption]*.'

It is unclear what pushed the Commission to launch the proposal for a Europol regulation before the Data Protection Directive was in force. As the JSB noted, it would have been preferable to wait for the outcome of the proposed data protection package.[1151] In any event, it is probable that ultimately the Europol regulation will not be adopted until the new EU data protection legal framework is in force.[1152] For the moment, both proposals are being examined by the EP and the Council.

[1149] Kaunert 2010, p. 656.
[1150] Cross 2013, p. 391.
[1151] Joint Supervisory Body, Opinion 13/31, pp. 2 and 5.
[1152] The indicative date by which the data protection directive will be adopted is Summer 2015, but EU lawmakers have already noted that serious differences among member states could delay the approval until 2016. See http://www.euractiv.com/sections/infosociety/eu-lawmaker-warns-data-protection-rules-delay-till-2016-311100 [8 January 2015].

## 5. Concluding remarks

Europol's cooperation with member states has intensified over the years – especially since 2009, when the Treaty of Lisbon and the Europol Council Decision entered into force. The first part of this chapter has demonstrated that Europol's involvement in national police investigations is advantageous from a privacy perspective. The agency offers high data security and data protection safeguards for both member states and individuals.

One of the data-sharing problems that member states have experienced lately is that they do not have a common communication channel for transferring information. While some member states have moved towards a more systematic use of the Europol channel (ENU), others continue to rely on the Interpol channel because of the traditional central role and ease of use of this instrument. Sometimes, such a multiplicity of available channels entails ineffectiveness at the EU level. Therefore, this chapter has studied the possibility to centralise every cross-border data transfer for law enforcement matters into the SIENA tool. SIENA could ideally be the default communication tool for all data transfers, ensuring the same data security standards in any data exchange.

This study has demonstrated that Europol includes higher data protection standards than many of the member states. In particular, Europol has exemplary data protection rules on the right of access, correction and deletion; purpose limitation principle; retention periods; SIENA as privacy-by-design tool; data quality; and external supervision, to name but a few. These will be maintained in the proposed Europol regulation. This study has examined the latest issues and controversies of this new proposal.

Third countries willing to conclude a cooperation agreement with Europol must first comply with the data protection standards of the agency. Europol has made several third countries align their legal frameworks to the Europol's data protection rules. In fact, negotiations between Europol and third countries are subject to much lower political pressures and lobbyism than an agreement adopted between the EU and third countries. Therefore, it is easier for non-US countries to find accordance with Europol than with the EU as a whole.

In light of the foregoing considerations, it can be concluded that Europol plays a key role in the global security environment. Its structure complements the existing networks of law enforcement officials for exchanging information within and beyond the EU. As

Mournier noted in 2009, the agency 'exports European standards of policing and contributes to shaping local police systems'.[1153] Therefore, the Europol data protection framework could be taken as a reference for all crime-related data exchanged among EU and non-EU countries. Yet, as pointed out earlier, intelligence services' data transfers do not follow the same data protection standards. This is examined in the next chapter of this thesis.

[1153] Mounier 2009, p. 584. See also Carrapiço H & Trauner F 2014, 'Europol and its influence on EU policy-making on organized crime: analyzing governance dynamics and opportunities', *Justice and Home Affairs Agencies in the European Union*, eds. Kaunert C, Léonard S & Occhipinti JD, Oxford, pp. 85-97.

## Chapter 4: Data safeguards for the intelligence collected and shared by member states

The previous three chapters have studied systems used by law enforcement authorities (mainly, police officers) to process data within and beyond the EU. They have examined the consistency between EU internal and external measures for data processing, as well as the impact they have on the EU fundamental right to data protection. Particularly, Chapter 3 has suggested looking at Europol's legal framework as a guideline for establishing common data protection principles in the field of law enforcement.

However, in the field of security, data is not only processed for law enforcement purposes, but also by intelligence services. Despite the existing legal differences of data processed by intelligence services and data processed by law enforcement authorities, in practice, the line separating their tasks has become difficult to draw. In the past, the law enforcement authorities' methodology was clearly to 'see and strike', whereas intelligence services' functions were to 'wait and watch'.[1154] In that sense, Germany still has a law of separation ('Trenungsgebot') that divides the roles between intelligence and police forces.[1155] However, this division became more and more blurred over the years. The 'wall' that separated law enforcement agencies from intelligence services crumbled after 9/11.[1156] Today, police agents and intelligence analysts maintain regular contact, to the point that in some member states (e.g. Spain), the intelligence community has a special department assigned to police agents, which allows direct contact between the two entities. In these cases, every time the intelligence agency gathers relevant information on a current or imminent crime, the centre informs police authorities, who will initiate an investigation based on that premise. The same occurs at the EU level with regard to the information sent from IntCen (intelligence centre) to Europol (law enforcement agency).

This chapter studies the main challenges that member states have with regard to the regulation and control of intelligence processed within the EU. As a general rule, the EU has no capacity to cover standard intelligence service activities. Yet, there is a

[1154] Svenden ADM 2011, 'On a "continuum with expansion"? Intelligence cooperation in Europe in the early 21st Century', *Journal of Contemporary European Research*, vol. 7, no. 4, p. 523.
[1155] Hillebrand 2012, p. 94.
[1156] De Busser 2010, p. 98.

blurred line between intelligence services and law enforcement activities today. In this sense, the aim of this chapter is to identify whether the EU could have legal competence to adopt legislation on data exchanges among intelligence agencies. First, the Snowden revelations and the activities that intelligence services conduct within and beyond EU borders will be studied. After that, a comparative study of intelligence agencies in France, Germany, Spain and the United Kingdom will be conducted. The choice of countries has been based on the locations where terrorist cells have been identified (Hamburg and Paris) and terrorist attacks have recently taken place (Madrid, London and Paris).

In summary, this study seeks to examine whether the lack of coordination of intelligence agencies, the systematic storage and data access by intelligence services, and the divergence in external supervision mechanisms could negatively affect the establishment of global data protection standards.

## 1. Data processed by intelligence services

According to Article 4(2) TEU and Article 72 TFEU, data processing for 'national security' purposes falls outside of the scope of the EU laws. This purpose is also expressly excluded from data protection instruments like Directive 95/46/EC or the Council of Europe's Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (108 CoE Data Protection Convention). Thus, national security measures are not protected by European privacy laws. But what exactly is 'national security'? A formal definition of this term is still missing in the EU laws.

Security policies in member states are essentially organised through law enforcement authorities, intelligence services and military staff. Whereas the former has a role at the EU level through Europol and laws adopted under the AFSJ, the regulation of intelligence and military agencies remain, for the most part, in each Member State. However, the division of roles between law enforcement and intelligence services is not always clear, and it causes confusion about what the EU can and cannot regulate. As the 'Future Group'[1157] of the Council of Ministers pointed out:

[1157] Informal High Level Advisory Group on the Future of European Home Affairs Policy.

'While an exchange of information between national police forces is increasingly seen as common sense, the exchange of information between intelligence services creates a considerable challenge for the European Union.'[1158]

Unlike law enforcement authorities, who are subject to several EU laws (e.g. the recently annulled Data Retention Directive) and international agreements (e.g. the PNR agreements), there is little Brussels can do to regulate laws governing intelligence services. Rules on these agencies are exclusively enacted by member states.

In June 2013, the ex-analyst of the US National Security Agency (hereinafter, the NSA)[1159] Edward Snowden revealed numerous controversial activities conducted by the NSA. According to Snowden's documents, the NSA access millions of personal data from Americans and foreign citizens every day. That revelation sparked a controversial debate about the NSA, because these activities have been kept secret for a long time and they constitute direct violations of the right to privacy and data protection. For its part, the US government justified the actions by explaining that all data accesses were carried out according to proportionality and necessity criteria, and that the only goal was to fight the global terrorism that emerged after 9/11.

The Snowden revelations have questioned the legality of the US intelligence services' practices of mass surveillance. However the US is not an exception. Most countries in the world are engaging in similar surveillance practices. There are many studies stating that Internet surveillance programmes in the EU are equivalent to those of the NSA.[1160] Thus, in the EU (as in the US) a significant part of the information exchanged for the prevention and combat of serious crimes is collected by intelligence services.

Information processed by intelligence services is, in 85% of cases, originally obtained through public sources and then transformed into intelligence (it is called Open Sources Intelligence or OSINT). The other 15% comes from private sources. They use software that allows them to crack passwords in a very short time. Hence, the main challenge of any intelligence agency is not the collection of data in itself, but rather the

[1158] Council of the European Union, 11657/08, 09.07.2008, p. 38.
[1159] On the history of the NSA, see http://www.nsa.gov/history/index.cfm [5 November 2014].
[1160] Heumann S & Scott B 2013 'Law and policy in Internet surveillance programs: United States, Great Britain and Germany', *Stiftung Neue Verantwortung,* vol. 25, no. 13, pp.1-17; Biermann K 2013, 'German intelligence service is as bad as the NSA', *The Guardian*, 4 October. Available from <http://www.theguardian.com> [5 November 2014].

selection and analysis of the immense amount of data, and its transformation into useful intelligence.[1161]

Thus, the main goal of analysts and experts of intelligence services is to provide useful knowledge rather that raw data.[1162] However, on occasion, the overabundance of information collected by intelligence services has been counterproductive. The Madrid terrorist attack of 2004 is an example of the inefficiency resulted of collecting too much information. Analysts of the Norwegian Defence Research Establishment (FFI) tracked a public document on the Internet about Islamist terrorism. It included a detailed analysis of the Spanish political situation and a lengthy explanation of why the country should be seen as a target for Islamist terrorist groups after it aligned its policies to those in the US and the UK.[1163] Unfortunately, that document did not end up in the right hands to prevent the attack in Madrid. As this proves, only with a coordinated system is data collected by intelligence services a relevant tool for the prevention and combat of terrorism.

## 2. The blurry scope of national security and implications for the EU legislation

In the US, surveillance activities conducted on US citizens within the US territory but falling under the scope of 'national security' are not protected by the US Fourth Amendment. This exception was first established by the US Supreme Court in *Katz* v. *United States* (1967).[1164] Since then, the US Supreme Court has invoked the national security exception in numerous cases, in order to justify warrantless surveillance activities.[1165]

---

[1161] There is no globally accepted definition about 'intelligence'. According to Michael Warner 'Intelligence is secret, state activity to understand or influence foreign entities'. Warner M 2002, 'Wanted: A Definition of "Intelligence". Understanding our craft', *Studies in Intelligence*, vol. 46, no. 3. Available from https://www.cia.gov [5 November 2014].

[1162] Lowenthal M 1998, 'Open Source Intelligence: New Myths, New Realities', *Defense Daily International*, Special Reports. Available from http://www.oss.net [5 November 2014]; Taplin W L 1989, 'Six general principles of intelligence', *International Journal of Intelligence and Counterintelligence*, vol. 3, no. 4, pp. 475-491; Davenport TH & Prusak L 2000, *Working knowledge: How organizations manage what they know?*, Harvard Business School Press, Boston.

[1163] Navarro Bonilla D 2005, 'Introducción' in *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional,* Grupo de Trabajo número 5/04, Dirección General de Relaciones Institucionales de la Defensa. Instituto Español de Estudios Estratégicos, Madrid, pp. 10-11.

[1164] *Katz* v. *United States*, 389 US 347 (1967).

[1165] United States v. United States District Court, 407 US 297 (1972); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973); United States v. Butenko, 494 F. 2d 593, 605 (3d Cir.1974); United States v. Buck, 548 F.2d 871, 875 (9th Cir.1977); United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir.1980); In re Directives to Yahoo! Inc., 551 F. 3d 1004 (FISA Ct. Rev. 2008).

Similarly, in the EU, national security measures do not offer a full privacy protection for the EU citizens. Article 4(2) TEU excludes aspects related to national security from the scope of the EU legislation. This provision was introduced in the Treaty of Lisbon after the UK insisted that intelligence matters should not be part of the EU competences.[1166] The clause expressly states that national security matters remain competence of the member states. However, there is today no single accepted definition in the European and international treaties on what 'national security' covers.[1167] Numerous scholars and politicians have offered definitions.[1168] Most of them agree that the term describes certain actions that society entrust to the governments to prevent adversaries from inflicting harm.

Security actions are often carried out by member states, but this is not always the case. For instance, the EU is not a state, but it can still adopt security measures. As Matlary points out, the EU security policy 'is both de-territorialised as well as de-nationalised'.[1169] Since 9/11, threats to security have been perceived as global. In that sense, the EP has noted that:

'While both the threats to national security and the responses to these threats have become increasingly globalised, accountability mechanisms have remained territorially bounded.'[1170]

The global war on terror has reshaped the essence of the state and, consequently, the concept of 'national security'.[1171] Member states are no longer limited to their domestic security strategies, but they also implement national security policies adopted by supranational organisations, such as the UN, NATO, and the EU. In the EU, Article 73 TFEU establishes that it is the responsibility of member states to cooperate and

[1166] Coolsaet 2010, p. 865.
[1167] WP 228, 05.12.2014.
[1168] Maier CS 1990, *Peace and security for the 1990s*. Unpublished paper for the MacArthur Fellowship Program, Social Science Research Council, NYC; Mangold P 1990, *National security and international relations*, Routledge, NYC, pp. 1-14; Paleri P 2008, 'National Security: Imperatives and Challenges', *Tata McGraw-Hill*, Delhi, p. 521; Sarkesian SC, Allen Williams J & Cimbala SJ 2008, 'National Security. Policymakers, processes and politics', *Lynne Rienner Publishers*, Boulder, CO, p. 4; Omand D 2010, *Securing the State (Intelligence and security)*, Oxford University Press, Oxford, p. 9.
[1169] Haaland Matlary J 2013, *European Union security dynamics. In the new national interest*, Palgrave Macmillan, London, p. 23.
[1170] 'Democratic oversight of Member State intelligence services and of EU intelligence bodies', *European Parliament, Working Document 5*, 12.12.2013, p. 4.
[1171] Buzan B 2007, 'What is national security in the age of globalisation?', *Utenriksdepartementet*. Available from <http://www.regjeringen.no> [5 November 2014].

coordinate between themselves for the safeguarding of national security.

In the EU, the concept of 'national security' is thus intertwined with the terms of 'EU internal security' and 'EU external security'.[1172] The EU regulates internal security matters as part of the AFSJ, [1173] and external security issues as part of the CFSP.[1174] Instead, the regulation of national security issues falls under the exclusive competence of the member states. The EU's role in this area would be purely coordinative, if any. For instance, one of the few examples of this limited EU role in national security matters is found in the regulation of the Schengen Information System.[1175] Article 93 of Schengen Agreement Application Convention (SAAC) states:

'The purpose of the Schengen Information System shall be in accordance with this Convention to maintain public policy and public security, including **national security**, in the territories of the Contracting Parties and to apply the provisions of this Convention relating to the movement of persons in those territories, using information communicated via this system.' (Emphasis on my own)

The areas of national security, EU internal security and EU external security overlap with each other. Intelligence services are identified as the bodies in charge of national security matters in each Member State but, in fact, they have a role in certain supranational bodies too. For instance, within the scope of the AFSJ, the European Cybercrime Centre (EC3) collects and processes cyber intelligence. The centre, established in 2013, is composed of national experts (police and intelligence agents) in the member states, as well as representatives of other institutions like the EEAS or the US Secret Service. Moreover, as part of the EU external security, the intelligence centre IntCen[1176] should be highlighted. IntCen is a central part of the EEAS, composed of representatives of intelligence services in the member states. Hence, the centre's activities are related to national security.

[1172] 'Draft Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs', 2013/2188(INI), European Parliament, 23.12.2013, p. 9; Opinion of the Advocate General Bot on the case C-658/11, 30.01.2014, para. 113.
[1173] Articles 67-89 TFEU.
[1174] Articles 21-46 TEU.
[1175] See Chapter 1, section 3 of this thesis.
[1176] On IntCen, see Chapter 2 section 1(2), and section 5(3) of this chapter.

For all said above, it can be concluded that the EU has *de facto* certain competences in the regulation of intelligence services' activities, despite the national security exception. The scope of Articles 4(2) TEU and Articles 72/73 TFEU needs to be concretised by the CJEU.[1177] The Court is the EU institution that can better distinguish this concept from the similar terms of 'State security', 'internal security' and 'public security'. It can also discern whether the exemption of Article 4(2) has a general nature or if it applies only for certain activities of intelligence agencies.

The lack of precision of the national security exclusion may lead to abusive situations by law enforcement authorities with respect to the right to data protection. If all intelligence activities are considered part of the national security exclusion, it means that no EU data protection laws are applicable for these agencies. What is the purpose of protecting individuals' data collected by law enforcement authorities, if intelligence services can still freely break into their computers or intercept their calls? As Scheinin pointed out in 2009, the shift in tasks from law enforcement to intelligence agencies may serve as a way to circumvent the privacy protections in a Member State.[1178]

### 3. The significance of the Snowden revelations at the EU level

Since the summer of 2013, mass surveillance activities conducted by intelligence services became an issue of concern in the EU. The close cooperation that the NSA has with some member states has called into question to what extend it violates the EU's right to data protection protected by the Charter of Fundamental Rights, the 108 CoE Data Protection Convention, Directive 95/46/EC and Framework Decision 2008/977/JHA.

This section studies the history of the NSA, the data collection programmes that the NSA uses, and its secret cooperation with some member states. It also examines the reaction to and potential consequences of the Snowden revelations with respect to the current EU-US data-sharing agreements.

---

[1177] Korff D 2014, 'Expert Opinion prepared for the Committee of Inquiry of the Bundestag into the "5EYES" global surveillance systems revealed by Edward Snowden', *Committee Hearing, Paul-Löbe-Haus*, Berlin, p. 38; WP 228, 05.12.2014.

[1178] Scheinin, M 2009, 'Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', *General Assembly of the United Nations*, A/HRC/10/3, NYC, p. 11.

### 3.1. The start of the NSA and ECHELON

The origins of the NSA date back to the end of the First World War (WWI).[1179] However, the NSA was not officially created until 1952, a few years after the establishment of the CIA.[1180] The NSA has its headquarters in Fort Meade (Maryland, USA). This agency is bigger than the CIA and the FBI combined. The main building in Fort Meade has more than 95,000 workers and it classifies from 50 to 100 million documents a year. During the first ten years after the establishment of the NSA, its existence was unknown among the general public. The history of this agency is based on secrecy. Analysts working there cannot reveal anything relating to the centre and they have minimal contact with the external world. The NSA is thus both the largest and the most clandestine of all US intelligence agencies.

Originally, the main purpose of the NSA was to provide detailed knowledge about the strategies and activities of the Soviet Union.[1181] It initially intercepted foreign communications in the political and military fields, but over the years the activities of this agency have expanded.[1182]

The NSA has used different methods to intercept telephone, fax and email communications. Initially these interceptions were mainly conducted via microphones or laser equipment in small rooms, which sent out radio waves within an area up to thirty meters, and through wiretapping.[1183] The interception of radio signals was called SIGINT[1184] and it was divided into two subsystems: COMINT[1185] and ELINT.[1186] The SIGINT system was based on several antennas that synchronised communications and electronic information with no awareness from the targets. This system was utilised

[1179] For a further analysis about the Agency's activities during WWI, see Powers T 2004, 'Intelligence wars: American secret history from Hitler to Al-Qaeda', *NYREV*, NYC, pp. 231-234.
[1180] The CIA was created in 1947 with the aim of detecting terrorist threats, and it was a direct consequence of the US failure after the Pearl Harbour attacks.
[1181] Powers 2004, p. 239.
[1182] An in-depth analysis of the NSA activities in Bamford J 1982, *The Puzzle Palace - A Report on America's Most Secret Agency,* Houghton Mifflin, Boston.
[1183] 'Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))', European Parliament, A5-0264/2001 PAR1, 11.07.2001, p. 30.
[1184] SIGINT comes from as 'SIGnals INTelligence' and it is obtained from electronic signals that produce foreign communication systems, radars, etc.
[1185] COMINT comes from 'COMmunications INTelligence' and it is a subcategory from SIGINT, which collects foreign messages and voice communications.
[1186] ELINT comes from 'Electronic INTeligence' and it collects intelligence through electronic sensors. It is used to detect nearby ships and aircrafts.

during the Vietnam War in the 1960s and the Gulf War in 1990-1991 to spy on enemies.[1187] The NSA has also conducted interceptions via submarine cables, although this was rather unusual. That method was used, for instance, in 1971 when the American submarine Heli Bot recorded communications coming from a Soviet Union cable. The submarines had a magnetic system that allowed the reading of signals running through the cables. However, submarines were mainly used during wartime to eavesdrop on enemy communications.[1188]

Two controversial operations came to light in the 1970s, after the Watergate scandal:[1189] Minaret and Shamrock. The Minaret operation started in 1967 and consisted of warrantless interception of domestic electronic communications. The NSA spied famous people like Jane Fonda, Malcolm X, Joan Baz, Dr. Benjamin Spock and Martin Luther King.[1190] More than 6,000 foreigners and 1,000 Americans were spied on during that operation.[1191] The Shamrock operation dated back to as early as 1945 and it consisted of NSA bulk collection of telegrams when one end was outside the US. The three largest telecommunication companies in the US – Western Union, RCA and ITT- provided the NSA with the transcriptions of all telegrams arriving and leaving the country every day. That information helped the agency identify left-wing individuals who demonstrated against the war. The information collected was then sent to other US authorities like the FBI, the CIA, the Secret Service, the Bureau of Narcotics and Dangerous Drugs (BNDD), and the Defense Department. That practice was carried out for four decades, until a Senate committee chaired by Senator Frank Church made it public.[1192] The report issued by Senator Church explained that the NSA collected 150,000 communications a month, which meant that at least one message was intercepted every forty-five minutes.

After the Watergate scandal, there was a big debate about the two operations and thus the NSA decided to terminate them. However, a more powerful system was still ongoing: ECHELON. In 1943 the UK and the US signed an agreement to share intelligence collected via signal interferences. The UK had the necessary equipment to

---

[1187] Powers 2004, p. 257.
[1188] 'Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))', European Parliament, A5-0264/2001 PAR1, 11.07.2001, p. 31.
[1189] For further information: http://watergate.info [5 November 2014].
[1190] Webb DC 2008, *ECHELON and the NSA*, IGI Global, Hershey, PA, p. 459.
[1191] Documentary 'Echelon de secret power', 2002, min. 29. Available from www.youtube.com [20 December 2014].
[1192] Webb 2008, p. 460.

read codified messages, so the country worked with the US in the deciphering of messages sent by their enemies, the Germans. They learned about the Germans' strategy and that helped them to win the war. Once the war was over, the two countries decided to sign a new secret agreement called UKUSA (in March 1946).[1193] According to Article 4(a) of that agreement:

'The parties agree to the exchange of the products of the following operations relating to foreign communications: 01. Collection of traffic. 02. Acquisition of communications documents and equipment. 03. Traffic analysis. 04. Cryptanalysis. 05. Decryption and translation. 06. Acquisition of information regarding communications organizations, procedures, practices and equipment.'

Later, three nations of the British Commonwealth joined the agreement: Canada, Australia and New Zealand. Together with the US and the UK they formed the so-called '5-Eyes'. Other countries like Germany, Japan, Norway, Denmark, South Korea and Turkey became third parties of the agreement. All of them had a common enemy, the Soviet Union, so the intelligence agencies of the five countries started to cooperate closely. In fact, today they still have a special relationship with each other, as proved in the Snowden disclosures.

In the 1970s, intelligence services noticed that High Frequency (HF) waves could be easily intercepted. By locating a satellite in the right position in the space, all communications could be easy intercepted. Thus, ECHELON was born.

ECHELON was the codename of a giant satellite called P415. The five intelligence agencies which had access to data collected by ECHELON were the National Security Agency (NSA) in the US, the Government Communications Headquarters (GCHQ) in the UK, the Communications Security Establishment (CSE) in Canada, the Defence Signals Directorate (DSD) in Australia, and the Government Communications Security Bureau (GCSB) in New Zealand. None of them could have created a global system like ECHELON individually.

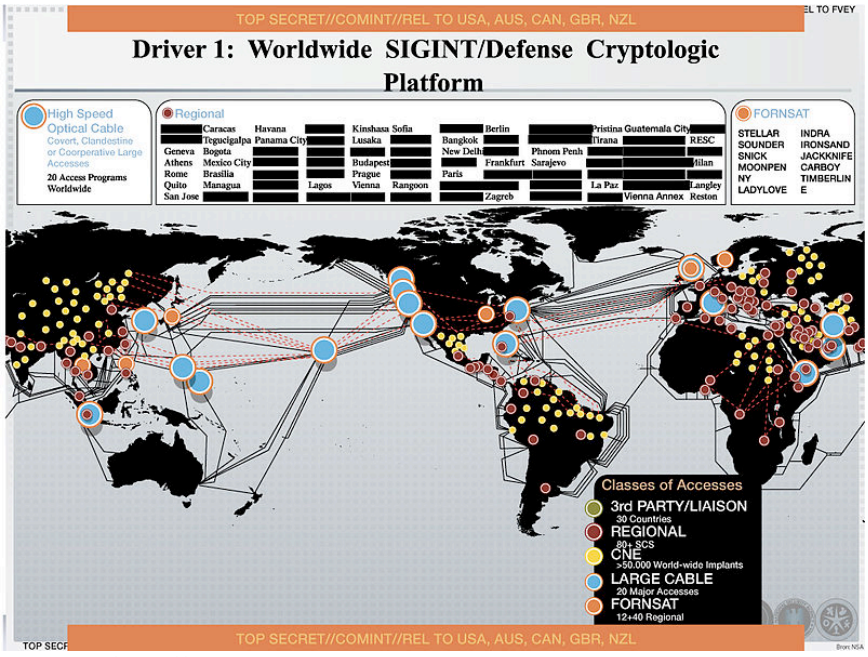
The initial objective of ECHELON was to intercept communications from the Soviet Union, but that goal expanded to the point that it currently intercepts and shares data from stations of commercial satellites around the world. In the last ten years, many

[1193] Amended version of 1955 available from http://www.nsa.gov [5 November 2014].

revelations by former analysts working in these five agencies have spoken out. These confirm that from the 1980s, intelligence agencies started to track activists such as Green Peace, the Red Cross, and Amnesty International; public figures like the Princess of Wales, the Pope, and Queen Elizabeth II; and even public bodies like the governments of Quebec, France and Japan.[1194]

The image below was leaked by Edward Snowden. The orange dots show the current locations of different FORNSAT/ECHELON stations.

*Figure 4.1.*



*Source: http://electrospaces.blogspot.com.es*

For many years, ECHELON was more powerful than the Internet itself. It collected and shared more than two million communications per hour,[1195] and it was not subject to any regulation. Through giant satellite disks established at each intelligence agency, it could globally intercept telephone calls, fax, Internet and email messages. Intelligence agencies received communications through specific antennas called 'radomes'. After processing the information, it was shared with other UKUSA members.

ECHELON not only collected millions of data, but also processed them. Several super-computers interconnected with each other scanned the information according to a

[1194] Documentary 'Echelon de secret power', 2002, min. 34.
[1195] Wright S 2005, 'The ECHELON trail: An illegal vision', *Surveillance & Society*, vol. 3 no. 2/3, p. 199.

list of key words that were integrated in the system. Each super-computer was known as a 'Dictionary' and its functions were similar to those conducted by a search engine today, but instead of scanning websites, it scanned landline and mobile phone calls. Every member in the '5-Eyes' had its own 'Dictionary'. They could modify the keyword list at their will. The super-computers had semantic intelligence and they filtered every word of a communication. If a word coincided with one in the list, the subjects of the communication automatically became targets. Then, that information was shared with other intelligence services via a global computer system called 'Platform'.[1196]

The activities of the NSA were ignored by the world for decades. The '5-Eyes' tried to hide the existence of ECHELON but that task became harder after Minaret and Shamrock came to light. In fact, the Watergate scandal led to a reform of the NSA laws. In 1975, a special committee of the US House of Representatives called the Pike Committee made a list of recommendations that became the premise of the Foreign Intelligence Surveillance Act (FISA) of 1978.[1197] FISA was created to obtain evidence for foreign intelligence. That law established the creation of the Foreign Intelligence Surveillance Court (FISC), which issued warrants based on probable cause that the target was an 'agent of a foreign power'. The court had to authorise surveillance activities conducted by the NSA and the FBI. According to the Snowden documents, in thirty-three years (1979-2013) the FISC received 34,000 requests, of which the court only rejected eleven (0.03%).[1198]

As ECHELON was not subject to any regulation, the individuals whose data were intercepted did not have any protection, since they were not residents in the country where the interception took place.[1199] ECHELON was first revealed by the journalist Duncan Campbell in his article 'Somebody's listening', published in New Statesman in 1988.[1200] The article was later complemented by the Nicky Hager[1201] and Steve

---

[1196] Webb 2008, p. 455.

[1197] For a criticism of the law, see Khan Z 2006, 'The National Security Agency (NSA) eavesdropping on Americans. A programme that is neither legal nor necessary', *Utrecht Law Review*, vol. 2, no. 2, pp. 61-80.

[1198] 'Edward Snowden Testimony to the European Parliament', March 2014, p. 7. Available from http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf [5 November 2014].

[1199] 'Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))', European Parliament, A5-0264/2001 PAR1, 11.07.2001, p. 24.

[1200] Campbell C 1988, 'Somebody's listening', *New Statesman*, 12 August. Available from http://www.newstatesman.com [5 November 2014].

Wright[1202] findings. All of these reports on ECHELON pushed the EP to constitute a temporary committee – not an enquiry committee – on the ECHELON Interception System on 5 July 2000.[1203] The committee lasted twelve months and it comprised thirty-six MEPs.[1204]

The results obtained by the committee were not especially fruitful. They could not confirm the statements made by Campbell and Wright on the economic espionage conducted through ECHELON. These authors explained in their reports that ECHELON was not longer used to defend the US against the Soviet Bloc but rather to spy on big companies such as Airbus or Thompson CFS. However, the EP limited its report to a call for member states to ensure that intelligence services in their countries did not process competitive intelligence. The Parliament stated that these practices would interfere with the loyalty duty, the common market, and the principle of free competition among states. As for the legal framework of ECHELON, the EP concluded that it fell beyond the scope of the EU laws since it was an instrument used in the field of 'national security'.[1205]

### 3.2. The NSA data collection programmes

ECHELON is not the only NSA system to have been uncovered. The biggest revelation on the NSA's secret activities came from Edward Snowden, an ex-analyst who disclosed more than 1.7 million US top-secret documents that proved the intrusiveness of the Agency since 2001.

After 9/11, former US President George W. Bush announced that the country had entered into a 'War of Terror'.[1206] In consequence, the powers granted to law enforcement and intelligence agencies needed to be expanded in order to prevent and

---

[1201] Hager N 1996, 'Secret Power - New Zealand's role in the International spy network', *Craig Potton Publishing*, New Zealand.
[1202] Wright 2005.
[1203] OJ L 121, 24.04.2001, p. 131.
See details at: http://www.europarl.eu.int/comparl/tempcom/echelon/mandate_en.htm [20 December 2014].
[1204] Piodi F & Mombelli Y 2014, 'L'affaire ECHELON. Les travaux du Parlement européen sur le système global d'interception 1998 – 2002', *EPRS Service de Recherche du Parlement européen*, PE 538.877, Brussels, p. 19. See also Görlitz N 2013 'Le droit d'enquête du Parlement européen', *Cahiers de droit européen 49*, pp. 783-820.
[1205] 'Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))', European Parliament, A5-0264/2001 PAR1, 11.07.2001, pp. 18, 22 and 80-82.
[1206] 9/11 was used to justify all NSA programs. See NSA, FOIA Case: 71184B, 17.10.2013.

combat terrorism. In that sense, the NSA Inspector General stated in a report:

'Here is NSA standing at the U.S. border looking outward for foreign threats. There is the FBI looking within the United States for domestic threats. But no one was looking at the foreign threats coming into the United States. That was a huge gap that NSA wanted to cover.'[1207]

The 9/11 attacks were carried out by individuals from outside the US, in communication with people within the US (the 9/11 hijackers). Therefore, on 26 October 2011, the US Congress passed the Patriot Act.[1208] This act lowered the threshold of the so-called 'FISA wall', which minimised the interaction between law enforcement and intelligence agencies. Yet, after 9/11, former US President George W. Bush decided to promote the communication between all security agencies. Section 215 of that act[1209] enabled the US government to collect bulk telephone metadata of US citizens provided there were reasonable grounds that it was relevant for international terrorism or any foreign intelligence investigation. Metadata includes telephone numbers, the origin/destination of the call, and the date of the call. These are stored for a five-year period.

A few years later, in 2008, an act amending FISA (hereinafter, FISAA)[1210] expanded the US government's powers for the collection and processing of foreign intelligence. In particular, Section 702 of FISAA[1211] permits the government to target communications of non-US individuals 'reasonably believed' to be outside the US without a FISA warrant. The NSA only needs to send an annual report to FISC determining the targets for the coming year.[1212] As in Section 215, most of the data collected is retained for five years in the NSA database.

For almost a year, Snowden downloaded top-secret documents while working in

---

[1207] ST-09-0002 Working Draft, Office of the Inspector General National Security Agency, Central Security Service, 24.03.2009. Available from www.theguardian.com [29 November 2014].
[1208] The name stands for **U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism Act of 2001. 107th Congress Public Law 56. Available from http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm [5 November 2014].
[1209] 50 U.S.C. 1861.
[1210] FISA Amendments Act of 2008, H.R. 6304 (110th), 19.6.2008; reauthorised again in 2012.
[1211] 50 U.S.C. 1881a.
[1212] Greenwald G 2014, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Hamish Hamilton, London, p. 74. For the procedure, see 'NSA's Implementation of Foreign Intelligence Surveillance Act Section 702', NSA Director of Civil Liberties and Privacy Office Report, 16.04.2014, pp. 4-5.

Hawaii at Booz Allen Hamilton. He then travelled to Hong Kong and shared the information with *The Guardian* and *The Washington Post*. The first programme disclosed by Snowden was PRISM. In general terms, PRISM operates under Section 702 of FISAA and consists of collecting data from targeted individuals stored in the servers of nine major Internet companies: Google, Yahoo!, Facebook, Pa!Talk, YouTube, Skype, AOL and Apple. Through PRISM, the NSA and the FBI exchanged information provided by those companies. These companies have cooperated with the US government,[1213] and those that have sought resist it[1214] have usually been coerced by the Foreign Intelligence Surveillance Court (FISC). In 2011, FISC stated that the NSA was collecting 250 million Internet communications per year under PRISM. The data is held for five years.

FISC is comprised of District Court judges who do FISA work as an additional part of their duties. The Department of Justice issues the application to a single judge, who will decide whether the warrant is issued or not. The threshold is set on the existence of probable cause. This decision can be appealed to the FISA Intelligence Surveillance Court of Review (FISCR) and, ultimately, to the Supreme Court of the United States. Originally, FISC judges just reviewed the facts for individual surveillance orders. Yet, following the Patriot Act in 2001, FISA judges increasingly considered legal arguments too. These judges had to make very difficult legal decisions and they generally heard only from the government. Their opinions are not public, so there is no opportunity for outside feedback.

*Figure 4.2.*


In the EU, the collaboration of telecommunication service providers' (TSPs) with the

[1213] However, in the beginning they denied any knowledge of the existence of PRISM. Greenwald 2014, p. 109.
[1214] Exceptionally, in July 2013 Yahoo! won a case against the disclosure of users' data through PRISM. See Neal RW 2013, 'Yahoo wins victory against PRISM: FISA court orders NSA to declassify documents', *Ibtimes*, 16 July. Available from <http://www.ibtimes.com> [5 November 2014].

NSA was condemned by the Art. 29 WP. Reports released by this group are not binding, but they have a great political impact on the EU institutions and member states. Regarding the collaboration of Google, Facebook, Apple, etc. with the NSA, the Art. 29 WP pointed out that they could be infringing the EU laws:

'Companies need to be aware that they may be acting in breach of European law if intelligence services of third countries gain access to the data of European citizens stored on their servers or comply with an order to hand over personal data on a large scale.'[1215]

Other programmes used by the NSA under Section 702 FISAA were based on interception methods. Companies were not aware of such practices, but foreign governments were. For example, through BOUNDLESS INFORMANT the NSA collected more that three billion phone calls and emails passing through US telecommunication systems.[1216] MUSCULAR is another interception programme, which collects traffic and content data of Yahoo and Google's users.[1217] Similarly, RAMPANT-A is a programme that taps into cables and intercepts the content of phone calls, faxes, e-mails, Internet chats and even calls using VoIP like Skype.[1218] UPSTREAM surveillance consists of collecting data as it transits a network in real time. Telephone and Internet companies knew about the data collection but they had previously been compelled to sign a cooperation agreement with the NSA to lawfully permit that interception.[1219] All of these programmes have not been claimed illegal because the NSA does not break into the servers of the TSP but only intercepts the communications as they flow over fibre optic cables.

Programmes like BULLRUN, CHEESY NAME, EDGEHILL, and QUANTUMHAND have a more sophisticated nature. Through these systems, the NSA

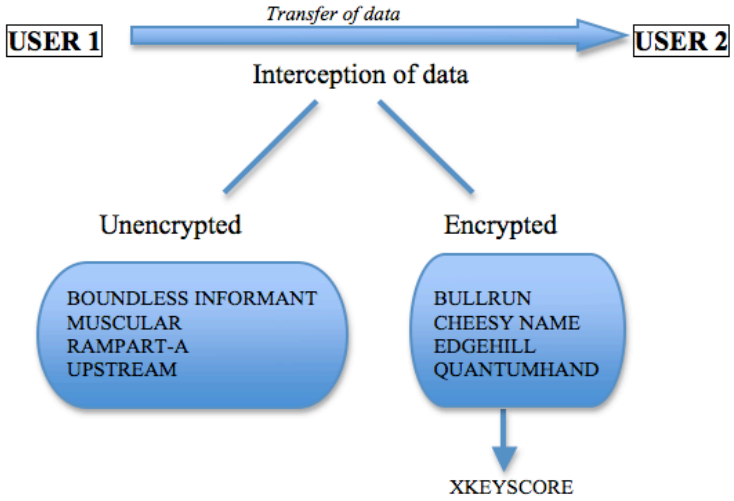
---

[1215] WP 215, 10.04.2014, p. 7.
[1216] Greenwald 2014, pp. 81 and 92.
[1217] Peterson A 2013, 'PRISM already gave the NSA access to tech giants. Here's why it wanted more', *The Washington Post*, 30 November. Available from <http://www.washingtonpost.com> [5 November 2014].
[1218] Gallagher R 2014a, 'How Secret Partners Expand NSA's Surveillance Dragnet', *The Intercept*, 18 June Available from <https://firstlook.org/theintercept/> [5 November 2014]. See also RAMPART-A Project Overview, 01.10.2010. Available from http://www.statewatch.org/news/2014/jun/usa-nsa-ramparts-2.pdf [5 November 2014].
[1219] 'NSA's Implementation of Foreign Intelligence Surveillance Act Section 702', *NSA Director of Civil Liberties and Privacy Office Report*, 16.04.2014, p. 5; and Bowden C 2013, 'The US surveillance programmes and their impact on EU citizens' fundamental rights', PE 474.405, *Policy Department Citizens' Rights and Constitutional Affairs, European Parliament*, Brussels, p. 15.

is able to break encryption technologies. For instance, BULLRUN is a decryption software that circumvents online protocols such as HTTPS.[1220] Likewise, CHEESY NAME singles out encryption keys and EDGEHILL is used to decode encrypted traffic of major IT companies. Finally, QUANTUMHAND is a programme through which the NSA installs a malware in the target's computer and uses a fake Facebook account to access the target's computer.[1221]

Once the NSA obtains the encrypted information, a programme called XKEYSCORE enables the agency to glean information from it. It is distributed in connection points across the globe (it has 150 sites and over 700 servers). This programme allows targets to be monitored in real time as they are writing an email or surfing the net.[1222] The mechanism used by this programme consists of 'slowing down the Internet' so that analysts can go back and recover sessions that otherwise would have been dropped by the front data. Content data is kept from three to five days, whereas metadata is saved for longer, for approximately thirty days. Much of the largest collection occurs in the UK under the basis of Executive Order 12333,[1223] therefore it does not have US court oversight.

*Figure 4.3.*




[1220] 'Project Bullrun – classification guide to the NSA's decryption program', *The Guardian*, 05.09.2013. Available from <http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide> [5 November 2015].
[1221] Gallaguer R & Greenwald G 2014, 'How the NSA Plans to Infect 'Millions' of Computers with Malware', *The Intercept*, 12 March. Available from https://firstlook.org/theintercept/ [5 November 2014].
[1222] Heumann & Scott 2013, p. 5; Greenwald 2014, pp. 157-158.
[1223] EO 12333 covers any activity not considered 'electronic surveillance'. Activities within the scope of EO 12333 do not required a prior court order.

Some of the programmes disclosed by Snowden are based on Section 215 of the Patriot Act. For example STELLAR WIND allows the NSA to collect bulk metadata from a TSP, after a FISC order is issued. The metadata belongs to US and non-US citizens and the FISC order can be renewed every 90 days.[1224] Data collected by the NSA through all of the above-mentioned programmes (and more) is stored in a 'broker', which is connected to a Google-like search engine. It is called 'ICReach' and enables the intelligence community to search for any name or piece of information they need.[1225]

The NSA has always stated that it uses all these programmes for the prevention and combat of global terrorism. After the revelations, great criticisms were raised about the lack of efficiency of these programmes, which have not always led to the interruption of terrorist plots. In light of these criticism, the NSA felt obliged to explain in which cases these programmes had effectively contributed to stop terror plots. The NSA stated that Section 215 programmes had detected fifty-four terrorist activities,[1226] whereas Section 702 programmes had helped stop at least forty-two attacks.[1227] However, the agency has always used the case of Basaaly Moalin[1228] to justify the effectiveness of Section 215. As for the programmes established under Section 702, the agency has usually mentioned the cases of David Coleman Headley,[1229] Najibullah Zazi,[1230] Khalid Ouazzani,[1231] Jamshid Muhtorov and Bakhtiyor Jumaev,[1232] and Jihad Jane[1233] as its

[1224] Greenwald G & Ackerman S 2013, 'NSA collected US email records in bulk for more than two years under Obama', *The Guardian*, 27 June. Available from http://www.theguardian.com [5 November 2014].
[1225] ICReach contains more than 850 billion data in total. Gallagher R 2014b, 'The surveillance engine: How the NSA built its own secret Google', *The Intercept,* 25 August. Available from https://firstlook.org/theintercept/ [5 November 2014].
[1226] Inglis JC 2013, statement in 'Strengthening privacy rights and national security: Oversight of FISA surveillance programs: Hearing before the S. Comm. on the judiciary', 113th Congress.
[1227] Ledgett R 2014, 'The NSA responds to Edward Snowden's TED Talk', *TED2014*. Available from http://www.ted.com [5 November 2014].
[1228] Moalin was a cabdriver from San Diego who provided $8,500 to al-Shabaab (al-Qaeda affiliate) during 2007 and 2008.
[1229] Headley is a Pakistani-American who plotted to attack the Danish newspaper Jyllands-Posten in 2009. He was also involved in the planning of the 2008 terrorist attacks in Mumbai.
[1230] Together with Zarein Ahmedzay and Adis Medunjanon, Zazi plotted to bomb the New York subway system in 2009. Yet, studies say that it was not the NSA but the British intelligence that initiated the investigation. Bergen P, Sterman D, Schneider E & Cahall B, 'Do NSA bulk surveillance programmes stop terrorists?', *New America Foundation*, p. 10. Available from http://www.newamerica.org [5 November 2014].
[1231] Ouazzani owned a small business in Kansas City and the NSA found that he provided tens of thousands of dollars to al-Qaeda for many years.
[1232] Muhtorov and Jumaev, nationals from Uzbekistan, were accused of providing support to the terrorist organisation Islamic Jihad Union.
[1233] Jane plotted to kill the Swedish artist Lars Vilks because of his depiction of the prophet Muhammad.

principle successes.[1234]

In June 2014, the Office of the Director of National Intelligence revealed that 89,138 people were targets under Section 702 FISAA in 2013 alone.[1235] Considering these numbers, one might wonder whether the forty-two success stories really justify the fact that almost 90,000 people were exposed to the NSA's scrutiny. Moreover, another public debate questioned the work of the NSA after it was unable to prevent the Boston Marathon bombings in 2013.[1236]

The NSA has also explained that any interception made under Section 702 indergo executive, legislative and judicial oversight. The executive review is conducted by an independent inspector general, who carries out regular on-site reviews and sends reports to the Congress.[1237] The legislative oversight is conducted by the Intelligence Committee and the Judiciary Committee of the House of the Representatives and the Senate. As for the judicial review, the NSA has ensured that any interception or intelligence gathering needs prior order from FISC. Also, every thirty days, the NSA sends a report to FISC about the state of the investigation.[1238] However, this court has been highly criticised by pro-privacy experts and activists due to its secrecy; the poor information it gets to effectively assess the NSA activities;[1239] the number of targets that a single order can involve;[1240] and the low number of cases the court has rejected to date.[1241]

The Snowden revelations sparked several legislative and political changes in the US. For example, Congress is currently studying several proposals for a reform of the NSA.[1242] Likewise, a list of five basic principles was released by key IT companies

---

[1234] Document NSA, FOIA Case: 71184B, DOCID: 4081032, 17.10.2013, pp. 8-9.
[1235] '2013 Transparency Report, Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2013', Office of the Director of National Intelligence, 26.06.2014.
[1236] Bergen et al. 2014, pp. 13-15.
[1237] NSA, FOIA Case: 71184B, DOCID: 4081031, 17.10.2013, p. 3.
[1238] NSA, FOIA Case: 71184B, DOCID: 4081031, 17.10.2013, p. 6.
[1239] Heumann & Scott 2013, pp. 6-7.
[1240] Which can get up to 89,138 targets for a single order. See Transparency Report 2014.
[1241] As mentioned above, out of 34,000 requests, the court has only rejected 11. Edward Snowden testimony before the European Parliament, March 2014, 7. Available from http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf [5 November 2014].
[1242] These have been proposed by Sen. Diane Feinstein (D-CA), Sen. Saxby Chambliss (R-GA), Sen. Patrick Leahy, (D-VT), Sen. Ron Wyden (D-OR), Sen. Mark Udall (D-CO), Sen. Richard Blumenthal (D-CONN), Sen. Rand Paul (R-KY), Sen. Al Franken (D-MN) the Sen. Dean Heller (R-NV), and the attorney Justin Amash (R), among others.

against the NSA mass surveillance,[1243] and recommendations were published by the Privacy and Civil Liberties Oversight Board on Sections 215 and 702.[1244] The NSA has started to publish regular transparency reports,[1245] and it now has a chief privacy officer,[1246] as well as a Review Group on Intelligence and Communications Technologies for the oversight of the agency.[1247] All of these changes are taking place in the US. Yet, the Snowden revelations have also had an impact outside the US territory and, especially, in the EU.

### 3.3. Secret collaboration of the EU member states with the NSA

Since 9/11, the cooperation of intelligence services in the EU with the US authorities has increased significantly. The common goal is to prevent a major terrorist attack. Today it is well documented that a few months before the 9/11 attacks many warnings came into the hands of the Central Intelligence Agency (CIA) and other intelligence services about Al Qaeda's intentions, but they were not considered a threat.[1248] In July that year, an FBI agent in Phoenix claimed that terrorists could be attending flight schools in preparation for an attack. Around that time, the CIA informed former President George W. Bush about a possible Al Qaeda plane hijacking that would take place on 6 August 2001. Also, by early September three foreign intelligence services reported to the CIA that Bin Laden had ordered his four wives to urgently return to Afghanistan.[1249] None of these dots were adequately connected.

Following the attacks, the US government handed a list of recommendations to the CIA, the FBI and the NSA. It urged for the recruiting of more spies (especially those

---

[1243] Davis W 2013 'Tech Companies Call For Privacy Oversight After Latest NSA Revelation', *Mediapost*, 1 November. Available from http://www.mediapost.com [5 November 2014]. See also reformgovernmentsurveillance.com [5 November 2014].

[1244] Privacy and Civil Liberties Oversight, 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court', 23.01.2014; Privacy and Civil Liberties Oversight, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 02.07.2014.

[1245] 'NSA's Implementation of Foreign Intelligence Surveillance Act Section 702', NSA Director of Civil Liberties and Privacy Office Report, 16.04.2014.

[1246] Kamen A 2014, 'The NSA has a new, first time ever, privacy officer', *The Washington Post*, 28 January. Available from www.washingtonpost.com [5 November 2014].

[1247] 'Liberty and Security on a changing world. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies', 12.12.2013.

[1248] Bergen P 2013, 'Would NSA surveillance have stopped 9/11 plot?', *CNN*, 31 December. Available from www.cnn.com [5 November 2014].

[1249] Powers 2004, pp. 362, 388-389. On the hijackers Khalid al-Mihdharee and Nawaf al-Hazmi, see Bergen et al. 2014, p. 13.

with connections to terrorists groups), as well as hiring new agents who could speak and translate relevant languages. From that moment, the NSA had to transform itself from a passive gatherer into a proactive terrorist hunter.[1250] In 2004, the Bush Administration released the 9/11 Commission Report through which it called other nations to engage 'in developing a comprehensive coalition strategy against Islamist terrorism'.[1251] Consequently, national intelligence services within the EU committed to collaborating closely with the US government and, most particularly with the NSA, in the prevention and combat of terrorism and serious crimes.

As discussed above, the NSA has been maintaining a special relationship with four other English-speaking countries: Canada, Australia, New Zealand and the United Kingdom (UK). This collective group is known as the '5-Eyes'. The only EU country among the 5-Eyes partnership is the UK. A close cooperation has existed between the NSA and the Government Communications Headquarters (GCHQ), a British intelligence organisation, since the Cold War,[1252] when they signed the UKUSA Agreement. More recently, and according to the latest documents released by Snowden, the GCHQ receives fifty billion data messages per day through different programmes,[1253] some of which are provided by the NSA. The GCHQ does not need any warrant to access bulk NSA data.[1254] One of the most controversial systems the GCHQ uses is the above-mentioned PRISM. Through this programme, the GCHQ is technically able to circumvent any formal British legal procedure and obtain data collected by the main TSP located outside the country.[1255] As mentioned in previous chapters, it is not uncommon that law enforcement agencies informally contact TSPs in order to obtain users' data. The same occurs with respect to intelligence services. The Snowden documents reveal that TSP such as Verizon, British Telecommunications, Vodafone, Global Crossing, Level 3, Viatel and Interoute have long cooperated with the GCHQ providing it with users' information when requested.[1256]

---

[1250] Powers 2004, p. 411.
[1251] The 9/11 Commission Report 2004, p. 379. Available from http://www.9-11commission.gov/report/911Report.pdf [5 November 2014].
[1252] Powers 2004, p. 240.
[1253] Greenwald 2014, p. 100.
[1254] 'Secret policy reveals GCHQ can get warrantless access to bulk data', *Privacy International*, 28 October 2014. Available from https://www.privacyinternational.org [19 November 2104].
[1255] Gellman B & Poitras L 2013, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program', *The Washington Post*, 6 June. Available from www.washingtonpost.com [5 November 2014].
[1256] Edward Snowden speech at the European Parliament, April 2014, p. 4. Available from www.europarl.europa.eu [5 November 2014].

Another programme used by the GCHQ is TEMPORA. Due to its privileged location, the UK hosts a quarter of all Internet traffic in the world. In consequence, the UK is able to tap into dozens of undersea transatlantic cables and gather telecommunication data. TEMPORA was created precisely to collect and store such information. The Snowden documents unveiled that the NSA also has access to that data.[1257] A debate has arisen because TEMPORA is supposed to be used by the GCHQ to intercept foreign communications only. Yet, communications originating in the UK can still be intercepted by the NSA and then passed onto its '5-Eyes' partners, including the UK.[1258] In other words, through TEMPORA the GCHQ is able to obtain communications from British citizens, circumventing the prohibition established in the British laws.

Besides the GCHQ, intelligence services in other EU member states have also been cooperating with the NSA. Specifically, these countries are Austria, Belgium, the Czech Republic, Denmark, Germany, Greece, Hungary, Italy, Luxembourg, The Netherlands, Poland, Portugal, Spain and Sweden.[1259] After the UK, Germany is the member state that has intercepted the most personal communications. Snowden used the following example when he told a German newspaper about the collaboration between Germany and the NSA:

'For example, we tip them off when someone we want is flying through their airports (that we for example, have learned from the cell phone of a suspected hacker's girlfriend in a totally unrelated third country – and they hand them over to us). They don't ask to justify how we know something, and vice versa, to insulate their political leaders from the backlash of knowing how grievously they're violating global privacy.'[1260]

---

**1257** MacAskill E & Ball J 2013, 'Portrait of the NSA: no detail too small in quest for total surveillance', *The Guardian*, 2 November. Available from www.theguardian.com [6 November 2014]; Nielsen N 2013, 'EU asks for answers on UK snooping programme', *EUobserver*, 26 June. Available from http://euobserver.com/justice/120656 [6 November 2014].

1258 Bunyan T 2014, 'GCHQ is authorised to "spy on the world" but the UK Interception of Communications Commissioner says this is OK as it is "lawful", *Statewatch*. Available from www.statewatch.com [6 November 2014], p. 13.

1259 Greenwald G & Aranda A 2013a, 'El CNI facilitó el espionaje masivo de EEUU a España', *El Mundo*, 30 October. Available from www.elmundo.es [6 November 2014].

1260 'Edward Snowden Interview.The NSA and Its Willing Helpers', *Spiegel*, 07.08.2013. Available from <www.spiegel.de> [6 November 2014].

The collaboration between German intelligence services and the US has increased significantly since 9/11 due to the fact that Al Qaeda established terrorist cells in Germany to prepare the attacks. The cooperation between the two countries dates back to the Cold War, when the US assisted German troops in Afghanistan.[1261] Today, the Federal Intelligence Service – the *Bundesnachrichtendienst* (BND) – mostly spies on foreign communications in countries such as Russia, Central Asia or the Middle East, but it has also permission to target Germans on a case-by-case basis.[1262]

However, the relationship between the US and Germany has been damaged since it was revealed that the NSA had been tapping the German Chancellor Angela Merkel's mobile phone for more than a decade.[1263] The surveillance began three years before she became Chancellor because the US wanted to gather information about the German position on the Iraq war.[1264] Germany has always had a special sensitibity towards issues concerning personal privacy and data protection due to its horrific experiences during the Nazi regime, and later by the East German secret police.[1265]

Another EU country that carried out enormous surveillance during 2013 is France. It collected data from more that seventy million French phones in only one month. The French intelligence community is divided into the *Direction de la Surveillance du Territoire* (DST), a domestic intelligence agency, and the *Direction Générale de la Sécurité Extérieure* (DGSE), an external intelligence agency. The programme used to intercept communications is called US-985D, which targets both suspects and non-suspects. Phone calls and SMS messages registered by that programme have also been shared with the NSA.[1266] Ironically, one of the documents disclosed by Snowden reveals

[1261] Bryant C & Fontanella-Khan J 2013, 'US spy scandal sparks EU privacy fears', *Financial Times*, 15 October. Available from www.ft.com [6 November 2014].
[1262] Farivar C 2013, 'German NSA has deal to tap ISPs at major Internet Exchange', *Ars Technica*, 7 October. Available from http://arstechnica.com/ [5 November 2014].
[1263] Lenoir F 2013, 'United States tracked Merkel's phone since 2002: report', *Reuters*, 26 October. Available from www.reuters.com [5 November 2014]; Rawlinson K 2013 'NSA surveillance: Merkel's phone may have been monitored 'for over 10 years', *The Guardian*, 26 October. Available from www.theguardian.com [6 November 2014]; Noack N 2014, 'Yes, Berlin has its own spying scandals, but don't expect Germany to forgive the NSA', *The Washington Post*, 20 August. Available from www.washingtonpost.com [6 November 2014].
[1264] Lewis P 2013, 'NSA denies discussing Merkel phone surveillance with Obama', *The Guardian*, 27 October. Available from www.theguardian.com [5 November 2014].
[1265] Eddy M 2013, 'For Western Allies, a Long History of Swapping Intelligence', *The New York Times*, 9 July. Available from www.thenytimes.com [5 November 2014].
[1266] Follorou J & Greenwald G 2013, 'France in the NSA's crosshair : phone networks under surveillance', *Le Monde*, 21 October. Available from www.lemonde.fr [5 November 2014].

that France has also been considered a NSA target when the UN Security Council was preparing a resolution about the sanctions on Iran.[1267]

Another Member State that has been collaborating closely with the US is Spain. The cooperation between the two was reinforced in 2001. Two months after the 9/11 attacks, the former president of Spain, José María Aznar, gave the green light to the US intelligence services to operate on Spanish soil. In return, Aznar requested advanced interception equipment from the US government for Spain's *Centro Nacional de Inteligencia* (CNI). The documents leaked by Snowden show that the NSA intercepted data from more than 60 million Spanish citizens in only one month.[1268] After the leak, the Spanish public prosecutor argued that such surveillance should take place without a prior court order. However, he added that it is especially complicated to learn more about the alleged violation since the interceptions are classified information and, consequently, the *Ministerio Público* has no access to them.[1269]

This analysis demonstrates that intelligence services of member states have individually consolidated a strong link with the US agencies. In return, the NSA equips all of these agencies with new technology and surveillance programmes.

### 3.4. EU reaction and consequences for the EU-US agreements

The Snowden disclosures put the spotlight on all of the current and future data-sharing agreements between the EU and the US. One of the main concerns of EU officials was that if data was collected by the NSA under Section 702 of FISAA then EU citizens had no redress mechanisms at all.

After the revelations, the former Vice-president of the Commission Viviane Reding sent a letter to the US Advocate General Eric Holder, asking several questions relating to the EU citizens' data that the NSA was gathering.[1270] Likewise, the Art. 29 WP pointed out some aspects about PRISM that needed to be clarified.[1271] In order to find more answers, the Commission and the US government decided to create a transatlantic

[1267] Greenwald 2014, p. 144.
[1268] Greenwald G & Aranda A 2013b, 'La NSA espió 60 millones de llamadas en España en solo un mes', *El Mundo*, 28 October. Available from www.elmundo.es [6 November 2014].
[1269] Peral M 2013, 'La fiscal pide el documento del espionaje de la NSA en España', *El Mundo*, 5 November. Available from www.elmundo.com [6 November 2014].
[1270] Video 'Viviane Reding: 'Data protection is a right', *Al Jazeera*, 12.10.2013. Available from www.aljazeera.com [6 November 2014].
[1271] Article 29 Data Protection Working Party, Letter to Viviane Reding, Ref. Ares(2013)2872799 – 13.08.2013.

group of experts: the ad-hoc EU-US Working Group on Data Protection. Also, at the national level, governments of the majority of member states launched initiatives to improve data security against intelligence services' intrusions.[1272]

Many aspects of the current version of the proposed EU Data Protection Regulation have been questioned since the disclosures. In particular, there are two provisions of the proposal that have been given special attention: ex Article 42 and Article 43a, suggested by the EP. Article 42 was included in the original draft of the proposal, leaked in December 2011, but it was later removed. Paragraph 1 stated:

'No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.'

That provision was commonly known as the 'anti-FISA clause'. The US authorities intensively lobbied for the removal of the clause before the official document was released. The US considered that the anti-FISA clause would impede public regulatory agencies from accessing the data necessary for investigations and thus hinder the EU-US cooperation.[1273] Consequently, Article 42 was removed from the draft.

Once the proposal was published, it was sent to the EP, particularly to the LIBE Committee, for inspection and the suggestion of amendments. The LIBE Committee made more than 4,000 amendments. Among them, it decided to include Article 43a, which has almost the same wording as the original Article 42. If Article 43a is finally added, the US authorities might have more difficulties in obtaining EU citizens' data through court orders, subpoenas, letters of request and letters rogatory.[1274] Also, companies could be sanctioned if they transfer data to the US authorities outside the scope of a MLA treaty or a specific international agreement, or without the approval of a data protection authority. However, the real impact of the provision is unclear,

[1272] Bryant & Fontanella-Khan, 2013; Kaufmann S 2013, 'Europe, Lost on the Digital Planet', *The New York Times,* 14 October. Available from www.nytimes.com [6 November 2014].
[1273] Federal Trade Commission, 'Informal Note on Draft EU General Data Protection Regulation', December 2011, p. 8.
[1274] Wiese Svanberg C 2014, 'The questionable legality and practicality of the EU's proposed anti-FISA clause', *Privacy Perspective*, 16 January. Available from https://privacyassociation.org [6 November 2014].

considering that member states' national security exclusion is maintained in the proposal.

Current EU-US agreements have also been affected by the Snowden revelations. One of the concerns referred to the Safe Harbour scheme, which was called for suspension by the EP. In 2000, the Commission adopted the Safe Harbour principles[1275] to solve the problem of the lack of a complete data protection framework in the US. The principles had the aim of complying with the adequacy requirement of Article 25 of Directive 95/46/EC. Today the scheme includes more than 3,000 certified companies based in the US. According to the agreement, US companies implementing Safe Harbour principles comply with the adequacy standards in the terms of Article 25 of Directive 95/46/EC. However, some controversies arose when it was found that at least 10% of the companies claiming membership to the Safe Harbour scheme were not actually listed there.[1276] Moreover, one of the NSA programmes disclosed, PRISM, showed that Safe Harbour did not prevent companies from transferring personal data to governments without EU approval.

After the revelations, the former Vice-president of the Commission Viviane Reding expressed concerns about Safe Harbour and issued recommendations in order to improve the legal framework.[1277] She noted that ironically '[t]he Safe Harbour may not be so safe after all'.[1278] Similarly, the Art. 29 WP released recommendations on the scheme in April 2014.[1279] For its part, the EP has taken a more drastic position calling for the immediate suspension of the scheme. That would be possible according to Article 3 of the Safe Harbor Decision. Yet, this option has been already discarded since the termination of Safe Harbor would most likely hinder the economy on both sides of the Atlantic.[1280]

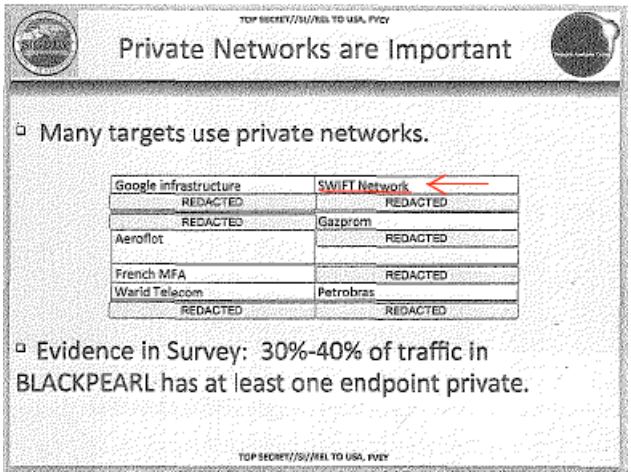
Safe Harbor continues to function for the moment. However, two EU actions might impact on the future of the agreement. On the one hand, the Commission will soon assess whether the US has taken into account the recommendations. Unfortunately, they have no binding effects. On the other hand, the CJEU is currently examining a

[1275] Decision 2000/520/EC. OJ L 215, 25.08.2000, pp. 7-47.
[1276] European Commission, COM(2013) 847 final, 27.11.2013, p. 7.
[1277] European Commission, COM(2013) 847 final, 27.11.2013.
[1278] Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, 'Towards a more dynamic transatlantic area of growth and investment', SPEECH/13/867, 29.10.2013, p. 6.
[1279] Art. 29 WP, Letter to Viviane Reding, Ref. Ares(2014)1139376, 10.04.2014.
[1280] US Surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation, PE524.633v01-00, *European Parliament, Working Document 4,* p. 3

preliminary ruling brought by the Austrian student Max Schrems on the data protection adequacy of Safe Harbour.[1281] After the annulment of the Data Retention Directive, some scholars have considered the possibility that the CJEU similarly invalidates the agreement.[1282]

The revelations have also raised concerns about the current SWIFT agreement. One of the documents disclosed by Snowden confirmed that SWIFT data have also been compromised:

*Figure 4.4.*




*Source: Greenwald 2014, p. 135*

This revelation was met with huge disappointment among EU institutions, especially the EP, which had long fought to achieve adequate data protection standards for SWIFT. Therefore, the EP called for the immediate suspension of the agreement.[1283] The MEP Jan Albrecht drafted an unofficial joint motion, pointing out that:

'Although the Parliament has no formal powers under Art. 218 of the TFEU to initiate a suspension or termination of an international agreement, the Commission will have to act if Parliament withdraws its support for a particular agreement.'[1284]

[1281] This is analysed in section 5.4 of this chapter.
[1282] Padova Y 2014, 'PRISM scandal threatens EU-US 'Safe Harbour' agreement', *EurActiv*, 12 November. Available from www.euractiv.com [14 November 2014].
[1283] 'MEPs call for suspension of EU-US bank data deal in response to NSA snooping', *Press Release, European Parliament*, 23.10.2013.
[1284] Joint Motion for a Resolution on the Suspension of the TFTP agreement as a result of NSA surveillance, European Parliament, 23.10.2013, para. 12.

Similarly, the former EU Home Affairs Commissioner Cecilia Malmstrom initiated formal consultations with the US as the first step towards a suspension of the agreement.[1285] The Belgian and Dutch Data Protection Authorities also investigated whether the NSA had been unlawfully accessing bank transaction data at SWIFT,[1286] but they finally concluded that there had been no violation.[1287] SWIFT and Europol officials arrived at the same result too.[1288] Therefore, the SWIFT agreement has not been suspended for the moment.

The EU-US PNR agreement has also been in the spotlight. The Joint Review for the implementation of the agreement stated that during 2012-2013 the DHS made twenty-three disclosures of PNR data to the NSA.[1289] However, the Joint Review stated that these were made on a case-by-case basis and according to the terms of the agreement. What the Joint review did not mention is that those EU citizens whose data were transferred to the NSA lacked judicial and administrative redress.[1290] It goes against the safeguards that the PNR agreement endorses. Therefore, if it is found that there has been a violation due to the lack of redress, the agreement could still be suspended, in accordance with the terms of Articles 24 and 25.

Finally, a few words on the expected Data Protection and Privacy Agreement (DPPA) between the EU and the US. As seen in Chapter 2 of this thesis, negotiations for the DPPA have suffered an immense delay. They officially started in March 2011 but they are still ongoing. The main reason why these negotiations are at a standstill is precisely the issue of judicial redress for EU citizens. The former Vice-president of the Commission Viviane Reding tried to include a clause on this issue during the negotiations, but the US kept blocking the EU demands. The Snowden revelations have brought some changes to the negotiations in this respect. The US, which has always been leading the decisions on the agreement, is now more willing to consider the EU suggestions on redress. In November 2013, Reding announced the US efforts to

[1285] Article 19 of SWIFT Agreement.
[1286] 'European Data Protection Authorities investigate bank data security. The Dutch and Belgian DPAs join hands for a security investigation of SWIFT', *Commission for the protection of privacy*, 13.11.2013.
[1287] 'Data protection authorities have not found any violations at SWIFT', *Press Release Dutch DPA,* 08.05.2013.
[1288] 'US Surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation', *European Parliament, Working Document 4,* PE524.633v01-00, p. 5.
[1289] European Commission, SEC(2013) 630 final, 27.11.2013, p. 16.
[1290] European Parliament, 2013/2188(INI), PE526.085v01-00, 23.12.2013, p. 14.

accelerate the completion of the agreement.[1291] The EP has also highlighted the importance that the DPPA incorporates a clause permitting EU citizens to enjoy judicial redress, irrespective of where they have their residence.[1292] Hence, it seems that the revelations have helped the EU negotiate the provision on judicial redress in the future proposal of the agreement.

In conclusion, trust needs to be rebuilt on both sides of the Atlantic. The revelations have clearly damaged the cooperation between the EU and the US in the field of privacy. As Reding pointed out 'We are not seen as partners, but as a threat'.[1293] The Snowden revelations do not only involve the NSA. Similar activities take place in intelligence agencies in the member states within the EU. For instance, most of the intelligence services in the EU do not require any prior judicial authorisation to get private information from foreign persons. This and other aspects are examined in the next section.

## 4. Systematic storage and access to data by intelligence services in the EU

The previous section has shown that intelligence services of the member states have maintained a close collaboration with the NSA. However, these intelligence services are also using massive surveillance programmes themselves, even if the information is not sent to the US. These programmes might violate the EU right to data protection, but due to their secrecy, it is not easy to get information about their actual functions and scope.

As seen in previous chapters, individuals of a Member State are able to go to the national and European police forces and request access to all information they keep about them. Yet, this right does not always exist for data collected and stored by intelligence services.

GCHQ in the UK has one of the most controversial legal frameworks in the EU. In 2013, the Interception of Communications Commissioner released a report stating that it

[1291] Video of Mrs. Reding speech, available from http://www.euractiv.com/video/eu-commissioner-reding-us-meetin-531789 [5 November 2014].
[1292] Baker J 2013, 'EU Parliament could block data sharing with the US', *CSO*, 19 November. Available from http://www.cso.com.au [6 November 2014].
[1293] Reding R 2013, 'Towards a more dynamic transatlantic area of growth and investment', SPEECH/13/867, 29 October, pp. 6-7.

is lawful for GCHQ to intercept communications and acquire communication data.[1294] Two laws regulate the GCHQ functioning: the Intelligence Services Act (ISA) 1994[1295] and the Regulation of Investigatory Powers Act (RIPA) 2000.[1296] The ISA sets rules about the warrant that the Secretary of State needs to give before certain actions. RIPA regulates all surveillance activities conducted by intelligence and law enforcement authorities. It establishes two types of interception warrants: the Section 8(1) warrants and the Section 8(4) warrants. They normally last six months and are authorised by the Secretary of State.

As for Section 8(4) warrants (also known as 'certified warrants'), they allow the intercepting of external communications and are issued by the Foreign Secretary. Debates have been raised because of the broad certificates given by the secretary.[1297] Section 8(1) warrants are required for the interception of content data stored in telecommunication service providers (TSPs). Yet, if GCHQ seeks to access traffic data hold by these service providers, an authorisation by a senior official is sufficient.[1298] RIPA also serves as the legal basis for surveillance carried out by GCHQ via satellites and fibre-optic undersea cables. Since it does not involve direct contact with the TSPs, there is no need to send them a notice in the sense of Article 33(4) RIPA. In fact, these interceptions are not authorised by a senior official, but they require Section 8(4) certificates issued by the Foreign Secretary.[1299] However, UK laws on intelligence services need to be tightened up, since many questions are still unanswered about these interceptions – for instance, it is unclear how domestic communications and foreign information are sorted out by the British intelligence services.[1300]

Besides the interception of communications, intelligence services in the UK may obtain information through voluntary disclosures by private entities. According to the Counter-Terrorism Act 2008, even if someone volunteers to disclose information to the intelligence agency, such information still needs to pass the tests of necessity and

---

[1294] 2012 Annual Report of the Interception of Communications Commissioner, HC 571 SG/2013/131, 03.07.2013. Available from http://www.statewatch.org/news/2013/jul/uk-ann-rep-interception-of-communications-2012.pdf [6 November 2014].
[1295] Intelligence Services Act 1994, 05.12.1994.
[1296] Regulation of Investigatory Powers Act 2000, 28.07.2000.
[1297] Bunyan T 2013, 'Interception Commissioner fails to report on Section 8(4) certificates authorising GCHQ's mass data collection', *Statewatch*. Available from www.statewatch.com [6 November 2014].
[1298] Article 22(3) RIPA.
[1299] Bunyan 2014; MacAskill E, Borger J, Hopkins N, Davies N & Ball J 2013, 'Mastering the Internet: how GCHQ set out to spy on the world wide web' 23 June. Available from www.theguardian.com [6 November 2014].
[1300] Article 16(3) RIPA; Heumann & Scott 2013, p. 9; Bunyan 2014, p. 12.

proportionality before it is processed by the agency.[1301] However, these criteria might be very ambiguous at times, since there is no judicial or independent body in control of the compliance.

Systematic processing of data is also present in the French intelligence services. In fact, due to its overseas territories, France possesses the technical infrastructure to operate a global interception system without cooperating with foreign countries.[1302] The French Code of Criminal Procedure was amended in 2011 in order to enhance law enforcement and intelligence services' powers for the collection of data. This law authorises practices such as the decryption of protected computer data, numeric infiltration and the enrolment of online chatroom conversations.[1303] Likewise, the so-called *Loi de Programmation Militaire* (LPM), adopted in December 2013, enables French secret services to intercept any communication if it is authorised by the Prime Minister. Many debates have emerged with regard to this law, since its individual safeguards, adequacy and collected categories of data are undetermined.[1304] Lastly, another systematic collection of French citizens' data comes from the *Direction générale de la sécurité extérieure* (DGSE). The DGSE systematically collects the electromagnetic signals launched by computers and phones within the country, as well as the communications between France and other countries.[1305]

The German Foreign Intelligence Services or *Bundesnachrichtendienst* (BND) are based on a law passed in 1990.[1306] This law authorises the BND to collect information from foreign communications and to request data obtained by TSP. Surveillance activities by German intelligence agencies are also regulated in the *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*, also known as G-10 law.[1307] The law has been highly controversial since it provides additional surveillance

[1301] Articles 19-21 of Counter-Terrorism Act 2008. See also Memorandum to the Home Affairs Committee. 'Post-legislative Scrutiny of the Counter-Terrorism Act 2008'. March 2014, p. 10.
[1302] 'Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))', A5-0264/2001 PAR1, European Parliament, 11.07.2001, p. 11.
[1303] 'The use of the Internet for terrorist purposes', United Nations Office on Drugs and Crime, September 2012, pp. 45-46 and 57.
[1304] Champeau G 2013, 'Les députés enverront-ils l'article 13 de la LPM au Conseil Constitutionnel?', *Numerama*, 11 December. Available from http://www.numerama.com/ [5 November 2014].
[1305] Follorou J & Johannes F 2013, 'Révélations sur le Big Brother français', *LeMonde*, 4 July. Available from www.lemonde.fr [6 November 2014]; 'No Warrant Internet Spying By French Authorities', *Edri*, 04.12.2013. Available from https://edri.org [6 November 2014].
[1306] Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG), 20 December 1990 (BGBI. I S. 2954, 2979).
[1307] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10), BGBl. I S. 1254, 2298, 26.06.2001.

powers to the BND, by limiting Article 10 of the German Constitution (protection of the privacy of correspondence, posts, and telecommunications). According to the supreme law, the BND can access letters and communications in order to avoid a) an armed attack, b) an international terrorist attacks, c) illicit foreign trade transactions in goods, data processing programmes and technologies, d) an unauthorised commercial shipment of narcotics into the EU, e) the impairment of monetary stability in the euro zone, f) international organised money laundering, and g) commercial organised smuggling of foreign persons in the territory of the EU.[1308] The BND monitors international communications (mostly e-mails) through the largest German Internet point 'DE-CIX', located in Frankfurt. The agency identified thirty-seven million communications in 2010 through DE-CIX, but the number was reduced after that year because the BND started to use other automatic filtering programmes.[1309]

Germany has established some limitations for the BND surveillance activities. The German Constitutional Court declared in 2008 that secret online searches of private computers by domestic intelligence services were unlawful, and stricter conditions were imposed after that.[1310] One of the changes was the amendment of G-10 Law in 2009,[1311] incorporating new safeguards and restrictions on surveillance. For instance, the collection of data about an untargeted individual's basic private life is now prohibited (Article 3a); the information on the private life of an individual that has been collected with no judicial supervision needs to be deleted (Article 5a); and new conditions have to be verified for the BND's transfer of intelligence to foreign public bodies (Article 7a). It confirms that data protection provisions are more visible in the G-10 Law than in other countries.

It can be concluded that intelligence services in member states often have a *carte blanche* to collect and process information and turn it into intelligence. Data collected does not only belong to EU citizens under suspicion or linked to criminal groups, but it includes data from innocent individuals too.

[1308] Article 5(1) G-10 Law.
[1309] Heumann & Scott 2013, p. 12.
[1310] Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 27 February 2008, reference number: 1 BvR 370/07.
[1311] Erstes Gesetz zur Änderung des Artikel 10-Gesetzes (1. G10uaÄndG k.a.Abk.), 30. Juli 2009 (BGBl. I S. 2437).

## 5. Could the EU set up data protection standards for the exchange of intelligence?

Two interesting points have been examined in this chapter so far: the first refers to the rupture of the EU-US confidence since the Snowden revelations. From the moment the NSA's programmes and practices were disclosed, current and future agreements between the two parties have been called into question, and some members of the EU institutions have even suggested suspending them. These drastic statements have borne fruit: We see now a more flexible US government, willing to adapt to the EU demands in the field of data protection.

The second interesting issue seen in the previous section is that intelligence services' activities might hinder the effective establishment of global data protection rules in the field of security. Intelligence services, unlike law enforcement, are only regulated at the national level. There are no EU laws regulating the information processed by these bodies. As a result, EU data protection rules can be circumvented via intelligence services. This is particularly alarming if we bear in mind that the division of tasks between intelligence services and law enforcement authorities is becoming very diffuse today.

Taking all this into account, the third and final issue this chapter will examine is the possibility to approximate and harmonise EU data protection rules that affect national intelligence services, especially those provisions relating to individual safeguards and rights. These norms should not clash with articles 4(2) TUE and 72 TFEU, which state that the adoption of laws on the safeguarding of national security is the responsibility of each Member State.

### 5.1. Lack of coordination of intelligence services within the EU

All member states except for Ireland[1312] have their own intelligence agencies, which act according to their specific domestic laws.[1313] Intelligence agencies collect and analyse the data they deem necessary and, once it becomes intelligence, it is forwarded to national governments.

[1312] Functions of national security in Ireland are fully conducted by police forces. See W215, 10.04.2014, p. 9.

[1313] Yet, not all member states have the same level of experience as regards the collection and analysis of intelligence. Mai'a K. Davis Cross explains that the UK, Spain, and Germany have a lot of experience in the intelligence sector whereas newer member states like Poland and Slovenia are relatively inexperienced. See Cross 2013, p. 391.

Espionage practices in Europe have their origins in ancient civilisations. Several historians of Greek and Latin civilisations have found documents revealing episodes of espionage during these periods. In the Middle Ages, such practices were improved by the inclusion of diplomatic services within governments, and the practice gradually developed over the centuries until the institutionalisation of intelligence services, and new forms of data collection and processing through cryptographic techniques became available. During the 20th century, espionage became an extremely entrenched practice among European governments, who took advantage of the developments in signals intelligence technology that were made during that period. The First and Second World Wars, the civil wars in some European countries, and the period of the Cold War were all characterised by the important role of secret services in gathering intelligence and counterintelligence related to rival countries. In contrast, the nineties was a somewhat quiet decade for the intelligence centres. This is precisely why 9/11 came as such a shock.

The attacks of 11 September 2001 caused a revolution in the global intelligence society. Terrorists communicate globally and use all types of Internet services (email accounts, fora, social media, VoiP systems, etc.). Consequently, intelligence activities are no longer conducted at a state-to-state level, and coordination among public and private actors around the world is increasing. In particular, the US and the EU embarked on a significant joint effort to improve the coordination among its national communication systems by establishing a common political authority.[1314]

Austria and Belgium suggested the creation of a CIA-style agency in the EU, but the other member states did not support that initiative.[1315] Nevertheless, two new bodies were established after the 9/11 attacks: The Counter-Terrorism Group (CTG) and the Intelligence Analysis Centre (IntCen). The CTG is a forum composed of the parties of the 'Berne Club', namely, all EU member states plus Switzerland and Norway. Their heads of security and intelligence services meet regularly in order to discuss data and analyses related to terrorism (mostly Islamic extremist terrorism) and to develop periodic threat assessments.[1316] IntCen is the evolution of a previous European centre called Joint Situation Centre (SitCen). SitCen was created by the former High Representative of the CFSP Javier Solana one year before the 9/11 attacks, and it had

[1314] Moret Millás V 2005, 'El Centro Nacional de Inteligencia: Un aproximación a su régimen jurídico', *Foro Nueva época*, no. 2, p. 264.
[1315] Bures & Ahern 2007, p. 217.
[1316] Occhipinti 2013, pp. 158-159.

three departments: the Operations Unit, the Analysis Unit and the Consular Unit. However, it did not tackle counter-terrorism issues at first.

After the attacks, SitCen enhanced its scope in order to examine internal and external threats related to terrorism and other serious crimes.[1317] There were other attempts to improve SitCen capabilities after the attacks in Madrid (2004), London (2005), and Oslo (2011).[1318] For instance, in 2005 the Analysis Unit established links with the CTG, which started to influence EU decisions on internal security matters.[1319] SitCen also recruited seconded analysts from member states and internal security services,[1320] and it began to provide strategic reports to the Council of the EU and to member states. These reports are usually in the form of signals intelligence (SIGINT),[1321] human intelligence (HUMINT) and imagery intelligence (IMINT).[1322]

In April 2012, the EU re-named the body as 'IntCen'. IntCen's legal basis is not completely clear. The only mention of the centre is found in the Annex of EEAS Council Decision.[1323] Although not all EEAS instruments are part of the CFSP,[1324] IntCen would probably fall under its scope. In that case, the current High Representative of the CFSP Federica Mogherini would be in charge of the centre. The other possibility is that IntCen uses Article 73 TFEU as its main legal basis. This provision does not belong to the CFSP, but to the AFSJ. This proves, once more, that the boundaries between the CFSP and the external dimension of the AFSJ are ambiguous. Moreover, IntCen does not only deal with external security matters, but it also carries out EU internal security functions. For instance, it cooperates with Europol and it drafts reports that it then sends to the Commission and the Council.[1325] Therefore, the legal basis of the centre needs to be clarified. In that sense, in December 2013 the EP urged the

---

[1317] Occhipinti 2013, p. 160.
[1318] On 21 July 2011, Anders Behring Breivik detonated a bomb in Oslo and subsequently killed 77 (mostly young) people on the island of Utoya.
[1319] Mills M, Vermeulen M, Born H, Scheinin M, Wiebusch M & Thornton A 2011, 'Parliamentary oversight of security and intelligence agencies in the European Union', *European Parliament-Directorate General for Internal Policies, Policy Department c: Citizens' rights and Constitutional Affairs*, Brussels, pp. 54-55.
[1320] Busuioc M & Groenleer M 2013, 'Beyond Design: The evolution of Europol and Eurojust', *Perspectives on European Politics and Society*, vol. 14 no. 3, p. 294.
[1321] Particularly from France's satellites Helios and Pleiades, Germany's satellite SAR-Lupe and Italy's satellite Cosmo-SkyMed,
[1322] Council of the European Union, 17303/1/10 REV 1, 03.12.2010; Svenden 2011, p. 536.
[1323] OJ L 201, 03.08.2010, pp. 30-39.
[1324] For instance, EEAS measures outside of the scope of CSFP tackle issues related to the neighbourhood policy, development, financial matters, the external dimension of human rights, environment, transport, etc.
[1325] Council of the European Union, 12243/14, 30.07.2014, p. 2.

Commission to present a proposal for a legal basis for the activities of IntCen.[1326]

IntCen has recruited military intelligence and police analysts from member states in order to increase the cooperation among national intelligence services.[1327] The tasks of the new IntCen have been viewed with optimism by scholars.[1328] Yet, the reality is that the competences of the centre are still very small, in comparison with those of a regular intelligence centre. In fact, the EEAS has made it very clear that IntCen is not an intelligence service, since the centre mainly provides information on crisis management situations. In addition, it does not have information collection powers or any operational role, and it only shares assessed intelligence among member states, as well as with EU institutions and bodies.[1329]

IntCen has achieved a certain degree of intelligence integration within the EU. Some Open-source (OSINT) partnerships have been consolidated among some member states like Germany, Denmark, the Netherlands, the UK, Italy, Austria, Sweden, Norway, France and Belgium.[1330] Member states have discretionary powers on the decision of whether to share information with the centre or not. In this sense, there is still a low level of political will among member states to cooperate with the IntCen, and they are often resistant to share intelligence with the centre.[1331] Consequently, the 80% of the intelligence stored by IntCen comes from only four EU-countries.[1332]

There are many reasons why member states are reluctant to share intelligence among each other. First, they do not always trust how other agencies are going to use the intelligence. They are very cautious about the risk of manipulation if they forward it. Likewise, they are often concerned about free-riding from others, or the loss of privileged influence if the intelligence circulates beyond the country. In addition intelligence services in the EU seek to establish a close link with the US government. Sometimes, they simply decide not to share information with other EU countries to maintain the privilege of enjoying a close cooperation with the US.[1333] Another reason for this lack of cooperation is the fact that there are no clear boundaries of what information should be collected by law enforcement authorities and what is to be

[1326] European Parliament, 2013/2188(INI), PE526.085v01-00, 23.12.2013, p. 25.
[1327] Cross 2013, p. 289.
[1328] Svenden 2011; Fägestern 2014.
[1329] Mills et al. 2011, pp. 55-56.
[1330] Svenden 2011, p. 529.
[1331] Cross 2013, pp. 288 and 400; Archick 2013, p. 3.
[1332] Nielsen N 2015, 'No new mandate for EU intelligence centre', *EUobserver*, 6 February. Available from https://euobserver.com/justice/127532 [18 February 2015].
[1333] Cross 2013, p. 390.

obtained by intelligence services. In order to regulate these synergies between police and intelligence forces, in 2008 the Council suggested establishing networks of anti-terrorist centres in all member states, as well as enhancing the role of IntCen.[1334] Eight years on, this recommendation is still on the table.

### 5.2. Divergence in the oversight over intelligence agencies

In 2001, the EP released an analysis of the activities conducted by intelligence authorities.[1335] Intelligence services are characterised as having a secretive nature and for collecting a large volume of data. The report highlighted the difficulties for evaluating the effectiveness of their activities, as well as their compliance with the laws. In particular, one of the recommendations made was the establishment of an appropriate legal and parliamentary supervision over secret services in all member states.

Today most (but not all) intelligence services within the EU borders are monitored by oversight bodies. Yet, these supervisory bodies are not all alike. They have different tasks and features depending on the Member State. Particularly, three main types of control are identified within the EU: i) executive control, ii) parliamentary control; and iii) (quasi) judicial control. Sometimes this control will be *ex ante*, and sometimes it will be *ex post*. This section examines the intelligence oversight in France, Germany, Spain and the UK.[1336]

The executive (or non-parliamentary) control is found in the British, German and French oversight regimes. Concerning the British legal framework, RIPA states that interception by intelligence services in the UK[1337] needs to be authorised by the Secretary of State. The Secretary issues surveillance warrants as long as the interception is proportionate and necessary.[1338] In addition, such interception needs to pursue one of the following purposes: a) national security, b) the prevention or detection of serious crimes, c) the safeguard of the economic well-being of the UK, and d) giving effect to

[1334] Council of the European Union, 11657/08, 09.07.2008, p. 38.
[1335] 'Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))', A5-0264/2001 PAR1, European Parliament, 11.07.2001.
[1336] For an extended comparative analysis on the oversight of national intelligence agencies see Aidan Mills et al. 2011, pp. 84-145 and 191-411.
[1337] Intelligence services in the UK include the GCHQ, the National Criminal Intelligence Service (NCIS), the Security Service or MI5 (SS) and the Secret Intelligence Service or MI6 (SIS).
[1338] Article 5(2) RIPA. Bunyan notes in his article that the 'Snowden revelations have shown that in this context the concepts of "minimum" and "necessary" have no limits'. Bunyan 2014, pp.17.

the provisions of any international mutual assistance agreement.[1339] In Germany, the BND has an obligation to report all activities to the Chancellery, the Ministry of Interior and the Ministry of Defence. At the same time, these bodies will report the activities to the *Parlamentarisches Kontrollgremium* (PKG). Moreover, the G-10 Law obliges the BND to get the Chancellery's approval before sharing information with any foreign intelligence agency.[1340] Finally, in France procedures consisting of tapping cables require political authorisation from the Prime Minister.[1341]

Control through parliamentary committees is the most usual oversight system within the EU. Classical parliamentary control consists of organising regular meetings in which several questions are posed to the Ministers. Although Ministers have the obligation to answer the queries, in practice they can decline to by arguing that it would jeopardise the national security of the country.[1342] The four countries chosen for this study have a parliamentarian system that supervises national intelligence services. They have chosen this type of control because of the idea that, since intelligence services are a political tool of the government, the control must originate in the government too.[1343]

In the UK, the Intelligence and Security Committee of Parliament (ISC) is the parliamentary body in charge of the British intelligence community. The oversight is *ex-post facto*. The ISC publishes annual reports and supervises that the agencies comply with their tasks, budget, effectiveness and limitations.[1344] However, as pointed out by a member of the ISC, the Committee also experiences some shortcomings in its supervisory activities.[1345] The Interception Communications Commissioner's Officer has also ex-post auditing tasks. It has access to any information from intelligence services and law enforcement authorities and it releases recommendations for such agencies afterwards.[1346] However, there are numerous limitations in its oversight. For instance, the body cannot always be fully transparent because of the confidentiality

[1339] Article 5(3) RIPA.
[1340] Article 7a G-10 Law
[1341] Article 4 of the Loi n° 91-646 du 10/07/1991, Contrôle de l'application de la loi relative au secret des correspondances émises par la voie des télécommunications.
[1342] For this reason, parliamentary commissions have been seen as inefficient by part of the doctrine. See, for instance, Aranda Álvarez E 2003, 'Servicios de inteligencia: Un estudio comparado' in *Estudios sobre inteligencia: Fundamentos para la seguridad internacional*, Grupo de Trabajo número 5/03, Instituto Español de Estudios Estratégicos, p. 100.
[1343] Ruiz Miguel C 2007, 'Problemas actuales del derecho de los servicios de inteligencia', *Inteligencia y Seguridad: Revista de Análisis y Prospectiva,* no.2, pp.13-46.
[1344] Heumann & Scott 2013, pp. 9-10.
[1345] Rifkind M 2014, '*Intelligence agencies in the Internet age - Public servants or public threat?*', Wadham College, Oxford, p. 8.
[1346] In 2014, it released 350 recommendations. Speech by Joana Cavan, Interception Communications Commissioner's Officer, CPDP2015, Brussels, 23.01.2015.

agreements it needs to sign. Also, it is not always easy to reach an effective remedy, and errors and breaches are difficult to identify.

France did not implement a parliamentary oversight over intelligence services until 2007. That year the country passed a law[1347] establishing the *Délégation parlementaire au renseignement* (DPR). However, the DPR has numerous limitations. For instance, this institution has no right to conduct investigations and it is not disclosed the details of the operational activities conducted within the centre.[1348] There are other oversight bodies in France, like the *Autorités Administratives Indépendantes,*[1349] but their powers are also very small. In December 2013, the French Government approved the Defence Bill 2014-2019, which enhances electronic surveillance for French residents.[1350] Yet, it does not establish changes on intelligence oversight.

The German Constitution (GG) states in Article 45(d) that the German Parliament or *Bundestag* can establish special committees to scrutinise intelligence activities of the Federation. The aforementioned G-10 Law foresees in Article 5 that intelligence services will be subject to parliamentary control by two different institutions: The *Parlamentarisches Kontrollgremium* (PKG) and the *G-10 Kommission*.

The PKG's tasks are described in the Law on the Parliamentarian Control of Intelligence Services of 2009 (PKGrG).[1351] It oversees the *Bundesnachrichtendienst* (BND), the *Militärischer Abschirmdienst* (MAD) and the *Bundesamt für Verfassungsschutz* (BfV) and it is composed of up to ten members set by the *Bundestag* at the beginning of each mandate. The German government has an obligation to inform the committee about the general activities of the intelligence services, as well as the most relevant ongoing operations at least once every six months. The committee also supervises the annual budget plan of the centres (Article 9(2) PKGrG) and it can even ask for a report on specific issues. Meetings are secret and closed-doors and they take place every three months on average (Article 3 PKGrG). All the information is then

[1347] Loi n° 2007-1443 du 9 octobre 2007, JO nº 235 10.10.2007.
[1348] Mills et al. 2011, p. 210.
[1349] Wolf C 2013, 'Is personal data better protected from government surveillance in Europe than the U.S.? Maybe not, *IAPP*, 20 June. Available from www.privacyassociation.com [4 November 2014].
[1350] Texte adopté nº 251, Projet de loi relatif à la programmation militaire pour les années 2014 à 2019et portant diverses dispositions concernantla défense et la sécurité nationale, 3.12.2013. See also Sayare S 2013, "France Broadens Its Surveillance Power", *The New York Times,* 14 December. Available from www.nytimes.com [6 November 2014].
[1351] Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumgesetz - PKGrG), BGBl. I S. 2346, 09.07.2009.

transferred to the *Bundestag*, which will ultimately decide whether the German government has complied with its obligations or not (Article 13 PKGrG).

The other parliamentary control over German intelligence services is the 'G-10 Commission', which is appointed by the PKG. The G-10 Commission was created by the *Bundestag* in light of the constitutional right to privacy of correspondence, posts and telecommunications of Article 10 GG. It comprises members of the *Bundestag*, who are in charge of deciding on the permissibility and necessity of surveillance activities conducted by German intelligence agencies.[1352] The objectives and functions of the G-10 Commission are regulated in Article 15 of the G-10 Law. Members meet at least once a month and they control that the agencies' collection, processing and storage of personal data is adequate. The G-10 Commission has access to any information it deems necessary, and it examines complaints issued by citizens on potential surveillance abuses. In contrast to the rest of the intelligence services analysed in this study, the BND offers the possibility for individuals to request access to their data.[1353] Although the agency can always reject the request if there is an ongoing investigation, this right offers better safeguards for Germans than for the citizens of the three other member states.

It is worth adding as for the German oversight intelligence framework that, after the Snowden revelations, the German Bundestag established a temporary Committee of Inquiry for the investigation of mass surveillance activities by the German secret service and its cooperation with the NSA. The committee was unanimously voted in by all parties in the parliament, and it is composed of eight members: four conservatives, two social-democrats, one socialist and one from the green party. It is a temporary committee and it is expected to be operational until 2017. The committee is conducting interviews with expert witnesses in the fields of national law, international law and technology. It also examines technical issues regarding the intervention of communications by intelligence agencies in Germany. Yet, this committee does not have access to documents that involve other intelligence services (e.g. documents related to '5-Eyes'), and its contact with Edward Snowden has been restricted.[1354]

---

[1352] G-10 Statute, Article 15(5); Schwartz PM 2012, 'Systematic government access to private-sector data in Germany', *International Data Privacy Law*, vol. 2, no. 4, p. 297.
[1353] Heumann & Scott 2013, pp. 13-14.
[1354] Speech of Anne Roth, member of the NSA Inquiry Committee of the German Bundestag, at CPDP2015, Brussels, 23.01.2015.

Similar to the British, French, and German systems, the Spanish Parliament is the institution controlling the activities of the *Centro Nacional de Inteligencia* (CNI). Article 11 of the Law 11/2002[1355] details the procedure for this control, which requires the appointment of the so-called *Comisión de Secretos Oficiales* (or Secret Funds Committee), as part of the Congress. This Committee has access to most of the classified information in the CNI.[1356] It also oversees that the budget provided to the centre is not misused.

The UK, Germany and Spain have established judicial oversight over intelligence services. The British intelligence community is monitored by a) the Independent Reviewer of Terrorism Legislation, b) the Interception of Communications Commissioner (ICC), c) the Intelligence Services Commissioner (ISC) and d) the Investigatory Powers Tribunal. The current Independent Reviewer of Terrorism Legislation is David Anderson. He is not part of the government and is in charge of issuing reports and recommendations about the functioning of the British intelligence community to ministers and the Parliament.[1357] The ICC and the ISC provide independent quasi-judicial oversight *ex post* and they are appointed by the British Prime Minister.[1358] The ICC supervises warrants issued for the interception of communications[1359] and the disclosure of communications data.[1360] In contrast, the ISC controls the adequacy of warrants issued by the Secretary of State authorising intrusive surveillance. Both commissioners give assistance to the Investigatory Powers Tribunal when it is required for an ongoing investigation. The Investigatory Powers Tribunal is composed of nine senior members who hear complaints related to illegal surveillance. However, this tribunal has a very opaque nature: because it is not an independent judicial body,[1361] it cannot initiate investigations in its own, and its decisions are mostly secret.[1362]

---

[1355] BOE núm. 109, 07.05.2002.
[1356] Article 7(1) of the Secret Funds Act, Article 11(2) Law 11/2002.
[1357] For further information, see https://terrorismlegislationreviewer.independent.gov.uk [6 November 2014].
[1358] Articles 57 and 59 RIPA.
[1359] Chapter 1-Part 1 of RIPA.
[1360] Chapter 1-Part 2 of RIPA.
[1361] Bickford D 2013, 'Judicial Scrutiny of Intelligence Agencies', European Parliament LIBE enquiry, 7 November. Available from <www.europarl.europa.eu> [6 November 2014].
[1362] Heumann & Scott 2013, p. 9.

German intelligence services are also subject to judicial control, but only if basic rights are infringed.[1363] This judicial review has a limitation: Article 99(1) of the Code of Administrative Court Proceedings (VwGO) allows specific files or electronic documents to be classified as secret if they affect the interests of the Federation or the *Land*.

As far as the Spanish regime is concerned, since 2002 the CNI is subject to judicial oversight under the basis of Organic Law 2/2002.[1364] According to Article 12 of Law 11/2002 and the single Article of LO 2/2002, the Spanish Supreme Court can rule on cases regarding the infringement of the right to inviolability of the home and the secrecy of communications (Articles 18(2) and (3) of the Spanish Constitution). If CNI activities clash with any of these constitutional rights, they require prior authorisation from a judge. When a court order is requested, the judge must verify that such activity is necessary for the goals assigned. Article 12 of Law 11/2002 must be read in conjunction with Article 74(a) of the CNI Statue, which establishes an obligation for the agency to act according to the Spanish Constitution and the rest of the national laws.[1365] Yet, even if this is the formal procedure to get information in Spain, the CNI has sometimes circumvented the prior authorisation from a judge.[1366]

It can be thus concluded that there are no common rules on oversight for data protection issues over intelligence services within the EU. From the analysis above it has been seen that some national systems are very lax (e.g. France), whereas others are highly protective. Therefore, minimum standards on oversight in all member states would improve the data protection for the information processed by intelligence services. Regarding the ideal control system, some scholars have seen many advantages in having an executive or non-parliamentary control,[1367] whereas others opt for a dual parliamentary and judicial mechanism.[1368] For instance, the EP has suggested a two-fold system: An *ex-ante* control by an independent magistrate, and an *ex-post* parliamentary

[1363] Article 19 GG.
[1364] BOE núm. 109, 07.05.2002.
[1365] Real Decreto 240/2013, de 5 de abril, por el que se aprueba el Estatuto del personal del Centro Nacional de Inteligencia. BOE Núm. 89, 13.04.2013.
[1366] Documentary 'Salvados', 17.11.2013.
[1367] Mills et al. 2011, pp. 90-91.
[1368] Hillebrand 2012, pp. 44-57.

oversight.[1369] For its part, the Art. 29 WP suggests making national DPAs responsible for supervising the activities of the intelligence services.[1370]

In my view, the ideal situation would be to adopt one single instrument with common oversight rules for intelligence services in all member states. This could only occur if an EU legal basis for such development was effectively established. In that case, the EU rules would operate as a lowest common denominator in all member states. Since parliamentary oversight is the predominant system among member states – at least 18 out of the 28 member states have implemented parliamentary committees,[1371] this could be the nature of the system. Any executive or judicial scrutiny would have a complementary role. Parliamentary committees would have access to all classified information (with the appropriate security clearance)[1372] and they would oversee that the intelligence services' activities conform to the law and effectiveness criteria. Naturally, it is not a perfect mechanism, since these parliaments would lack sanctioning powers,[1373] and there would be a risk of having too many parliamentary bodies involved in the scrutiny procedures.[1374] However, a single instrument could never be adopted today, since the EU has no legal basis to regulate oversight mechanisms for national intelligence services.

### 5.3. Current challenges at the CJEU and the ECtHR

As seen above, Article 4(2) TEU excludes national security matters from the competences of the EU so, according to this provision, national security issues are beyond the scope of the Charter of Fundamental Rights' scope and the CJEU jurisdiction, too.[1375] As for the Charter, Article 51 states that this is only applicable to EU citizens to the extent that member states are implementing EU laws. Regarding the CJEU, Article 276 TFEU establishes:

---

[1369] Democratic oversight of Member State intelligence services and of EU intelligence bodies, *European Parliament, Working Document 5*, 12.12.2013, p. 5.
[1370] It is already happening in thirteen EU member states. These are Austria, Belgium, Cyprus, Estonia, Finland, France, Germany, Ireland, Italy, Latvia, Luxembourg, Poland and Sweden. See WP215, 10.04.2014, p. 10.
[1371] See Table 1 in Mills et al. 2011, pp. 92-95.
[1372] Today there is also a disparity in terms of the information that overseers can access during the scrutiny of national intelligence services. See Tables 3 and 4 in Mills et al. 2011, pp. 119, 127-128.
[1373] Hillebrand 2012, p. 48.
[1374] 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin', *United Nations, General Assembly*, A/HRC/10/3, 04.02.2009, para. 46.
[1375] Korff 2014, p. 35.

'The Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.'

In accordance with that article, the Court has no competence to examine preliminary rulings on operations undertaken by law enforcement authorities for the maintenance of 'internal security' (here equivalent to 'national security').[1376] Nonetheless, there is still one issue under review by the CJEU within the field of public order and the safeguarding of internal matters: the compatibility of national security measures with EU law. The CJEU has reiterated that even if member states retain exclusive competence on certain security measures, the Court can verify if these are appropriate and conform to the EU treaties.[1377]

As mentioned above, a definition of what national security covers is urgently required. In this regard, Germany has recently suggested clarifying the concept of internal security 'in order to avoid overlapping with tasks assigned to intelligence services in order to protect the security of the State from internal threats'.[1378] The CJEU has stated that 'public security' encompasses both internal and external security.[1379] Yet, it is uncertain whether the term 'public security' is equivalent to that of 'national security'. The Court should thus demarcate the scope of Articles 4(2) TEU and 72/73 TFEU, similar to the rulings on the production and trade in arms, munitions and war material. In the field of defence procurement, the Court has always maintained a strict interpretation of Articles 346(b) and 347 TFEU.[1380] Likewise, a clear list on the specific national security measures should be established. This list would make it easier to determine whether certain operations carried out by intelligence services go beyond

[1376] For a criticism on this provision, see Hinarejos A 2011, 'Law and order and internal security provisions in the Area of Freedom, Security and Justice: before and after Lisbon' in *Crime within the AFSJ*, eds. Christina Eckes and Theodore Konstadinides, Cambridge University Press, Cambridge, pp. 270-271.
[1377] See case C-265/95 Commission v. France ('Spanish Strawberries') [1997] ECR I-6959, para. 33-35, 56-57; and case C-124/95 The Queen, ex parte Centro-Com Srlv. HM Treasury and Bank of England [1997] ECRI-81, para. 25.
[1378] Council of the European Union, 15659/1/14 REV 1, 19.11.2014.
[1379] Case C-285/98 Tanja Kreil v Bundesrepublik Deutschland [2000] ECR I-69, para. 17.
[1380] Koutrakos P 2013, 'The EU common security and defence policy', Oxford University Press, Oxford, p. 257-278.

national security purposes. If so, the EU principles would still apply for those operations.[1381]

In fact, a case that indirectly affects intelligence services is now being examined by the CJEU. The case was brought to the Irish High Court by the Austrian student Max Schrems in June 2014. After the Snowden disclosures on PRISM, the applicant claimed to the Irish DPA that data transfers between Facebook Ireland and Facebook Inc. had to cease. The DPA maintained that the company fulfilled Safe Harbour principles and, therefore, there was no reason for a suspension.[1382] The Irish High Court referred the case to the CJEU, asking whether the Irish DPA is obliged to investigate a complaint in relation to the transfer of personal data by Facebook to the US.[1383] The case will indirectly examine the lawfulness of PRISM in light of Article 8 of the Charter, Directive 95/46/EC and the 2000 Safe Harbour Decision.

Besides the Charter, any EU citizen can invoke Article 8 of the ECHR (right to respect for privacy and family life) against intelligence services' practices, as long as they have exhausted the national remedies. Although it is an exclusive competence of the member states to legislate on national security matters, as Contracting Parties of the ECHR, national laws cannot violate the clauses of the Convention. Moreover, according to Article 52 ECHR, the Secretary General of the Council of Europe can *ex officio* request information from the member states in order to verify that they are complying with the provisions of the Convention. In January 2015, the Secretary announced that he would use these powers to obtain information about the intelligence services' activities of the Contracting Parties.[1384]

The ECtHR has dealt with numerous cases concerning mass surveillance activities that clashed with Article 8 ECHR. According to the Court's jurisprudence, the interference could occur even when the information is available in the public domain,[1385] when police install covert listening devices in someone's home,[1386] and when a national

[1381] Korff 2014, p. 41.
[1382] Schrems -v- Data Protection Commissioner, [2014] IEHC 310, 18.06.2014.
[1383] Reference for a preliminary ruling from High Court of Ireland (Ireland) made on 25 July 2014 – Maximillian Schrems v Data Protection Commissioner (Case C-362/14).
[1384] Council of Europe, Parliamentary Assembly, Committee on Legal Affairs and Human Rights Mass surveillance Report, Rapporteur: Mr Pieter Omtzigt, AS/Jur (2015) 01, p. 2.
[1385] Segerstedt-Wiberg and Others v. Sweden, Application no. 62332/00, Judgment of 6 September 2006; Rotaru v. Romania, Application no. 28341/95, Grand Chamber judgment of 4 May 2000; Shimovolos v. Russia, Application no. 30194/09, judgment of 28 November 2011.
[1386] Khan v. the United Kingdom, Application no. 35394/97, judgment of 4 October 2000; PG. and J.H. v. the United Kingdom, Application no. 44787/98, judgment of 25 December 2001; Copland v. the United Kingdom, Application no. 62617/00, judgment 3 April 2007.

judge or a public prosecutor issues certain wiretapping orders.[1387] The Court has likewise concluded that mass surveillance activities can only be used as long as they pursue a relevant national security interest.[1388]

The majority of cases brought before the ECtHR refer to police surveillance activities, but the Court has examined intelligence services' practices too. For instance, the case *Association 21 December 1989 and others* v. *Romania* dealt with surveillance activities of anti-government demonstrators by the Romanian Secret Service.[1389] Likewise, in the cases *Klass and others* v. *Germany*[1390] and *Weber & Saravia* v. *Germany*[1391] the Court examined whether the G-10 Act in Germany was contrary to the Convention.

There are currently two pending applications issued by British and Hungarian citizens before the ECtHR. As for the Hungarian application, it challenges the practices conducted by the Hungarian Anti-Terrorist Centre (TEK), which includes intelligence and law enforcement authorities. Hungarian citizens have claimed that TEK is allowed to spy on them with no prior court order.[1392] In the UK, several British activists lodged an application before the ECtHR in September 2013. They argued that the use of GCHQ programmes like PRISM and Tempora (which have no legal basis in UK laws) was in breach of Article 8 of the Convention.[1393] However, the right to privacy of Article 8 is not absolute, and governments can conduct surveillance as long as it is 'necessary' and serves a 'legitimate aim' (Article 8(2)). In previous cases,[1394] the ECtHR has stated that national laws allowing data processed by member states need to specify the offences and categories of persons monitored; the duration for the surveillance; its purpose; and

---

[1387] Kruslin v. France, Application no. 11801/85, judgment of 24 April 1990; Amann v. Switzerland, Application no. 27798/95, judgment of 16 February 2000; Wisse v. France, Application no. 71611/01, judgment of 20 December 2005; Vetter v. France, Application no. 59842/00, judgment of 31 May 2005; A. v. France Application no. 14838/89, judgment of 23 November 1992; Uzun v. Germany, 2.9.2010, Appication no. 35623/05, judgment of 2 September 2010; Malone v. UK, Application no. 8691/79, Judgment of 2 August 1984; Pruteanu v. Romania, Application no. 30181/05, Judgement of 3 February 2015.

[1388] Segerstedt-Wiberg and Others v. Sweden, Application 62332/00, judgment of 6 September 2006; Klass and others v. Germany, Application 5029/71, judgment of 6 September 1978, paragraph 48; Marper v United Kingdom, Application no. 30562/04 and 30566/04, judgment of 4 December 2008.

[1389] Application no. 33810/07 and 18817/08, judgment of 24 May 2011.

[1390] ECtHR, Application no. 5029/71, judgment of 6 September 1978.

[1391] ECtHR, Application no. 54934/00, judgment of 29 June 2006.

[1392] ECtHR, Mate Szabo and Beatrix Vissy v. Hungary, Application no. 37138/2014, 13.5.2014.

[1393] ECtHR, Big Brother Watch, Open Rights Group, English PEN and Kurz v. the United Kingdom, Application no. 58170/13, 4.9.2013.

[1394] See, for instance, ECtHR Klass v. Germany (1978), Liberty and Others v. the UK (2008); S and Marper v United Kingdom (2009); Gillan and Quinton v United Kingdom (2010); Kennedy v. UK (2010); and Brunet v. France (2014).

the oversight mechanism. Moreover, Contracting Parties have a positive obligation to ensure that private companies do not cooperate in abusive surveillance activities.[1395]

In general, no application could be admitted before the ECtHR if national court instances have not been exhausted first. However, in that particular case, the ECtHR has admitted the application without it first being examined by the Investigatory Powers Tribunal, since that tribunal does not afford an effective remedy due to its particularly secretive nature.[1396] A court decision for both the Hungarian and the British applications is still pending.

Because of the limited redress that individuals have at the European level against mass surveillance activities, some of them have opted for initiating national procedures instead. In this sense, proceedings started in 2014 in German, French and British courts about the lawfulness of the PRISM programme. On 3 February 2014, three German NGOs[1397] lodged a criminal complaint before the German courts against the NSA and GCHQ about 'mass surveillance, illegal covert intelligence activities, violations of the basic rights to privacy, and obstruction of justice by tolerating and supporting illegal surveillance of German citizens'.[1398] In August 2014, in France, The International Federation for Human Rights (FIDH) and the French Human Rights League (LDH) filed a complaint before the *Tribunal de Grande Instance de Paris*.[1399] In the UK, Privacy International issued a complaint before the UK's Investigatory Powers Tribunal (UKIPT) on 13 May 2014, challenging the use of hacking tools (particularly, Upstream and PRISM) by the British intelligence services.[1400]

The only court that has issued its decision to date is the UKIPT. The tribunal stated in December 2014 that the interception of the claimants' communications did not contravene Articles 8 and 10 ECHR and, therefore, no breach had been committed.[1401] However, in February 2015 the UKIPT clarified that before the PRISM and Upstream

---

[1395] Korff 2014, p. 33.

[1396] Letter of the ECtHR accepting the case, 16 January 2014, available from https://www.privacynotprism.org.uk/assets/files/privacynotprism/letter_from_ecthr_to_uk_gov.pdf [16 November 2014].

[1397] The International League for Human Rights, Chaos Computer Club (CCC) and Digitalcourage.

[1398] 'German govt and intelligence agencies face penal charges for spying', *EDRi-gram newsletter - Number 12.3*, 12.02.2014.

[1399] Available from http://es.scribd.com/doc/153099627/Plainteprism-Finale [23 December 2014].

[1400] Investigatory Powers Tribunal, Application MPS/FT/002295/000, 13.05.2014; Witness Statement on behalf of GCHQ, Case N. IPT/13/92/CH, 16.5.2014.

[1401] [2014] UKIPTrib, 13_77/H. Case no. IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH, 05.12.2014.

disclosures, the regime governing GCHQ data processing originally contravened the ECHR but that it was now adequate.[1402]

From this examination, it can be concluded that the EU could eventually have a role in intelligence services' matters. However, there are legal and also political issues that stop the EU from legislating on intelligence services, under the assumption that their activities are part of the 'national security' exclusion. Yet, there is no clear definition within the EU laws of what this concept includes.[1403]

Besides the current judicial cases involving national intelligence services, one might wonder whether IntCen could be reviewed by the CJEU. If we consider that IntCen falls completely within the scope of the CFSP, the general rule is that the CJEU does not have jurisdiction in the field of CFSP.[1404] Yet, there are two exceptions to this rule.[1405] One is the Court's jurisdiction on matters concerning the delimitation between areas. According to Article 24 TEU, the CJEU has:

'[J]urisdiction to monitor compliance with Article 40 of this Treaty and to review the legality of certain decisions as provided for by the second paragraph of Article 275 of the Treaty on the Functioning of the European Union.'

Under this provision, the Court could decide whether IntCen falls completely under the scope of the CFSP or for only certain of its activities. For those actions adopted as EU internal security measures, IntCen could be subject to external supervision in the future. The body in charge of it may be composed of national DPAs (similar to the current Joint Supervisory Body for Europol) or even the CJEU.

Another exception of the CJEU non-jurisdiction rule concerns those restrictive measures that affect natural or legal persons. The most discussed case regarding this exception is *Kadi and Al Barakaad* about economic sanctions.[1406] As seen in Kadi saga, the CJEU safeguards that all EU measures and EU bodies respect the EU fundamental principles such as accountability, the right to fair hearing, the right to respect for

[1402] [2015] UKIPTrib, 13_77/H. Case no. IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH, 06.02.2015.
[1403] 'The relation between the surveillance practices in the EU and the US and the EU data protection provisions', PE524.632v01-00, European Parliament, Working Document 3, 12.12.2013, p. 4.
[1404] Article 275(1) TFEU.
[1405] Brkan M 2012, 'The role of the European Court of Justice in the field of Common Foreign and Security Policy after the Treaty of Lisbon: New challenge for the future' in *EU external relations law and policy in the post-Lisbon era*, ed. Paul-James Cardwell, Springer, Berlin, pp. 97-118.
[1406] Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, 18.07.2013.

property and principle of proportionality, and the right to effective judicial review are complied with. In order to do that, the Court can request classified intelligence during its reviews. This is established in Article 65 of the Rules of Procedure, which state that the CJEU may participate in an inquiry as part of ongoing judicial proceedings.[1407] This inquiry can include the request of classified intelligence. The Court did not need to use this provision for *Kadi*, but it might have a crucial role if the CJEU ever needs to review IntCen activities in the future.

### 5.4. The relevance of Article 39 TEU

Article 39 TEU was included for the first time with the Treaty of Lisbon. This clause gives a possibility to establish specific EU rules on the processing of personal data for activities falling under the scope of the CFSP. As seen in Chapter 2 of this thesis, data processed by IntCen and data collected during CSDP missions are two of the activities that could be regulated under Article 39 TEU. This provision regulates 'the processing of personal data by the Member States'. IntCen does not currently have any operational role, and it cannot collect information by itself. The centre gathers representatives of intelligence agencies in the member states for exchanging information and drafting terrorism assessment reports. In other words, intelligence processed in the centre comes directly from member states and other EU bodies. Therefore, Article 39 TEU could certainly serve as legal basis for the activities of the centre.

The Council is the institution that would regulate IntCen's data processing activities. The kind of measure to be taken would not be a legislative act, since this is not permitted under the CFSP.[1408] Instead, the Council should adopt a decision, which would be voted in unanimously.[1409] Such a Council decision on Article 39 TEU, even if it constitutes an exception of the general data protection provision of Article 16 TFEU, would improve the current situation in which every member state has its own legal framework, if they have any at all.

As mentioned earlier, IntCen connects both EU internal security and external security matters. In that sense, Salmi points out that the centre can 'also provide analysis of terrorism and other global threats that are reflected in the EU internal

[1407] OJ L 265, 29.09.2012, pp. 1-42.
[1408] Article 24(1) TEU.
[1409] Article 31(1) TEU.

security'.[1410] Article 39 TFEU rules would only apply for external security issues. That information collected within the scope of the EU internal security, as part of the AFSJ, would conform the general rules on data protection as stipulated in Article 16 TFEU. In other words, intelligence exchanged through IntCen to prevent or detect EU threats would fall within the scope of the AFSJ and, consequently, it would be subject to Article 16 TFEU. In contrast, intelligence exchanged by the centre beyond the EU territory to investigate international threats will be processed as part of the CFSP. In such cases, Article 39 TEU – never used to date – could serve as legal basis.

Either way, it is clear that the EU has competence to establish rules for IntCen. A transparent mandate for the centre would surely increase the intelligence cooperation within the EU for the years to come.

## 6. Conclusions

The Snowden revelations about intelligence services' data collection and processing activities have caused great concern within the EU. The leaked documents show that not only is the NSA collecting massive amounts of personal data from untargeted individuals, but also that intelligence agencies in the member states are carrying out these same practices within the EU. This chapter has identified some of these activities, scrutinising their potential infringement of the EU fundamental right to data protection.

This chapter has presented two different case scenarios in which intelligence services' activities may clash with EU citizens' right to data protection: 1) when foreign intelligence services collaborate with private companies and EU intelligence services to process mass data of EU citizens (section 3); and 2) when intelligence services in the EU process mass data of EU citizens (section 4). What both cases have in common is that EU laws are in principle not applicable.

Nevertheless, the EU has several forms of redress for EU citizens at the national, European and international levels against intelligence services' activities. At the national level, despite all member states having oversight mechanisms over intelligence services' activities, these differ from one country to the other. In some countries, intelligence agencies have the power to access information lawfully without a prior court order, whereas in other countries more stringent limitations apply. A way to

[1410] Salmi I 2014, 'Multilateral intelligence cooperation in the EU', *Gnosis Rivista italiana di Intelligence*, no. 2. Available from http://gnosis.aisi.gov.it/Gnosis/Rivista39.nsf/ServNavig/24 [28 October 2014].

harmonise these oversight measures would be by clarifying the IntCen's mandate. This chapter suggests the use of Article 39 TEU to establish rules on the information exchanged by intelligence services through IntCen, including the data protection standards they would have to comply with.

The EU has assumed that 'national security' activities are those carried out by intelligence services and, consequently, its regulation and control is almost non-existent at the EU level. However, this chapter has showed that national security duties can be conducted by either intelligence services or law enforcement authorities. Police agencies have been taking on intelligence-gathering roles over the years and, therefore, the tasks of both types of agencies overlap at times. Likewise, although intelligence services have national security tasks, they may also conduct EU 'internal security' and 'external security' functions. Therefore, the 'national security' exclusion of Articles 4(2) TEU and Articles 72/73 TFEU needs to be clarified.

Finally, even if no express provisions are currently found in the Treaty of Lisbon and EU secondary laws, intelligence services' activities of member states need to comply with the ECHR and the Charter of Fundamental Rights. There are at the moment three pending cases involving intelligence services at the ECtHR and the CJEU. On the one hand, the ECtHR is examining whether British and Hungarian secret services' activities are infringing Article 8 of the ECHR. On the other hand, an Irish court has issued a preliminary ruling before the CJEU asking whether Facebook and other tech companies have infringed Articles 7 and 8 of the Charter by cooperating with intelligence agencies via PRISM. These might become landmark cases. They will not only show the effectiveness of data protection rules for EU citizens, but will also reveal to what extent EU laws might be enforceable against global tech companies (like Facebook), secret services of the member states (like GCHQ) and even intelligence agencies beyond the EU borders (like NSA).

## Chapter 5: The feasibility of global data protection standards for information processed for security purposes

Chapters 1 and 2 presented the existing EU frameworks for data shared by law enforcement authorities within the EU and between the EU and third countries. The data protection challenges to which these give rise have also been examined. As a response to these challenges, Chapter 3 has suggested enhancing the use of Europol during cross-border police investigations. Europol has strong data protection and security standards, which member states and third countries could also incorporate in their own legal frameworks. Despite this thesis being mainly focused on law enforcement data transfers, Chapter 4 has examined data processing activities conducted by intelligence services. The reason for this chapter is that law enforcement authorities work hand in hand with intelligence services, and the division of their activities has become more diffuse over the years.

So far this thesis has suggested increasing the role of Europol and IntCen as a way to establish global data protection standards in the field of security. The final part of this thesis will identify other current international initiatives that put forward global data protection principles in the field of security. It will present an overview of the main instruments for establishing global data protection standards and it will then discuss some shortcomings related to some of these initiatives.

In order to understand the necessity for common data protection standards in the field of security, a first assessment of the compatibility of mass surveillance activities with the public international law will be conducted. These activities are mostly carried out by intelligence services (rather than by law enforcement agencies), as the Snowden documents have proved. After that, it will analyse the principles enshrined in the OECD Privacy Guidelines, the APEC Privacy Framework, the UN Guidelines for the Regulation of Computerised Personal Data Files, the 1981 CoE Convention and the Cybercrime Convention. Other general principles not linked to any international organisation will be also considered. This examination will help identify which of these rules would bind security agents.

In sum, this chapter seeks to assess whether it is feasible to have data protection standards at the international level establishing rules that compel both law enforcement and intelligence services. If so, it will determine what the ideal global data protection

framework would be. It will particularly discuss whether rules should be enclosed in one single law, a dual system, or a multiple legal framework.

## 1. Compatibility of mass surveillance systems with public international law

From the international law perspective, the debate on the lawfulness of intelligence services' activities is unresolved. Under public international law, espionage is neither permitted not prohibited.[1411] But what about the specific mass surveillance activities that were exposed by Snowden?

If mass surveillance activities are seen as an 'intervention' in the terms of international law, then they are generally prohibited.[1412] The principle of non-intervention in customary international law may only be breached in times of war, and if the parties are engaged in armed conflict.[1413] Likewise, that 'intervention' could also be permitted if there is consent from the targeted state.[1414] The Snowden disclosures have proved that the NSA and the other members of '5-Eyes' have been spying on the governments of numerous countries such as Germany,[1415] Mexico,[1416] France[1417] and Brazil.[1418] When that took place, there was no armed conflict affecting these countries, and they never consented to that surveillance.[1419]

Another rule stemming from the customary international law is that an 'intervention' is prohibited if it takes place 'within the domestic jurisdiction of any state'.[1420] Because of this rule, it becomes very difficult to condemn the activities conducted by the '5-Eyes' members. Since the communications are, in principle, intercepted from outside of the country, the activities are not considered unlawful.[1421]

---

[1411] Aust HP 2014, 'Stellungsnahme zur Sachverständigenanhörung', Humboldt-Universität zu Berlin, 05.06.2014. Available from www.bundestag.de [6 November 2014].
[1412] Article 2(7) UN Charter.
[1413] Article 51 UN Charter.
[1414] Article 24 UN Charter.
[1415] Oltermann P 2014, 'NSA tapped German ex-chancellor Gerhard Schröder's phone – report', *The Guardian*, 4 February. Available from http://www.theguardian.com [22 December 2014].
[1416] Glüsing J, Poitras L, Rosenbach M & Stark H 2013, 'Fresh Leak on US Spying: NSA accessed Mexican President's email', *Spiegel*, 20 October. Available from http://www.spiegel.de [22 December 2014].
[1417] 'Success Story': NSA Targeted French Foreign Ministry', *Spiegel*, 01.09.2013. Available from http://www.spiegel.de [22 December 2014].
[1418] 'Report: NSA spied on Brazilians, Mexican presidents', *CBSNews*, 01.09.2013. Available from http://www.cbsnews.com [22 December 2014].
[1419] Korff 2014, p. 4.
[1420] Article 2(7) UN Charter.
[1421] Korff 2014, pp. 6-7.

Nevertheless, the majority of surveillance activities that have been unveiled have not had other states as targets, but individuals. The customary international law regulates the possible breach of inter-state norms about respecting each other's sovereignty, but the question of the violation of individual human rights is dealt with as a separate issue. For these cases, international human rights law applies as a special branch of the public international law. Human rights laws protect individuals, not states, and they are characterised for being both treaty-based and customary. There are two specific UN laws on international human rights that include a provision on the right to privacy: the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR). Articles 17 ICCPR and 12 UDHR establish that:

> '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.'

According to these provisions, the UN High Commissioner for Human Rights,[1422] as well as the former[1423] and the current[1424] UN Special Rapporteurs on human rights and counter-terrorism have noted that mass surveillance programmes used by intelligence agencies are almost certainly illegal under international law. All members of the '5-Eyes' are parties to the ICCPR and the UDHR, but only the ICCPR has legally binding effects for its members. This treaty was adopted by the UN in 1966 (but it did not enter into force until 1976) and has 167 states parties, including the US.

The ICCPR is supervised by the Human Rights Committee. This committee is composed of several independent experts and it assesses whether the parties of the Covenant are complying with their obligations. In addition, it adopts General Comments on the interpretation of each of the ICCPR provisions. Unfortunately, the only General Comment on Article 17 ICCPR was released by the committee in 1988. In it, it was

[1422] The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, 30.06.2014.
[1423] Scheinin, M 2013, 'LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens Hearing', *European Parliament*, 14 October, p. 6.
[1424] United Nations, General Assembly, Promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/297, 23.09.2014.

concluded that the idea of 'correspondence' needed to be extended to the digital sphere.[1425]

The main instrument that can be used to assess whether the NSA programmes violate Article 17 ICCPR is the privacy limitation test published by the former Special Rapporteur on human rights and counter-terrorism Martin Scheinin in 2009.[1426] The test consists of seven points that, if complied with, could justify the limitation of any human right by the government. The specific requirements are the following: i) the restriction must be provided by law, ii) the essence of the human right cannot be restricted, iii) the restriction must be necessary in a democratic society, iv) any discretion in the restriction must not be unfettered, v) the restriction must be necessary for reaching a legitimate aim, vi) the restriction must obey the principle of proportionality, and vii) the restriction must be consistent with the other ICCPR rights.

As Scheinin explained before the EP in October 2013, the NSA mass surveillance systems fail to comply with 'several separate elements of the permissible limitations test' as regards the right to privacy.[1427] The failure was based on six elements: a) the NSA programmes are not provided by law so they lack of a proper legal basis; b) the essence of the right to privacy is violated because the collection of data does not distinguish among types and sensitivity of the information; c) the interferences are not justified for the actual prevention of terrorism and other serious crimes; d) FISA leaves room for unfettered discretion; e) the intrusion is disproportionate in comparison with the results achieved; f) and the restrictions clash with other human rights besides the right to privacy like the right to non-discrimination (Article 26), the freedom of expression (Article 19), the freedom of association (Article 22) and the freedom of movement (Article 12).

The inconsistency of both US and UK security laws with other ICCPR rights is particularly visible as regards the right to non-discrimination. The RIPA in the UK and the FISA in the US make distinctions between foreign and domestic communications. Consequently, there is a distinction between nationals (and long term residents), and

---

[1425] United Nations, Compilation of General Comments and General Recommendations adopted by Human Rights Treaty Bodies Human Rights Committee, General Comment No. 16 (Article 17), para. 10, HRI/GEN/1/Rev.9 (Vol. I), 27.05.2008, p. 193.

[1426] Scheinin 2009, para. 17. The limitations test is endorsed by La Rue, F 2013, 'Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', *General Assembly of the United Nations*, A/HRC/23/40.

[1427] Scheinin 2013, p. 3.

non-nationals. According to RIPA, 'external' warrants allow the collection of bulk data,[1428] whereas 'internal' warrants do not permit it. Likewise, FISA discriminates non-US citizens, whose privacy is not protected by the US Fourth Amendment. In that sense, Korff suggested redrafting these laws to conform to Article 26 ICCPR.[1429]

The issue of extra-territoriality of the ICCPR is crucial for determining whether the '5-eyes' activities have violated the Covenant or not. Most of the surveillance programmes that have been revealed by Snowden allow intelligence agents to access foreign communications without even moving from their headquarters. The Internet has changed the way espionage works. Today, simply by installing software, analysts are able to break into any computer or tap any phone and collect all types of information.

That being said, NSA mass surveillance programmes will only be subject to ICCPR if extra-territoriality applies. The answer is not clear, since Article 17 ICCPR does not include any reference to its territorial scope of application, which means that the definition of the scope for the right to privacy is entrusted to Article 2(1) ICCPR.[1430] According to this provision, the Contracting Parties are obliged to comply with the rights of the Covenant 'within its territory and subject to its jurisdiction'. This has been the argument used by the US government to conclude that the surveillance of 'foreign' communications does not fall under the scope of ICCPR.

In contrast, the Human Rights Committee has long taken the position that the ICCPR applies extra-territorially. In 2004, the Committee released General Comments on the nature of the ICCPR obligations, in which it noted that rules included in the Covenant were 'erga omnes'. The Committee added that the Contracting Parties must ensure the ICCPR rights to anyone 'even if not situated within the territory of the State Party'.[1431] The Committee has kept this position to date, giving rise to numerous cases that confirm the extraterritorial reach of the ICCPR.[1432]

The International Court of Justice has also addressed the extraterritorial scope of human rights treaties, including the ICCPR. In its Advisory Opinion on the Wall built

[1428] Section 8(4) warrants. See Korff 2014, p. 21; and Bowcott O 2014, 'Social media mass surveillance is permitted by law, says top UK official', *The Guardian*, 17 June. Available from www.theguardian.com [6 November 2014].
[1429] Korff 2014, p. 26.
[1430] Scheinin M 2014, 'To the Extent the ICCPR has Extraterritorial Effect, the Right to Privacy Is Not an Exception', written statement for *Privacy and Civil Liberties Oversight Board*'s hearing on 19.03.2014 Washington, D.C., p. 3.
[1431] Human Rights Committee, General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004), para.10.
[1432] For instance, Lopez Burgos v. Uruguay (52/1979), Sophie Vidal Martins v. Uruguay (57/1979), and Guye et al. v. France (196/1985).

by Israel in the Occupied Palestinian Territory (OPT), it concluded that 'while the jurisdiction of States is primarily territorial, it may sometimes be exercised outside the national territory'.[1433]

Similarly, both the former and current UN Special Rapporteurs on the promotion and protection of human rights and fundamental freedoms believe that the ICCPR has an extraterritorial effect. On the one hand, Scheinin noted that positive state obligations may not apply outside a country's own territory, but negative obligations not to violate human rights apply everywhere and in respect of everyone.[1434] One the other hand, Emmerson stated that States are legally bound to the Covenant and should offer the same protection to nationals and to non-nationals.[1435] According to these arguments, the US and the rest of the '5-Eyes' members have infringed the negative obligation of not violating individuals' right to privacy. Likewise, intelligence services' surveillance activities, even if conducted from home, are in breach of the right to privacy of Article 17.[1436]

Assuming that the ICCPR applies extra-territorially, one last question needs to be answered: what are the legal remedies on public international law when a violation of the ICCPR occurs? The supervisor on the compliance of the ICCPR provisions is the Human Rights Committee. The UN adopted an Optional Protocol of the ICCPR, which allowed individuals within the jurisdiction of one of the Contracting Parties to issue a complaint for the alleged violation of any of the ICCPR provisions. Individuals need to exhaust all domestic remedies first, and the application cannot be examined by another international body (e.g. the ECtHR) at the same time. Also, it must be noted that the only '5-Eyes' members that have ratified the protocol are Australia,[1437] Canada[1438] and New Zealand.[1439] Thus, since the US and the UK have not ratified it, no individual complaint against those countries could be issued today.

The Human Rights Committee can still evaluate the compliance of the ICCPR, even if the Contracting Parties have not ratified the protocol, through two other mechanisms: The inter-state complaint procedure (Article 41) and the mandatory reports that parties

[1433] Cour Internationale de Justice, 'Consequénces juridiques de l'edification d'un mur dans le territoire Palestinien occuppé', Advisory Opinion 09.07.2004, para. 109.
[1434] Scheinin 2014, p. 5.
[1435] United Nations, General Assembly, Promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/297, 23.09.2014, pp.17.
[1436] Scheinin 2014, p. 7.
[1437] It was ratified on 20 September 1991.
[1438] It was ratified on 19 May 1976.
[1439] It was ratified on 26 May 1989.

must submit under the Committee request (Article 40). The possibility to submit an inter-state complaint has never been used to date, but it would allow one State party to complain about the violation of the Covenant by another party. For instance, it could occur that Germany or another targeted country starts an inter-state complaint procedure against the US. As for the periodical state reports, the Human Rights Committee has recently released concluding observations of the Fourth report of the United States of America[1440] in which it expressed serious concerns about the NSA surveillance. On this matter, the Committee recommended that the US conform to the obligations of Article 17 ICCPR by specifying in detail the circumstances, duration, procedures and safeguards of the surveillance. In addition, the Committee urged a reform of the oversight system over surveillance activities and the inclusion of judicial supervision.[1441] The legal nature of the Human Rights Committee Concluding Observations is imprecise. Some of the literature establishes that they constitute mere recommendations,[1442] whereas other scholars describe them as a 'soft law' instrument.[1443] Therefore, even if the Committee Concluding Observations might carry a considerable legal weight, it is not certain that they will shape the subsequent practice in the US as regards mass surveillance activities.

After this analysis it can be concluded that the ICCPR appears to be insufficient for the protection of the right to privacy against mass surveillance programmes used by law enforcement and intelligence services. In that sense, the Art. 29 WP proposed to adoption of an additional protocol to Article 17 in which the meaning of 'data processing' is clarified and its safeguards are guaranteed to all individuals.[1444] However, the proposal has not been successful. Others have urged the Human Rights Committee to adopt an up-to-date General Comment on Article 17 to codify and clarify the existing law, including on the issue of extraterritorial effect.[1445] This has yet to occur.

---

[1440] Fourth Periodic Report of the United States of America to the United Nations Committee on Human Rights Concerning the International Covenant on Civil and Political Rights, 30.12.2011.
[1441] Human Rights Committee. Concluding observations on the fourth report of the United States of America, 110th session (10–28 March 2014), p. 9.
[1442] 'Implementation of UN Treaty Body Concluding Observations: The Role of National and Regional Mechanisms in Europe', Summary and recommendations form the High Level Seminar held on 19-20 September 2011, pp. 1-2.
[1443] Guzman AT & Meyer T 2011, 'International Soft Law', *UC Berkeley, Public Law and Legal Theory Research Paper Series*, Berkeley; and 'Sources of International Law', *Icelandic Human Rights Center*. Available from www.humanrights.is [6 November 2014].
[1444] WP215, 10.04.2014, p. 16.
[1445] 'Privacy Rights in the Digital Age. A Proposal for a New General Comment on the Right to Privacy

## 2. Initiatives to establish international data protection principles

After the examination of the international rules that could criminalise those mass surveillance activities conducted by intelligence agencies, it is crucial to explore whether there are also any international data protection principles that compel these agencies. If not, could any of the existing data protection legal frameworks be established globally in the future?

Previous chapters of this thesis have analysed the data protection rules adopted within the EU legal framework (i.e. those included in Directive 95/46/EC, Council Framework Decision 2008/977/JHA and Europol Council Decision). That analysis has confirmed that the EU has stricter data protection principles than other third countries. Likewise, it has concluded the EU does not apply the same rules if data is processed for commercial purposes, rather than for security reasons. It has also been shown that EU laws do not include, in principle, intelligence services. Because of these complexities, the EU can hardly become the model institution for a universal data protection framework today.

That said, it is necessary to scrutinise whether other international organisations would be in a better position to export their data protection principles worldwide. In this sense, the Organisation for Economic Co-operation and Development, the United Nations, and the Council of Europe have included principles on privacy and data protection in their legal frameworks. Particularly, this section examines principles enshrined in the OECD Privacy Guidelines, the APEC Privacy Framework, the UN Guidelines for the Regulation of Computerized Personal Data Files, the 1981 CoE Convention and the Cybercrime Convention.

### 2.1. OECD Privacy Guidelines

The Organisation for Economic Co-operation and Development (OECD) is the organisation that represents the major world economies. It released a Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (hereinafter, OECD Privacy Guidelines) in September 1980. OECD Privacy Guidelines include principles such as the collection

---

under Article 17 of the International Covenant on Civil and Political Rights: A Draft Report and General Comment by the American Civil Liberties Union', *ACLU*, March 2014.

limitation, data quality, purpose specification, use limitation and accountability. Back in the 1980s, these Guidelines had a crucial role since they served as the source of inspiration for other legal frameworks, such as Directive 95/46/EC in 1995; Generally Accepted Privacy Principles (GAPP) in 2003, 2006 and 2009;[1446] and Asia-Pacific Economic Cooperation (APEC) privacy principles in 2005.[1447]

In addition to the OECD Privacy Guidelines, in 2007 the OECD adopted a Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy.[1448] It was later developed by an Action Plan for the Global Privacy Enforcement Network (GPEN), which connects twenty-two privacy enforcement authorities from around the world.[1449] Unfortunately, neither the OECD Privacy Guidelines nor the GPEN have binding effects on the Contracting Parties.

Because of the massive growth of international data flows in the last thirty years, the OECD Privacy Guidelines urged the amendment of the rules. The review of the OECD Guidelines was officially announced during the Seoul Declaration for the Future of the Internet Economy in 2008.[1450] In October 2011 the OECD Working Party on Information Security and Privacy (WPISP) released the terms of reference for the review.[1451] The review of the guidelines finally took place in July 2013 by a Privacy Experts Group of the OECD Working Party on Information Security and Privacy.

The 2013 OECD Privacy Guidelines incorporate new rules on data breach notification, risk management and interoperability activities through national strategies. All principles that existed in the 1980, however, remain unchanged.[1452] This issue has caused different reactions among privacy experts: one the one hand, there are some scholars who agree with keeping the principles as they were in 1980; but on the other hand, there are those experts in favour of changing them. Regarding the latter, a study conducted by Cate, Cullen and Mayer-Schönberger in December 2013 suggested

---

[1446] American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. *Generally Accepted Privacy Principles*. Last version from August 2009. Available from www.aicpa.org [6 November 2014].

[1447] APEC Privacy Framework 2005. Available from www.apec.org [6 November 2014].

[1448] Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, 12.06.2007, p. 9. Available from <http://www.oecd.org/dataoecd/43/28/38770483.pdf> [6 November 2014].

[1449] GPEN Action Plan, 15.06.2012; Part E amended 22.01.2013. For further information, see https://www.privacyenforcement.net/public/activities [6 November 2014].

[1450] OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea, 17/18.06.2008.

[1451] Terms of reference for the review of OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, Working Party on Information Security and Privacy, DSTI/ICCP/REG(2011)4/FINAL, 31.10.2011.

[1452] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, C(80)58/FINAL, 11.07.213.

lowering the existing standards of privacy and data protection.[1453] In particular, it proposed a reduction of the rules on data collection, as well as more focus on data processing guidelines. Moreover, that study noted that, instead of specifying the purpose by which certain data was used, rules on the 'not compatible' purposes should be included. In that sense, the authors proposed replacing the 'collection limitation principle' and the 'use specification principle' for a simple 'collection principle' and 'use principle'. Finally, they suggested including an 'enforcement principle' to ensure that all countries have the adequate laws and bodies to achieve effective compliance of the principles.

In contrast, a study released in March 2014 by Ann Cavoukian, Alexander Dix and Khaled El Emam[1454] suggested maintaining the current OECD principles. The only change the authors proposed was the addition of the privacy by design principle.[1455] They also criticised the report of Mayer-Schönberger et al., arguing that the OECD rules needed to be reinforced rather than diminished.

It can thus be seen that, even after the revision of OECD Privacy Guidelines, many issues are still unclear. The 2013 OECD Privacy Guidelines came out in the same month Snowden exposed the mass surveillance conducted by intelligence services around the world. OECD rules only cover data processing activities within the scope of commercial or economic operations. Any data collected by law enforcement or intelligence authorities falls out of the competence of the organisation. However, the revelations have proved that a large amount of information collected by private companies for commercial purposes is later processed by governments for security reasons.

Because of this, my view is that the OECD guidelines could maintain the same foundational principles but they should include rules limiting the use and transfer of personal data collected by companies located in one of the OECD Contracting Parties (including the US, which is a member of the OECD). In any event, since the OECD Guidelines are not mandatory, the possibilities to use this instrument for the establishment of global data protection safeguards are minimal.

---

[1453] Cate FH, Cullen P & Mayer-Schönberger V 2013, 'Data Protection Principles for the 21st Century. Revising the 1980 OECD Guidelines', Oxford Internet Institute (OII), University of Oxford.
[1454] Cavoukian A, Dix A and El Emam K 2014, 'The unintended consequences of privacy paternalism', *Information and Privacy Commissioner Ontario, Canada*. 5 March.
[1455] See Appendix of their study for the 7 foundational principles of Privacy-by-Design.

## 2.2. APEC Privacy Framework

Another international organisation that has released privacy principles to be met by its members is the Asia-Pacific Economic Cooperation forum (APEC). APEC is comprised of twenty-one economies around Asia and the Pacific, which represent the 40% of the world population and the 54% of the world GDP.[1456]

In the last ten years, APEC has brought great progress to the field of privacy. In November 2004 it established privacy guidelines that protected the information transferred among APEC economies. In particular, these guidelines established nine core privacy principles: preventing harm, notice, collection limitation, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, and accountability.[1457] However, the rules were non-binding and, hence, they could not be enforced.

Therefore, in 2010, the APEC guidelines were reinforced through the establishment of APEC Cross-Border Privacy Enforcement Arrangement (CPEA). It promoted the creation of Privacy Enforcement Authorities (PEAs) that would supervise data shared among APEC regions.[1458] One year later, APEC announced the establishment of the Cross-Border Privacy Rules (CBPR) system 'to reduce barriers to information flows, enhance consumer privacy, and promote interoperability across regional data privacy regimes'.[1459] Unlike the previous guidelines, these are mandatory for their members.

For a country to be part of the APEC CBPR system, it needs to first comply with the Charter of the Cross Border Privacy Rules Joint Oversight Panel, as well as a self-assessment questionnaire. The questionnaire is based on the nine APEC Privacy Principles mentioned above, and is reviewed by an APEC-recognised Accountability Agent, who assesses and enforces the laws.[1460] The country must also have a PEA, as a public body responsible for enforcing the Privacy Law of the Economy's jurisdiction.[1461] A Joint Oversight Panel is the body in charge of supervising the

[1456] Kropf J & Crompton M 2013, 'The EU and APEC: A roadmap for global interoperability?', *IAPP*, 26 November. Available from www.privacyassociation.org [6 November 2014].
[1457] APEC Privacy Framework 2005.
[1458] APEC Cooperation Arrangement for Cross-Border Privacy Enforcement, 2010/SOM1/ECSG/DPS/013, Data Privacy Subgroup Meeting Hiroshima, Japan, 28.02.2010.
[1459] 2011 Leaders' Declaration The Honolulu Declaration - Toward a Seamless Regional Economy, 12/13.11.2011. Available from www.apec.org [6 November 2014].
[1460] APEC cross-border privacy rules system. Policies, rules and guidelines, p. 3. Available from www.apec.org [6 November 2014].
[1461] That body could have the position of Accountability Agent and PEA at the same time.

adequacy of Accountability Agent and PEAs, with powers to suspend them if they commit any irregularity.[1462] It is composed of representatives from three APEC economies, who are appointed for a period of two years.

The first country to participate in the APEC CBPR system was the US in September 2012; and IBM was the first certified company in August 2013. The system is binding, so the countries and companies subscribing to it must have privacy policies consistent with the APEC principles. Unfortunately, there are today only four APEC economies (the US, Mexico, Canada and Japan) and four companies (IBM, Merck, Workday, Lynda.com and Yodlee) participating in the CBPR.[1463] The number of countries can, however, increase in the future. In fact, Australia is already on its way to joining the system.[1464]

A relevant issue of the CBPR is its to the Binding Corporate Rules (BCR). The scope of the BCR is foreseen in the proposal for an EU regulation on data protection. These rules will allow the establishing of standards within the EU for the transfer of data, irrespective of the data protection framework in the destination country.[1465]

However, the CBPR and the BCR are not fully equivalent. On this issue, the Art. 29 WP published a study in February 2014 identifying the common aspects and differences between the CBPR and the BCR.[1466] One of the main distinctions is that the BCR must be approved by national DPAs whereas the CBPR have APEC Accountability Agents as supervisory bodies.

In any event, as in the OECD principles, APEC privacy rules would never apply for information processed by individuals or governments. Consequently, even if the twenty-one economies decided to join the regime, it would hardly become a model to follow for global data protection principles, since its scope is very limited.

---

[1462] APEC cross-border privacy rules system. Policies, rules and guidelines, p. 9.
[1463] Available from http://www.cbprs.org [6 November 2014].
[1464] Heyder M 2014, ' The APEC cross-border privacy rules – Now that we've built it, will they come?', *Privacy perspectives*, 4 September. Available from https://privacyassociation.org [6 November 2014].
[1465] Preamble 83 of the Proposed Regulation. On BCR see also the Art. 29 WP opinions WP 74, 03.06.2003; WP 107 and 108, 14.04.2005; WP 153, WP 154 and WP 155, 24.06.2008.
[1466] WP 212, 27.02.2014.

### 2.3. UN Guidelines for the Regulation of Computerised Personal Data Files

In 1990, after more than ten years of negotiations,[1467] the United Nations (UN) released guidelines concerning computerised personal data files.[1468] This instrument establishes that personal information cannot be used for purposes contrary to the provisions of the UN Charter. These guidelines include privacy principles such as lawfulness and fairness, accuracy, purpose specification, non-discrimination, data security and interest-person access. They also require the designation of an independent supervisory authority, and they foresee sanctions in case of a violation.

The UN today has 193 members. Therefore, any law adopted under the framework of this organisation can already be considered 'universal'. However, the UN guidelines concerning computerised personal data files have been adopted by the UN General Assembly and, hence, they do not have binding effects. Moreover, they are guidelines that need to be implemented at the country's discretion. For this reason, these principles have often been under-used and undervalued.

Today, the UN Guidelines concerning computerised personal data files have been abandoned. They were created in 1990, but in the last twenty-five years enormous technological advances have taken place. These changes have made it a necessity to reform all existing privacy laws but, strangely, no amendment on the UN guidelines has been announced for the moment.

The UN Guidelines need to be updated. An alternative to this amendment has been suggested by Paul De Hert and Vagelis Papakonstantinou. These scholars proposed the creation of a new specialised UN Agency, similar to the World Intellectual Property Organization (WIPO), to promote the principles.[1469] The same guidelines from 1990 could be utilised, but they would have a greater impact because they would fall under the scope of a specialised UN agency.

The only reaction on privacy changes under the UN legal framework has been recently launched by Germany and Brazil. In response to the Snowden disclosures, these two countries presented to the UN General Assembly in November 2013 a resolution claiming the expansion of the right to privacy internationally, as well as the

[1467] De Hert P & Papakonstantinou V 2013, 'Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN Agency?', *I/S: a Journal of Law and Policy for the Information Society*, vol. 9, no. 3, p. 281.
[1468] Guidelines for the Regulation of Computerized Personal Data Files, General Assembly resolution 45/95, 14.12.1990.
[1469] De Hert &Papakonstantinou 2013, p. 321.

end of the mass surveillance.[1470] This resolution was replaced one year later by a new text, which claimed the limitation of metadata processing, among other particularities.[1471] The new resolution, which still needs to be voted in the UN General Assembly, is entitled 'Right to privacy in the digital age' and it specifies the States' obligations in the processing of data for security purposes.[1472] However, as with the 1990 UN guidelines, this resolution will be non-binding.

### 2.4. Council of Europe 1981 Convention and Cybercrime Convention

For more than thirty years now, the Council of Europe (CoE) has been participating in the creation of rules concerning the right to privacy and data protection among its Contracting Parties. As a general rule, Article 8 ECHR enshrines the right to respect everyone's private and family life and correspondence. More particularly, the CoE has two significant instruments: a) the Convention for the protection of individuals with regard to the automatic processing of personal data (hereinafter, 1981 CoE Convention),[1473] and b) the Cybercrime Convention.[1474] Both instruments have binding effects for its members but while 1981 CoE Convention covers all fields of data processing, the Cybercrime Convention of 2001 deals specifically with crimes committed by means of electronic networks. However, none of these conventions has direct applicability for the individuals: every Contracting Party needs to adopt the necessary measures at the domestic level in order to enforce the principles enshrined in the conventions.[1475]

The CoE has also released numerous recommendations tackling data protection issues in 1981,[1476] 1983,[1477] 1985,[1478] 1986,[1479] 1987,[1480] 1989,[1481] 1990,[1482] 1991,[1483]

[1470] United Nations, General Assembly, A/C3/68/L.45, 01.11.2013.
[1471] Nichols M 2014, 'Germany, Brazil push the U.N. to be tougher on digital spying', *Reuters*, 6 November. Available from www.reuters.com [8 November 2014].
[1472] Ribeiro J 2014, 'UN committee calls on countries to protect right to privacy', *Pcworld*, 25 November. Available from http://www.pcworld.com [26 November 2014].
[1473] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, Council of Europe, 28.01.1981.
[1474] Convention on Cybercrime, CETS No. 185, Council of Europe, 23.11.2001. Entered into force on 1 July 2004.
[1475] On the non-direct applicability of 108 CoE Convention, see Spanish Constitutional Court, Case 254/1993, 20.7.1993.
[1476] Recommendation No. R (81) 1 on regulations for automated medical data banks, 23.01.1981.
[1477] Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics, 23.09.1983.
[1478] Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing, 23.09.1985.

1995,[1484] 1997,[1485] 1999,[1486] 2002,[1487] 2010,[1488] 2012,[1489] and 2014.[1490] However, these recommendations are not legally binding and, therefore, only the 1981 CoE Convention and the Cybercrime Convention are examined in this section.

The 1981 CoE Convention sets up minimum standards and values on the right to privacy that all Contracting Parties need to observe. According to Article 1 of the convention, the right to privacy is guaranteed to individuals irrespective of their nationality or the place of residence. The convention introduces principles referring to the duties of the parties, categories of data, safeguards for the data subjects, transnational data flow rules, mutual assistance provisions, and the role of the Consultative Committee, among others.

The 1981 CoE Convention has been ratified for more than forty countries,[1491] becoming a reference for numerous national legislations that have adapted their privacy laws to conform to the CoE principles. Moreover, unlike APEC and OECD principles, these are applicable to both private and public sectors.

The Art. 29 WP found in 1998 that the 'adequacy' criteria foreseen in the convention are almost equivalent to the adequacy conditions of Directive 95/46/EC.[1492] In fact, an Additional Protocol adopted in 2001 reinforced the weak points of the convention,

---

[1479] Recommendation No. R (86) 1 on the protection of personal data used for social security purposes, 23.01.1986.
[1480] Recommendation No. R (87) 15 regulating the use of personal data in the police sector, 17.09.1987.
[1481] Recommendation No. R (89) 2 on the protection of personal data used for employment purposes, 18.01.1989.
[1482] Recommendation No. R (90) 19 on the protection of personal data used for payment and other related operations, 13.09.1990.
[1483] Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies, 09.09.1991.
[1484] Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, 7.2.1995.
[1485] Recommendation No. R (97) 5 on the protection of medical data, 13.02.1997; Recommendation No. R (97) 18 concerning the protection of personal data collected and processed for statistical purposes, 30.09.1997.
[1486] Recommendation No. R (99) 5 on the protection of privacy on the Internet, 23.02.1999.
[1487] Recommendation No. R (2002) 9 on the protection of personal data collected and processed for insurance purposes, 18.09.2002.
[1488] Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23.11.2010. See also Polakiewicz, 2013.
[1489] Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, 04.04.2012; Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, 04.04.2012.
[1490] Recommendation CM/Rec(2014)6of the Committee of Ministers to member States on a Guide to human rights for Internet users, 16.4.2014.
[1491] European Commission, MEMO/12/192, 19.03.2012.
[1492] 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive', WP 12, 24.07.1998.

bringing it closer to Directive 95/46/EC.[1493] Could the 1981 CoE Convention set global privacy standards? As many academics have already pointed out,[1494] it is a very feasible option. The following paragraphs discuss the reasons why these principles would comply with ideal territorial and temporal features.

With regard to the territorial scope of the 1981 CoE Convention, the CoE is an international organisation constituted after the Second World War with the purpose of establishing common human and social rights among countries in Europe. Today, forty-seven countries are part of the CoE, forty-five of which have ratified the 108 CoE Data Protection Convention.[1495] Unsurprisingly, the majority of these countries are located within European borders. The fact that this international organisation is focused on one continent (Europe) could indeed cause problems in its use as reference for the establishment of global data protection standards. However, the 108 CoE Data Protection Convention is open for accession to non-CoE parties. In that sense, Morocco[1496] and Uruguay[1497] joined to the convention in 2013, and other countries like Mexico have already expressed interest in joining it in the future.[1498] Therefore, the clause for accession of non-members solves the territorial issue. The fact that the CoE is a Europe-oriented organisation does not impede the convention's principles from gaining global relevance in the future.

The second issue of concern is the fact that the content of the convention is, at first sight, outdated. Like the OECD Privacy Guidelines, the 108 CoE Data Protection Convention was published in 1981, before the era of the Internet. The original goals of the 108 CoE Data Protection Convention have not changed today, but privacy has been challenged by phenomena that did not exist at the time it was adopted. In particular, the global technological evolution as well as the increasing number of counter-terrorism measures have led to massive collection, processing and storage of data, urging the

---

[1493] 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, ETS No. 181, 08.11.01.

[1494] Polakiewicz J 2011, 'International Data Protection Conference Convention 108 as a global privacy standard', Speech in Budapest, 17 June Available from www.coe.int [6 November 2014].

[1495] List available from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CL=ENG [7 November 2014].

[1496] 'Morocco: Convention 108 accession to strengthen DPA's powers', *Data Guidance*, 20.06.2013. Available from www.dataguidance.com [7 November 2014].

[1497] 'International: Uruguay accedes to Convention 108; Morocco to follow', *Data Guidance*, 18.04.2013. Available from www.dataguidance.com [7 November 2014].

[1498] 'Council of Europe promotes personal data protection in Latin America', *MercoPress*, 31.19.2012. Available from www.mercopress.com [7 November 2014].

amendment of all current data protection legislations. A small amendment in the 1981 CoE Convention took place in 1999 to enable the EU to become a partner.[1499] As mentioned above, an additional protocol was included in 2001 with new provisions on transborder data flows and the establishment of DPAs. Yet, a new thorough reform of the 108 CoE Data Protection Convention was still needed. Therefore, a full reform of the convention started to be discussed in 2011.

The proposal for the modernisation of the 108 CoE Data Protection Convention was launched in January 2011[1500] in the form of a public consultation.[1501] Replies from governments, data protection authorities, NGOs, the private sector and professional associations were compiled by May 2011,[1502] and the report on the consultation was issued one month later.[1503] The document with the proposals for the new 108 CoE Data Protection Convention was issued in November 2011,[1504] and the Consultative Committee of the Convention released an official report with the most significant changes in January 2012.[1505] This was reviewed in March[1506] and April 2012.[1507] The proposal for modernisation was finalised in December 2012,[1508] and the draft[1509] was then sent to the Committee of Ministers. A specialised group called the Ad□Hoc Committee on Data Protection (CAHDATA) has been studying the proposal and suggesting amendments.[1510] The third and last CAHDATA meeting took place on 1-3 December 2014.[1511] The modernised 108 CoE Data Protection Convention has now been submitted to the Committee of Ministers, ready for adoption. Then, the Contracting Parties will need to sign it. Like in the current 1981 CoE Convention, there is a clause that allows non-Contracting Parties to access the Convention.

---

[1499] Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108] allowing the European Communities to accede of 15 June 1999.
[1500] Speech of Mr Thorbjørn Jagland, Secretary General of the Council of Europe, Data Protection Day (30th Anniversary) Brussels, 28.01.2011.
[1501] Public consultation, 'Modernisation of Convention 108: Give us your opinion!'. Available from http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_EN.pdf [7 November 2014]
[1502] Council of Europe, T-PD-BUR(2011) 02 prov MOS rev 4, 30.05.2011.
[1503] Council of Europe,T-PD-BUR(2011) 10 en, 21.06.2011.
[1504] Council of Europe, T-PD-BUR(2011) 27_en, 15.11.2011.
[1505] Council of Europe, T-PD-BUR(2012)01EN, 18.01.2012.
[1506] Council of Europe, T-PD-BUR(2012)01Rev, 05.03.2012.
[1507] Council of Europe, T-PD-BUR(2012)01Rev2, 27.04.2012.
[1508] Convention 108 Consultative Committee (T□PD) 29th plenary meeting Strasbourg 27-30 November 2012.
[1509] Council of Europe, T-PD_2012_04_rev4_E, 18.12.2012.
[1510] Working Document, Convention 108 with Additional Protocol and Modernisation proposals, CAHDATA(2014)1, 25.03.2014.
[1511] Council of Europe, CAHDATA(2014)RAP03Abr, 03.12.2014.

The new proposal includes several issues that need to be highlighted. First, the scope foreseen in Article 3 is broader than that in the current convention. It applies to any processing of personal data, and not only to automated personal data files. Moreover, the proposal reinforces principles such as transparency, proportionality, purpose limitation, the right of access, the right to object, the right not to be subject to an automated decision, accountability and the duty to notify data breaches.[1512] As for the definitions, the term 'automated processing' is replaced by the wider concept of 'data processing'. The definition of data controller is also modified.[1513]

Article 12 on transborder data flows is particularly relevant for those countries who are non-Members of the CoE or have not ratified the convention. An 'appropriate' level of protection in any transborder data flow will be presumed when data is transferred between Contracting Parties. However, according to paragraph 4, a procedure will be required to examine the appropriateness when the recipient is a non-Contracting Party. For instance, the US, being a non-Contracting Party, will not have the presumed 'appropriate' level of data protection, and will have to comply with Article 12(4) for every data transfer it receives from a Contracting Party (e.g. an EU Member State).

It is interesting that in previous versions of the proposal, third countries were required to have an 'adequate' level of protection, instead of an 'appropriate' level. It is not clear why the term has been modified, but this alteration might weaken the original data protection standards required for transborder data flows. As Greenleaf explains, the adjective 'appropriate' is not as strong as 'adequate', so the third country's compliance with some principles of the convention would be here sufficient.[1514] While adequacy requirements can be found in Directive 95/46/EC and the future Data Protection Regulation, the term 'appropriate' is not defined in any other data protection law. Therefore, there will no longer be a formal equivalence between the EU and the CoE data protection frameworks.

Even if the national laws implementing the convention involve national security issues,[1515] the application of the convention's rules can be restricted if the State has carried out an activity for national security purposes.[1516] Therefore, national security

[1512] Article 5(1), Article 7(2), Article 7(bis), and Article 8 of the draft Convention.
[1513] Article 2 of the draft Convention.
[1514] Greenleaf G 2013, 'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?', *Computer Law & Security Review*, vol. 29, no. 4, July/August 2013, pp. 430-436.
[1515] Currently, ten of the forty-five members have been implementing the convention but they have excluded 'State security' matters. WP 228, 05.12.2014, p. 19.
[1516] Article 9a of the draft Convention.

issues can be excluded from the 108 CoE Data Protection Convention. Yet, there is another CoE Convention that does bind national security matters: the CoE Cybercrime Convention.

The Cybercrime Convention (also known as the Budapest Convention) aims at combating all crimes committed through and against electronic networks. It was adopted due to the increasing number of digital crimes or cybercrimes, to the detriment of former 'conventional' crimes.[1517] It is not an instrument directly promoting the right to data protection but it includes a few data protection safeguards such as the establishment of an independent supervisory body (Article 15(2)), the need for data retention rules (Article 16), data security measures (Article 19), and the use of mutual assistance procedures for transnational data exchanges (Articles 25-28), among others. In addition, the Cybercrime Convention establishes a low-intrusive mechanism to preserve crime-related data that is exemplary. It is called the 'quick-freeze' method and it consists of freezing data only after a connected crime has been detected.

As in the 1981 CoE Convention, non-members of the CoE can still ratify the Cybercrime Convention. For the moment, six countries outside the CoE are part of the Convention: Australia, the Dominican Republic, Japan, Mauritius, Panama and the US. Furthermore, eleven other countries have already signed or showed interest in acceding to it in the future. Therefore, the Cybercrime Convention complements the 1981 CoE Convention by offering specific data protection rules in the field of law enforcement[1518] in the Internet age.

Considering the recent revelations proving that intelligence services can access unlimited information and interfere in all available communications, the Cybercrime Convention is of a special relevance. The convention does not include a 'national security' exemption, so it applies to certain intelligence services' activities too. However, the problem is that the Cybercrime Convention does not explicitly cover all mass surveillance activities, but only those data interferences through computer systems. Therefore, it should be amended in order to cover any intelligence services' data processing.

The Cybercrime Convention could, if amended, establish universal data protection standards to be obeyed by law enforcement and intelligence authorities around the

[1517] Van den Hoven van Genderen R 2008, 'Cybercrime investigation and the protection of personal data and privacy', *Council of Europe, Directorate General of Human Rights and Legal Affairs*, 25 May.
[1518] Also in the field of intelligence, as will be seen below.

world. Today forty-five countries are already bound to the convention, including the US, Panama, Mauritius, Japan, Dominican Republic and Australia.[1519] Also, the inclusion of an additional protocol on transborder data flows is currently being discussed. However, the prospects are not looking very positive for the moment. There is a risk that the new framework will soften the conditions for the exchange of crime-related data instead. As the former EDPS Peter Hustinx and the EP have warned, it could result in easier access of intelligence services to personal data.[1520]

### 2.5. Other global data protection principles

Besides the rules proposed by the OECD, the UN, the APEC and the CoE, there are a few other initiatives setting up global data protection and privacy principles. Particularly, the Fair Information Practice Principles (FIPPs), the Madrid Privacy declaration,[1521] the Charter of Digital Rights,[1522] the International Principles on the Application of Human Rights to Communications Surveillance (hereinafter, IPAHRCS),[1523] and the Tshwane Principles[1524] have been created for this purpose. Moreover, Australia, Canada and the EU already have their own core privacy principles. These are the Australian Information Privacy Principles;[1525] the Canadian Generally Accepted Privacy Principles (CICA principles);[1526] and Directive 95/46/EC[1527] and Council Framework Decision 2008/977/JHA[1528] in the EU.

---

[1519] On the signatures, ratifications and entry into force of the convention, see http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG [21.02.2015].

[1520] 'The relation between the surveillance practices in the EU and the US and the EU data protection provisions', *European Parliament, Working Document 3*, 12.12.2013; See also Presstv video 'EU-US data sharing deal seen as NSA's potential spying option', available from http://www.presstv.ir/detail/2013/10/08/328223/euus-data-sharing-deal-seen-as-nsas-potential-spying-option/ [7 November 2014].

[1521] Available from http://thepublicvoice.org/madrid-declaration/ [22 December 2014].

[1522] Avaialble from https://www.wepromise.eu/en/page/charter [22 December 2014].

[1523] Available from https://en.necessaryandproportionate.org/text [22 December 2014].

[1524] The Global Principles on National Security and the Right to Information (Tshwane Principles), 12.06.2013. Available from http://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf [22 December 2014].

[1525] Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which amends the Australian Privacy Act 1988.

[1526] Generally Accepted Privacy Principles issued by the AICPA/CICA, August 2009.

[1527] OJ L 281, 23.11.1995, 31-50.

[1528] OJ L 350, 30.12.2008, 60-71.

*Table 5.1.*

| | FIPPs | Australia IPP | UN guidelines | Canada GAPP | Dir95/46 | CD2008 | Madrid PD | Charter Digital Rights | IPAHRCS | Tshwane | 2013 OECD | APEC | CoE Conv |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Transparency | * | * | | | | | * | * | * | * | * | | |
| Notification and/or consent | * | * | | * | * | * | * | * | * | * | * | * | |
| Data access | * | * | * | * | * | * | | * | | * | * | * | * |
| Data correction | * | * | | | | * | | | | | * | * | * |
| Redress and remedies | * | | * | * | | | * | * | * | * | | | * |
| Purpose specification | * | * | * | * | * | * | | | | | * | * | |
| Use limitation | * | * | | * | * | * | | | | | * | * | |
| Data quality, integrity and accuracy | * | * | * | * | * | * | | | * | | * | * | * |
| Security | * | * | * | * | | * | | * | | | * | * | * |
| Accountability | * | | | * | | | | | | * | * | * | |
| Auditing and Supervision | * | | * | | * | * | * | * | * | * | | | |
| Anonymity and pseudonymity | | * | | | | | | * | | | | | |
| Limited disclosure to third countries | | * | * | * | * | * | | | * | | * | | * |
| Retention | | | | * | * | * | | | | * | | * | * |
| Special categories of data | | * | * | | * | * | | | | * | | | * |
| Necessity and Proportionality | | | | | * | * | | * | * | | * | | |
| Legality/ legitimacy | | | * | | * | * | | | * | * | | * | * |
| Interoperability | | | | | | | * | | | | * | | |

Table 5.1. identifies the principles enshrined in each of these instruments. In order to get a complete overview, it also includes the OECD Privacy Guidelines, the APEC rules, the UN Guidelines and the two CoE Conventions studied above.

As demonstrated in the table, the principles vary from one instrument to the next. Rules on notification, redress, data access, purpose specification, data quality, security, oversight, limited disclosure to third countries and the processing for special categories of data are included in almost all laws. Yet, there is no single principle common to all thirteen documents.

In order to discern the most adequate instrument in the field of public security, the principles applying to public entities first need to be identified. In this sense, FIPPs, UN Guidelines, the Australian principles, Directive 95/46/EC, Council Framework Decision 2008/977/JHA, the Madrid Declaration, IPAHRCS, the Tshwane Principles and the two CoE Conventions apply to the public sector. However, among these, only the Australian principles, Directive 95/46/EC, Council Framework Decision 2008/977/JHA and the two CoE Conventions are mandatory for the Contracting Parties.

Moreover, even if these five instruments compel public bodies, some of them exclude from their scope data processed for 'national security' purposes. These are particularly Directive 95/46/EC and the 1981 CoE Convention. As mentioned in the introduction to this chapter, there is no clarity about what the term 'national security' includes.

The 'national security' exemption is also found in Article 4(3) TEU. As seen in Chapter 4 of this thesis, intelligence agencies' laws and principles are inexistent at the EU level. This is because the EU has always presumed that the activities of intelligence agencies were part of the 'national security' exclusion, while police and judicial bodies activities were part of the AFSJ. Therefore, EU laws within the AFSJ involve law enforcement authorities, but not intelligence services.

The only intelligence agency that has openly claimed its compliance with privacy principles is the NSA. Particularly, the agency has stated that it implements six of the eight FIPPs: purpose specification, data minimisation, use limitation, data quality and integrity, security, and accountability and auditing.[1529] However, as observed above, FIPPs are not binding rules so they cannot be enforced.

[1529] Richards RJ 2014, 'NSA's civil liberties and privacy protections for targeted SIGINT activities under Executive Order 12333', *NSA Director of Civil Liberties and Privacy Office report*, 7 October; 'NSA's

In general terms, the establishment of a global data protection charter setting up common principles for intelligence services seems a very far-off goal for the moment. Some of the intelligence services are not even subject to a national regulation. In order to set up global data protection standards for these agencies, an alignment of the national laws constraining intelligence services is first needed.

The establishment of universal data protection principles for law enforcement bodies is much more feasible. Binding data protection rules for law enforcement authorities already exist in Europe and Australia. In the EU, law enforcement authorities are compelled by Council Framework Decision 2008/977/JHA and by the Europol Framework Decision. In Australia, law enforcement authorities are bound by Australian Information Privacy Principles.[1530] However, it is difficult to turn such principles into universal rules, since they are based on specific territorial laws.

### 3. The ideal regulatory system for a global data protection framework

Despite the existence of all these instruments enshrining international data protection principles, there is no single study to date analysing what the most adequate legal approach would be. There are, today, more than a dozen different legal frameworks establishing data protection rules. Their coexistence is at times confusing, since many of these instruments overlap in scope but they do not invoke the same principles. Also, some are non-binding whereas others have an obligatory nature for its Contracting Parties. Therefore, opposing the de Hert and Papakonstantinou's argument, which supports a 'multi-faceted international approach',[1531] this thesis opts for a dual data protection approach.

My particular preference for a global data protection framework is a combination of the 108 CoE Data Protection Convention and the Cybercrime Convention. As seen above, the principles these conventions enshrine are binding for its Contracting Parties. Today forty-five countries have already ratified the 108 CoE Data Protection Convention, and a further forty-two are bound to the Cybercrime Convention. The US

---

Implementation of Foreign Intelligence Surveillance Act Section 702', NSA Director of Civil Liberties and Privacy Office Report, 16.04.2014, p. 6;

[1530] However, there are some exceptions as regards the compliance of the principles by Australian law enforcement authorities. See 'Privacy and law enforcement agencies'. Available from http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/privacy-and-law-enforcement-agencies [7 November 2014].

[1531] De Hert & Papakonstantinou 2013, p. 309.

has signed the latter and could eventually join the 108 CoE Data Protection Convention since it is currently an observer on the Council of Europe's committee.[1532]

This two-fold system composed of the 108 CoE Data Protection Convention and Cybercrime Convention would establish a robust data protection framework, providing even more consistency than the current EU data protection regime. The EU today has two main instruments that protect EU citizens' data: Directive 95/46/EC and Council Framework Decision 2008/977/JHA. Whereas the latter applies when the data processing is carried out within the context of law enforcement, the former applies for all other non-security matters. The same duality is found in the proposed EU Data Protection Package released in January 2012. Again, it consists of two instruments: one in the form of a directive for law enforcement data exchanges; and a regulation for the rest of data-sharing operations. However, as seen in Chapter 4 of this thesis, no EU data protection rules are in force for intelligence services' activities.

In contrast, by choosing the 108 CoE Convention and Cybercrime Convention as global data protection instruments, all fields would be covered, including data processed by intelligence services. The 108 CoE Convention would apply for commercial and law enforcement purposes; whereas the Cybercrime Convention would be observed when intelligence services process information. This is also an ideal framework, since the majority of EU data-sharing instruments are already using 108 CoE Convention as a threshold.[1533]

Another advantage in choosing the two CoE conventions is that countries are not required to be CoE Contracting Parties accede them. Thus, its success will depend on how non-EU Members perceive the conventions. As an example, numerous non-EU countries and international organisations (the UN, OAS, African Union, APEC, etc.) have participated in the negotiations for the modernisation of the 108 CoE Convention. In order to attract non-CoE parties it is important that the conventions bring credibility, efficient functioning, and enough mechanisms for implementation. Only after doing so could their principles have a global relevance in the future.

However, there is still a lot of work to do in the amendment of both conventions. For instance, one of the current problems in the current Cybercrime Convention is that some Contracting Parties encourage TSPs to move their servers to third countries, which are

[1532] The non-EU countries with observer status are the US, Canada, Japan, Mexico, the Holy See. Accessed from http://www.coe.int/t/der/Observers_en.asp [29 October 2014].
[1533] See, for instance, Article 8 of Swedish Initiative; Article 27 of Europol Council Decision; and Article 25 Council Decision 2008/615/JHA (Prüm).

not part of the convention, in order to circumvent the law. Another issue that should be included in the amended convention is a mechanism by which security actors could directly request data from TSPs and maintain the necessary safeguards for the individuals at the same time.[1534]

It can be concluded that the CoE is the primary candidate among all the existing international organisations for the establishment of data protection and global privacy standards. The organisation has the 1981 CoE Convention, the Cybercrime Convention as well as Article 8 of the ECHR. After the appropriate amendments, these conventions would cover all data protection fields, including intelligence security activities.

### 4. The EU's role in designing global data protection principles through the CoE

As seen in Chapter 2 of this thesis, although the EU is now gaining increasing relevance as an international actor in the field of security, such 'actorness' is not always strong in practice. The CFSP/CSDP and the AFSJ policies are still very much influenced by the interests of member states and third countries.

In the area of data protection, continuous pressures from both private and public entities at the domestic and international levels have caused a lowering of the data protection safeguards in the EU. This has been seen in the current proposal for a EU Data Protection Package, which is composed of two instruments: a regulation and a directive. The regulation establishes data protection rules for information processed in all fields except for law enforcement. The first draft of the regulation included a provision (ex Article 42), which prohibited a government from accessing data stored by a private company without a prior mutual assistance treaty or an international agreement. One month before the proposal was launched, the US government pushed the Commission to remove that clause, and it succeeded: the provision is no longer found in the proposal. Similarly, the proposed directive for data exchanged among law enforcement authorities has been softened because of political interests. First, the fact that the nature of the instrument is a directive and not a regulation means that there will be no uniformity among member states in the implementation of its rules. Moreover, the future directive excludes sectoral data-sharing agreements as well as data processed by EU agencies like Europol and Eurojust. Finally, the proposal will not cover any data

[1534] Speech of Cornelia Kutterer (Microsoft) at CPDP conference, 23.1.2015.

transfer conducted by IntCen and national intelligence services, since these are not considered part of the EU internal security policy.

Chapter 3 has explained how, through Europol, the EU has influenced third countries to adapt their data protection laws as a condition for the adoption of a strategic/cooperation agreement with the agency. If, after a questionnaire, Europol has doubts about the adequacy of the rules in the third country, the agency will visit *in situ* the institutions in charge with the compliance of data protection laws and will advise about the necessary modifications prior to the adoption of the agreement. This procedure is much faster and effective than that in the Proposal of Police and Criminal Justice Data Protection Directive. According to Article 34 of the proposal, the Commission will also assess the adequacy of data protection rules in a third country before accepting international transfers. Yet, Article 36 allows the derogation of such adequacy in case of a) vital or legitimate interest, b) immediate and serious threat to the public security, c) prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and d) establishment, exercise or defence of legal claims. These situations, if interpreted broadly, could be used abusively to transfer massive amounts of data to any third country.

A similar carve-out provision for emergency situations is found in the proposed Europol Regulation too.[1535] However, if we compare these two articles, we see that the list of cases included in the Europol Regulation is much more restrictive than Article 36 of the proposed directive.[1536] Moreover, any derogation under the scope of the future Europol Regulation requires the approval of the Executive Director, the Management Board and even the EDPS, if the transfer is of a set of data. The same conditions do not apply for the proposed directive.

The EU has also used another mechanism to export high data protection standards without directly operating through its own instruments and institutions. This is the Council of Europe (CoE). Despite it being an international organisation outside the scope of the EU institutional structure, the close link between both parties is unquestionable. In 2005, the European Court of Human Rights (ECtHR) expressly stated that the EU provided human rights protection equivalent to that of the

[1535] Article 31(2) of Europol Regulation.
[1536] The reasons are: a) it is absolutely necessary to safeguard the essential interests, b) it is absolutely necessary to prevent imminent danger, c) it is required on important public interest grounds, and d) it is necessary to protect the vital interests of the data subject.

Convention.[1537] This presumption gained consistency with the inclusion of a provision for the accession of the EU to the ECHR in the Treaty of Lisbon.[1538]

Regarding their data protection principles, the same equivalence has existed since the 1980s. In a disconnection clause, the 108 CoE Convention explicitly refers to the Commission's involvement in the negotiations, and its intention to conclude an EC instrument on the same subject:

'The Commission of the European Communities, which carried out studies concerning harmonisation of national legislation within the Community in relation to transborder data flows and possible distortions of competition, as well as problems of data security, kept in close touch with the Council of Europe. The Commission decided to await the outcome of the work on this convention before deciding on its own action in the field of data protection.'[1539]

As prognosticated in the convention, the first data protection instrument in the EU had much in common with its predecessor. In Directive 95/46/EC, the Commission had included exactly the same data protection principles as those in 108 CoE Convention. At first glance, it may seem that the CoE influenced the EU, but in fact the Commission took an active role in designing the convention that it would then cite as a reference in its own directive.

In 2001 an additional protocol was included in the 108 CoE Convention.[1540] It incorporated provisions on supervisory authorities, and the adequacy criteria for data transfers to countries not part of the convention. It is not a coincidence that similar clauses were already found in Directive 95/46/EC. The CoE clearly sought to base its convention on the EU data protection standards. Unfortunately, the additional protocol has not been ratified by all Contracting Parties. At the time of writing this thesis, thirty-

[1537] ECtHR, Bosphorus Hava Yollari Turizm Ve Ticaret Anonim Şirketi v. Ireland, Application no. 45036/98, 05.06.2005.
[1538] For further information about the accession, see Blasi Casagran, 2010, pp. 16-20; see also CJEU opinion 2/13, 18.12.2014.
[1539] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETC No 108, para.16.
[1540] 2001 Additional Protocol to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, ETS, no. 181.

five countries have ratified this protocol, and a further nine have signed it but are pending for ratification.[1541]

Finally, the same mutual influence occurred recently during the negotiations of the 108 CoE Convention's amendment. They started in January 2012, the same month that the Commission released the proposals for a new EU data protection framework. The EU participated actively in shaping the modernised convention.[1542] As in the EU Data Protection Package, the modernised 108 CoE Convention includes clauses on basic principles, sensitive data, data security, transparency, rights of the data subject, sanctions and remedies, data transfers to third countries, and oversight. It has however omitted controversial provisions such as the 'right to be forgotten' or the new sanctions' system that includes the proposed regulation. The negotiations for the new 108 CoE Convention were subject to a lot less pressure from the US government and private companies that the EU Data Protection Package. And still, the EU played a key role in the final outcome.

As this section demonstrates, that there are alternative ways in which global data protection standards could adopt an EU 'style' without coming directly from EU instruments. Besides the Europol's role in exporting EU data protection standards, the CoE has also been the reflection of EU principles since the 1980s. There has always been a mutual influence between both organisations: the 108 CoE Convention has influenced Directive 95/46/EC; and now the EU Data Protection Package is influencing the modernised 108 CoE Convention.

## 5. Conclusions

The great technological progress that has occurred in the last fifteen years has prompted the need to establish global odata protection principles for data processed for the prevention and investigation of crimes. This chapter has examined the feasibility of such principles.

There are many limitations found in the current proposals to establish a common data protection framework for information exchanged in the field of security. One of the

[1541] Information available from http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=1&DF=08/11/2014&CL=ENG [25 February 2015].

[1542] 'Commission to renegotiate Council of Europe Data Protection Convention on behalf of EU', European Commission, 19.11.2012. Available from http://europa.eu/rapid/press-release_MEMO-12-877_en.htm [30 October 2014].

obstacles seen in many of the initiatives for universal data protection principles is that some of them are not binding for its members, and other exclude activities conducted for 'national security' purposes. This study finds that only one international organisation could establish binding common data protection rules for both law enforcement authorities and intelligence services: the Council of Europe. A combination of the 108 CoE Data Protection Convention and the Cybercrime Convention would be the best option for expanding common data protection principles covering all sectors, including the field of security. These two conventions already have more than forty Contracting Parties, including all EU member states and even the US in one of them. Once the modernised 108 CoE Data Protection Convention is released, it could attract further third countries, bringing the institution closer to becoming 'global'. The EU has indirectly participated in the negotiation procedures of the 108 CoE Data Protection Convention and its amendment. Therefore, through the CoE, the EU has found a way of exporting its own data protection principles, free of pressures from private and governmental interests.

It is essential to set up universal principles of data protection that bind any piece of information processed, regardless of its purpose. For data processed for security reasons, more accountability and control needs to be built up. Our history has shown that when governments have unlimited power, it can be easily abused. Therefore, basic principles need to be enforced to avoid abusive restrictions of human rights. Security cannot be used to justify a world in which individuals are permanently monitored by the State with no limitations. Any intrusion needs to be necessary and proportional in relation to the objective it pursues. There is no doubt that privacy is a universal right, so the adoption of a global instrument enforcing that right is the logical next step.

## Conclusions

This thesis has investigated the possibility of establishing global data protection rules for data processed in the field of intelligence and law enforcement. In this regard, it has identified several challenges that need to be overcome for its accomplishment.

Chapter 1 has determined that the creation of global data protection rules requires the EU to first harmonise its data protection framework within the AFSJ. This chapter offers an in-depth analysis on the state-of-play of the instruments and systems that the EU has adopted in order to process data for law enforcement purposes. There are at least nine different EU systems today (Prüm, the Swedish initiative, EIO, ECRIS, VIS, SIS, Eurodac, CIS, ENUs) that exchange information among law enforcement authorities in the member states. In addition, four other EU systems are are likely to be established in the future (EU PNR, TFTS, EES, RTP).

However, the EU data protection regime is rather fragmented. Each of these instruments has its own data protection rules, which in turn differ from the general Framework Decision 2008/977/JHA. Chapter 1 has also identified some of the member states' problems relating to the lack of implementation and usage of these instruments. Police authorities do not use the European information systems in a clear and consistent manner, and some of them do not have the systems fully operational yet. For instance, none of the member states has yet the DNA data searches of Prüm up and running, or the technical infrastructure to use ECRIS. Therefore, under these circumstances, it is impossible to create a global data protection framework if the EU itself does not provide homogeneous rules for the exchange of law enforcement information.

Another challenge to overcome is the lack of an equivalent legal framework on data protection between the US and the EU. Chapter 2 has delineated how the two parties have tried to overcome their legal differences by concluding numerous sectoral data-sharing agreements in the field of law enforcement. These are, in particular, the PNR agreements, the SWIFT agreement, and the EU-US agreement on the security of classified information. Moreover, negotiations for an umbrella EU-US data protection and data privacy agreement are currently ongoing. All of these instruments demonstrate the enormous efforts of both parties to reach a common approach in terms of data protection. However, in practice, all the existing EU-US agreements on data protection matters differ from the EU legal framework for data exchanges in the field of law

enforcement (i.e. Framework Council Decision 2008/977 and the EU proposal for a Police and Criminal Justice Data Protection Directive[1543]).

A third problem encountered in the creation of common global data protection standards is that any law would in principle exclude data exchanges carried out by intelligence services. Chapter 4 of this thesis has examined the increasing synergy between law enforcement and intelligence authorities. In the past, these two communities had very distinctive roles. While intelligence services were mainly conducting pre-emptive analytical tasks ('wait and watch'), police agents had an active role in enforcing the law ('see and strike'). Over the years, that division has become more and more blurred. Law enforcement agencies include analytical departments where police officers collect and process intelligence for the prevention of crimes. Similarly, many intelligence agencies have police departments within their headquarters, allowing a fluent communication between both entities.

Taking all of this into account, Chapter 4 has scrutinised whether the EU could adopt laws and issue court decisions affecting data shared among intelligence services. As seen in chapters 1 and 2, the AFSJ has rules concerning data exchanged among law enforcement authorities within and beyond the EU. The CJEU annulment of the Data Retention Directive case can be seen as one of the main EU achievements in the protection of data processed for law enforcement purposes. The court, for the first time, annulled an entire EU directive for being contrary to the provisions of the EU Charter. Articles 7 and 8 of the Charter are to be respected by any EU instrument that processes and shares data for the prevention, combat, investigation and prosecution of crimes. Also, the court stated that a directive must require member states to implement it in a Charter-compliant way. This is significant for the future of a more centralised, EU-level, harmonised system and, perhaps, for the content of EU-third country agreements. However, the Charter does not apply for areas falling outside the scope of the EU, like national security issues.

Article 4(2) TEU expressly excludes 'national security' matters from the competence of the EU laws. The concept of national security has been associated with intelligence services, but there is no clear definition of what the exact scope of this term is. Moreover, the EU has a new body called IntCen through which intelligence services of the member states are able to meet and exchange information with each other. This

[1543] These instruments have been discussed in chapter 1 sections 4.2.1. and 4.2.3., and chapter 2 sections 3.1.1. and 3.1.2 of this thesis.

implies that the EU currently has a certain degree of participation on intelligence services' matters.

For the establishment of global data protection rules, Chapter 3 suggests using Europol laws as a model. Europol currently operates on the basis of a council decision (ECD), although this will be soon replaced by a regulation. The ECD includes strong data protection provisions that refer to the right of access, correction and deletion; the purpose limitation principle; data retention data quality; and external supervision. Also, Europol uses the privacy-by-design tool SIENA to exchange information with member states and third countries. Thus, Europol's laws offer strong privacy rules, higher than most data protection laws in the member states. Therefore, this study proposes enhancing the role of Europol in cross-border criminal investigations, so as to increase the impact its rules and international agreements could have on EU and non-EU countries.

In fact, Europol has already been expanding its competences over the last ten years. It started as an intergovernmental organisation, regulated by a convention and with the purpose of supporting member states' criminal investigations when it was required. Europol's powers also increased in 2008 when it became an EU agency. Once the current proposed Europol Regulation is adopted, the agency will acquire new competences. For instance, the proposed regulation establishes in Article 6 that Europol will be able to request the initiation of a criminal investigation by national units when it considers that it adds value. Member states will have a deadline of one month to reply on the initiative. If a member state replies with a rejection, this will have to be accompanied by a reasoned justification.

However, the scope of Europol is limited to data shared among law enforcement authorities. Data exchanges among intelligence services are excluded from both the ECD and the future regulation. A way of clarifying intelligence services' activities would be by enhancing IntCen's role. IntCen was created in 1999 as a forum for exchanging sensitive information among intelligence services. At that time, it was called the Joint Situation Centre (SitCen) and was comprised of only seven member states. In 2012 the body was renamed IntCen and transferred to the EEAS. It has undergone organisational and structural changes but a concrete legal basis for its mandate has never been clarified. Chapter 4 of this thesis suggests the use of Article 39 TEU as a legal basis to regulate IntCen's data processing activities.

The terrorist attacks that occurred in Paris in January 2015 could lead to the political will to reinforce Europol and IntCen's powers. Previous terrorist attacks in the EU have led to legislative initiatives, or the unblocking of the legislative processes. Enhancing the Europol and IntCen's mandate and including high data protection standards could give the EU a consistent data protection legal framework in the field of security. Intelligence services and law enforcement authorities in the member states would then have a common body at the EU level, which would end the current divergences within the European borders.

Additionally, Chapter 5 examines the existing initiatives setting up international data protection principles that could regulate data exchanges for law enforcement purposes. These are specifically the Fair Information Practice Principles, the UN Guidelines, the Australian principles, the Madrid Declaration, the International Principles on the Application of Human Rights to Communications Surveillance, the Tshwane Principles, the 108 CoE Data Protection Convention and the Cybercrime Convention. Yet, some of these principles are not binding for the Contracting Parties, and others exclude national security data transfers. After a substantial analysis, Chapter 5 focuses on the principles of the 108 CoE Data Protection Convention together with those in the Cybercrime Convention. Each of these two conventions has more than forty Contracting Parties today. A reformed version of these instruments (a modernised 108 CoE Data Protection Convention is about to be adopted) could serve as a reference for the establishment of global data protection rules among law enforcement and intelligence agencies.

National security issues are excluded from the scope of 108 CoE Data Protection Convention. The same exclusion is found in other instruments such as Directive 95/46/EC, Council Decision 2008/977/JHA and the Treaty of Lisbon itself. However, as mentioned above, neither the CoE nor the EU institutions have formally defined what 'national security' really means. If national security is associated with intelligence services activities, these will not be bound by the 108 CoE Data Protection Convention, but the principles included in the Cybercrime Convention will still apply.

The level of data protection of the CoE and the EU is presumed equivalent. It is not a coincidence that all the principles in the 108 CoE Data Protection Convention are also found in Directive 95/46/EC. Also, the Commission is currently participating in the modernisation of the CoE convention. Whereas Chapter 2 highlights the US influence on specific EU international data-sharing agreements as well as the future EU-US Data Protection Agreement, Chapter 5 identifies the EU's active contribution to the CoE data

protection legislation. The EU has thus been expanding its data protection standards through the CoE. This close relationship could be the keystone for establishing strong data protection rules around the world.

This thesis has shown that the notions of privacy and data protection do not oppose the objective of security, but rather complement it. Chapters 1, 2 and 4 have mentioned numerous mass surveillance programmes and systems consisting of collecting large amounts of data from untargeted individuals. Apart from the potential clash between these systems and the right to data protection, its effectiveness has been questioned. This was precisely one of the issues raised by the CJEU in the Data Retention case. The 'collect-it-all' approach risks overloading databases with irrelevant data, which could divert attention from crucial data. This overabundance of data was an obstacle in the prevention of past terrorist attacks such as those occurred in Madrid and London or, more recently, in the 2012 Boston Marathon bombing. There was an available amount of intelligence, but it was improperly identified and processed.

The importance of privacy and data protection is underlined throughout the five chapters of this thesis. In the field of security, this right can easily be suppressed. 9/11 presented the ideal context to adopt measures that reduced privacy and enhanced security through laws like the Patriot Act. These measures are mostly preventive in nature, and now they have become operational it is extremely difficult to remove them because there are always potential threats that justify them.

For society, the over-surveillance creates the false notion that there is always someone watching and monitoring our actions. In particular, governments believe that constant surveillance can reduce criminal activity because an individuals' fear that someone might be watching may deter them from committing a crime. Jeremy Bentham first propagated the idea of 'permanent visibility' in the 18th century with his design for an institutional building called the 'panopticon'. His panopticon prison was to be a circular structure with prison cells surrounding a central tower (the 'inspection house') from which prison guards could view every cell. The central tower might not always be occupied by guards, but the fact that the prisoners could never know whether they were being watched or not would cause them to self-regulate their own behaviour. Although Bentham's prison was never built, the notion of continual control by the government is found in many other contexts today. As seen in Chapters 1 and 4, law enforcement authorities today have the means to monitor our daily lives with the help of the Internet and phone companies. New technologies play a decisive role in the collection of

information for criminal investigations. Chapter 1 has also shown that private actors collecting information for their own commercial purposes may be required to hand over such data to police or intelligence agents. In order to restrict that phenomenon, the purpose limitation principle should be included in the future global data protection framework.

At the time of finalising this thesis, new EU security measures are in the pipeline. Following the terror attacks linked to Al-Qaeda in Paris on 7 January 2015, member states of the EU activated their security alerts to the highest levels and have decided to adopt new counter-terrorism measures. As an example, fifteen member states have announced that by 2016 they would incorporate national PNR systems for the collection of data from passengers arriving in their countries. Also, other member states decided to enhance the power of the police, allowing them to intercept communications without prior judicial authorisation. These measures assimilate the controversial Patriot Act, adopted in 2001 after the 9/11 attacks.

At the same time, new data protection legislation in the field of law enforcement will soon be passed on both sides of the Atlantic. In the EU, a directive on data protection for police and judicial matters will replace the current Council Decision 2008/977/JHA. In addition, more concrete EU instruments such as the proposed Europol Regulation and the EU PNR Directive will include new data protection provisions for data processed for law enforcement purposes. In the US, several Patriot Act provisions are going to expire in May 2015 so new debates on their necessity and proportionality will surely arise by then. Likewise, US President Obama recently announced that stronger safeguards will be included for data processed through the US Foreign Intelligence Surveillance Act (FISA) and the EO 12333. Mainly, the US President seeks to end the bulk collection of data and to establish better oversight mechanisms for US intelligence agencies. Finally, the EU-US Data Protection Agreement is on its way, and it will set down minimal rules that both parties will need to comply with in the exchange of crime-related data. This agreement is likely to be compatible with the 108 CoE Data Protection Convention, facilitating the establishment of data protection global standards in the future.

Current and future security measures need to strike the right balance between data protection and privacy principles. In June 2013, the Snowden revelations demonstrated that a lack of restrictions for security agents in the collection and processing of personal data could cause serious conflicts with individuals' fundamental rights. In particular, the

exposé about the surveillance programmes used by the NSA has irrevocably damaged the trust that individuals, companies and governments all over the world once had for intelligence services. The curent lack of confidence in security authorities will only be repaired by reinforcing accountability and individual rights. Hence, data protection rules at the global level are now more necessary than ever.

## Bibliography


Abazi V 2013, 'Unveiling the power over Europol's secrets', *Amsterdam Centre for Law and Governance*, Working Paper Series 4, Amsterdam, pp. 1-34.

Abazi V 2014, 'The future of Europol's parliamentary oversight: A great leap forward?', *German Law Journal*, vol. 15 no. 6, pp. 1121-1143.

Aranda Álvarez E 2003, 'Servicios de inteligencia: Un estudio comparado' in *Estudios sobre inteligencia: Fundamentos para la seguridad internacional*, Grupo de Trabajo número 5/03, Instituto Español de Estudios Estratégicos, pp. 103-130.

Archick K 2013, 'U.S.-EU Cooperation against terrorism', *Congressional Research Service*, Report RS22030, pp. 1-24.

Argomaniz J 2010, 'Before and after Lisbon: legal implementation as the 'Achilles heel' in EU counter-terrorism?', *European Security*, vol. 19, no. 2, pp. 297-316.

Argomaniz J 2009, 'When the EU Is the "Norm-taker": The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms', *Journal of European Integration,* vol.31 no.1, pp. 119-136.

Argomaniz J 2012a, 'A coordination nightmare. Institutional coherence in European Union Counterterrorism' in *European Homeland Security. A European Strategy in the making?*, eds. C Kaunert, S Leonard & P Pawlak, Routledge, New York City, pp. 72-93.

Argomaniz J 2012b, 'A rhetorical spillover? Exploring the link between the European Union Common Security and Defence Policy (CSDF) and the external dimension in the EU counterterrorism', *European Foreign Affairs Review*, vol. 17, no. 2/1, pp. 35-52.

Aust HP 2014, 'Stellungsnahme zur Sachverständigenanhörung', Humboldt-Universität zu Berlin, 5 June. Available from <www.bundestag.de> [6 November 2014].

Baker J 2013, 'EU Parliament could block data sharing with the US', *CSO*, 19 November. Available from <http://www.cso.com.au> [6 November 2014].

Bäcker M & Hornung G 2012, 'Data processing by police and criminal justice authorities in Europe - The influence of the Commission's draft on the national police laws and laws of criminal procedure', *Computer Law & Security Review*, vol. 28 no. 6, pp. 627-663.

Bamberger K & Mulligan D 2013, 'Privacy on the ground: Governance choices and corporate practice in the U.S. and Europe', *George Washington Law Review*, vol. 81, no. 5, pp. 1529-1664.

Bamford J 1982, *The Puzzle Palace - A Report on America's Most Secret Agency,* Houghton Mifflin, Boston.

Baldaccini A 2008, 'Counter-Terrorism and the EU strategy for border security: Framing suspects with biometric documents and databases', *European Journal of Migration and Law*, vol. 10, no. 1, pp. 31-49.

Barros X 2012, 'The external dimension of EU counter-terrorism: the challenges of the European Parliament in front of the European Court of Justice', *European Security*, vol. 21 no. 4, pp. 518-536.

Baumeister P 2008, 'Das Subsdiaritätprinzip und seine Bedeutung im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen', *Alternativenentwurf Europol und europäischer Datenschutz*, eds. Jürgen Wolter, Wolf-Rüdiger Schenke, Hans Hilger, Josef Ruthig, Mark A. Zoller. C.F.Müller Wissenschaft, pp. 158-169.

Bellanova R & Duez D 2012, 'A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage', *European Foreign Affairs Review* vol. 17, no. 1/2, pp. 109-124.

Bender D 2014, 'Why is the U.S. on the defensive?', *IAPP*, 14 March. Available from <https://privacyassociation.org> [23 November 2014].

Bergen P, Sterman D, Schneider E & Cahall B, 'Do NSA bulk surveillance programs stop terrorists?', *New America Foundation*. Available from <http://www.newamerica.org> [5 November 2014].

Bergen P 2013, 'Would NSA surveillance have stopped 9/11 plot?', *CNN*, 31 December. Available from <www.cnn.com> [5 November 2014].

Bickford D 2013, 'Judicial Scrutiny of Intelligence Agencies', European Parliament LIBE enquiry, 7 November. Available from <www.europarl.europa.eu> [6 November 2014].

Biermann K 2013, 'German intelligence service is as bad as the NSA', *The Guardian*, 4 October. Available from < http://www.theguardian.com> [5 November 2014].

Bigo B, Carrera C, Hayes H, Hernanz N & Jeandesboz J 2012, 'Justice and Home Affairs databases and a smart borders system at EU External borders. An evaluation of current and forthcoming proposals', *CEPS Paper in Liberty and Security in Europe*, no. 52, Brussels.

Blachier G & Irish J 2015, 'France mobilizes 10,000 troops at home after Paris shootings', *Reuters*, 12 January. Available from <www.reuters.com> [1 February 2015].

Blasi Casagran C 2012, 'The reinforcement of fundamental rights in the Lisbon Treaty' in *The European Union after Lisbon*, ed. Søren Dosenrode, Ashgate Publishing Ltd, Surrey, pp. 75-94.

Blasi Casagran C & Blasi Casagran E 2012, 'Spain makes Google remove personal information from index', *Privacy, Laws & Business, International Report*, no. 120, pp. 27-30.

Blasi Casagran C 2013 'People c. Harris: El lado oscuro de la libertad de expresión en las redes sociales' in *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*, eds. Cotino Hueso L & Corredoira Alfonso L, Centro Estudios Políticos y Constitucionales, Madrid, pp. 306-319.

Boehm F 2011, 'EU PNR: European Flight passengers under general suspicion. The Envisaged European Model of Analyzing Flight Passenger Data' in *Computers, Privacy and Data Protection: An Element of Choice,* eds: Gutwirth S, Poullet Y, de Hert P & Leenes R, Springer, Berlin, pp. 171-199.

Boehm F 2012a, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Springer, Berlin.

Boehm F 2012b, 'Information sharing in the Area of Freedom, Security and Justice – Towards a common standard for data exchange between agencies and EU information systems' in *European Data Protection: In Good Health?*, eds. Gutwirth S, Leenes R, de Hert P & Poullet Y, Springer, Berlin, pp. 143-184.

Boehm F 2012c, 'Data processing and law enforcement access to information systems at EU level', *Datenschutz und Datensicherheit*, vol. 36 no. 5, pp. 339-343.

Boehm F & Cole M.D. 2014, 'Data Retention after the Judgement of the Court of Justice of the European Union', *Greens/EFA Group, European Parliament*, Brussels. Available from <http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf> [2 November 2014].

Bossong RS 2008, 'The Action Plan on combating terrorism – A flawed instrument of EU security governance', *Journal of Common Market Studies,* vol. 46 no. 1, pp. 27-48.

Bowcott O 2014, 'Social media mass surveillance is permitted by law, says top UK official', *The Guardian*, 17 June. Available from <www.theguardian.com> [6 November 2014].

Bowden C 2013, 'The US surveillance programmes and their impact on EU citizens' fundamental rights', PE 474.405, *Policy Department Citizens' Rights and Constitutional Affairs, European Parliament*, Brussels.

Brkan M 2012, 'The role of the European Court of Justice in the field of Common Foreign and Security Policy after the Treaty of Lisbon: New challenge for the future' in *EU external relations law and policy in the post-Lisbon era*, ed. Paul-James Cardwell, Springer, Berlin, pp. 97-118.

Bryant C & Fontanella-Khan J 2013, 'US spy scandal sparks EU privacy fears', *Financial Times*, 15 October. Available from <www.ft.com> [6 November 2014].

de Buck B 2007, 'Joint Investigation Teams: The participation of Europol officials', *ERA Forum*, no. 8, pp. 253–264.

Bunyan T 1993 ‘Trevi, Europol and the European state’, *Statewatching the new Europe*, pp. 1-15.

Bunyan T 2013, ‘Interception Commissioner fails to report on Section 8(4) certificates authorising GCHQ's mass data collection’, *Statewatch*. Available from <www.statewatch.com> [6 November 2014].

Bunyan T 2014, ‘GCHQ is authorised to “spy on the world” but the UK Interception of Communications Commissioner says this is OK as it is “lawful”, *Statewatch*. Available from <www.statewatch.com> [6 November 2014].

Bures O 2008, ‘Europol's fledgling counterterrorism role’, *Terrorism and Political Violence*, vol. 20 no. 4, pp. 498-517.

Bures O 2011, *EU Counterterrorism Policy. A Paper Tiger?,* Ashgate, Surrey.

Bures O 2013, ‘Europol's counter-terrorism role: A chicken-egg dilemma’, *European Security, Terrorism and Intelligence. Tackling New Security Challenges in Europe*, eds. Kaunert C & Léonard S, Palgrave Macmillan, pp. 65-93.

Bures O & Ahern S 2007, ‘The European Model of Building Regional Cooperation Against Terrorism’ in *Uniting against Terror. Cooperative nonmilitary responses to the global terrorist threat*, eds. D Cortright & GA López, Massachusetts Institute of Technology Press, Massachusetts, pp. 187-236.

de Busser E 2009, ‘Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities’, *Maklu Publishers*, Antwerpen.

de Busser E 2010, ‘EU data protection in transatlantic cooperation in criminal matters. Will the EU be serving its citizens an American meal?’, *Utrecht Law Review*, vol. 6, no. 1, pp. 86-100.

Busuioc M & Groenleer M 2013, ‘Beyond Design: The evolution of Europol and Eurojust’, *Perspectives on European Politics and Society*, vol. 14 no. 3, pp. 285-304

Buzan B 2007, ‘What is national security in the age of globalisation?’, *Utenrisksdepartementet*. Available from <http://www.regjeringen.no> [5 November 2014].

Callahan ME 2010, ‘New international privacy principles for law enforcement and security”, *The Privacy Advisor, The Official Newsletter of the International Association of Privacy Professionals (IAPP*), 1 January. Available from <http://www.dhs.gov> [23 November 2014].

Campbell C 1988, ‘Somebody’s listening’, *New Statesman*, 12 August. Available from <http://www.newstatesman.com> [5 November 2014].

Carrapiço H & Trauner F 2014, 'Europol and its influence on EU policy-making on organized crime: analyzing governance dynamics and opportunities', *Justice and Home Affairs Agencies in the European Union,* eds. Kaunert C, Léonard S & Occhipinti JD, Oxford, pp. 85-97.

Cate FH, Cullen P & Mayer-Schönberger V 2013, 'Data Protection Principles for the 21st Century. Revising the 1980 OECD Guidelines', Oxford Internet Institute (OII), University of Oxford.

Cavoukian A, Dix A and El Emam K 2014, 'The unintended consequences of privacy paternalism', *Information and Privacy Commissioner Ontario, Canada*, 5 March.

Champeau G 2013, 'Les députés enverront-ils l'article 13 de la LPM au Conseil Constitutionnel?', *Numerama*, 11 December. Available from <http://www.numerama.com/> [5 November 2014].

Coolsaet R 2010, 'EU counterterrorism strategy: value added or chimera?', *International Affairs*, vol. 86, no. 4, pp. 857-873.

Cremona M 2008a, 'EU External Action in the JHA Domain: A Legal Perspective', *EUI Working Papers Law* 2008/24, *European University Institute*, Florence, pp. 1-31.

Cremona M 2008b, 'Defining Competence in EU External Relations: Lessons From the Treaty Reform Process' in *Law and Practice of EU External Relations*, eds. Dashwood & Maresceau, Cambridge, pp. 34-69.

Cremona M 2009, 'EC competence, 'Smart Sanctions' and the Kadi case', in *Challenging the EU Counter-terrorism Measures through the Courts*, eds Cremona M, Francioni F & Poli P, EUI Working Papers AEL 2009/10, Florence, pp. 71-98.

Cremona M 2011, 'Justice and Home Affairs in a globalised world: Ambitions and reality in the tale of the EU-US SWIFT Agreement', *Austrian Academy of Sciences, Institute for European Integration Research,* Working Paper No. 04/2011, pp. 1-30.

Cross MKC 2013, 'A European transgovernmental intelligence network and the role of IntCen', *Perspectives on European Politics and Society*, vol. 14 no. 3, pp. 388-402.

Curtin D 2011,'Top Secret Europe', Inaugural Lecture, *Universiteit vvan Amsterdam*. Available from <http://dare.uva.nl/document/2/103309> [2 November 2014].

Davenport TH & Prusak L 2000, *Working knowledge: How organizations manage what they know?*, Harvard Business School Press, Boston.

Davis W 2013 'Tech Companies Call For Privacy Oversight After Latest NSA Revelation', *Mediapost*, 1 November. Available from <http://www.mediapost.com> [5 November 2014].

Disley E, Irving B, Hughes W& Patruni B 2012, '*Evaluation of the implementation of the Europol Council Decision and of Europol's activities*', RandEurope, The Hague.

Docksey C 2014, 'The European Court of Justice and the decade of surveillance' in *Data Protection Anno 2014: How to restore trust? Contributions in honour of Peter Hustinx European Data Protection Supervisor 2004-2014*, eds. Hielke Hijmans, Herke Kranenborg, Intersentia, Cambridge.

Eckes C 2011, 'The legal framework of the European Union's counter-terrorist policies: full of good intentions?' in *Crime within the AFJS: A European Public Order*, Cambridge University Press, Cambridge, pp. 127-158.

Eddy M 2013, 'For Western Allies, a Long History of Swapping Intelligence', *The New York Times*, 9 July. Available from <www.thenytimes.com> [5 November 2014].

Farivar C 2013, 'German NSA has deal to tap ISPs at major Internet Exchange', *Ars Technica*, 7 October. Available from <http://arstechnica.com/> [5 November 2014].

Faull J & Soreca L 2008, 'EU-US Relations injustice and Home Affairs', *Justice, Liberty, Security: New Challenges for EU External Relations*, eds. Martenczuk B & van Thiel S, VUBPress, Brussels, pp. 393-420.

Ferreira-Pereira LC & Oliveira Martins B 2012, 'The external dimension of the European Union's counter-terrorism: an introduction to empirical and theoretical developments', *European Security*, vol. 21, no. 4, pp. 459-473.

Follorou J & Greenwald G 2013, 'France in the NSA's crosshair : phone networks under surveillance', *Le Monde*, 21 October. Available from <www.lemonde.fr > [5 November 2014].

Follorou J & Johannes F 2013, 'Révélations sur le Big Brother français', *LeMonde*, 4 July. Available from <www.lemonde.fr> [6 November 2014].

Fox B 2012, 'Commission pushes for document secrecy despite court judgement', *EUObserver*, 8 May. Available from <http://euobserver.com> [6 November 2014].

Gallagher R 2014a, 'How Secret Partners Expand NSA's Surveillance Dragnet', *The Intercept*, 18 June Available from <https://firstlook.org/theintercept/> [5 November 2014].

Gallagher R 2014b, 'The surveillance engine: How the NSA built its own secret Google', *The Intercept,* 25 August. Available from <https://firstlook.org/theintercept/> [5 November 2014].

Gallaguer R & Greenwald G 2014, 'How the NSA Plans to Infect 'Millions' of Computers with Malware', *The Intercept*, 12 March. Available from <https://firstlook.org/theintercept/> [5 November 2014].

Gellman B & Poitras L 2013, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program', *The Washington Post*, 6 June. Available from <www.washingtonpost.com> [5 November 2014].

Gless S 2008, 'Zusammenarbeit von Europol mit Drittenstaaten und Drittenstellen', *Alternativenentwurf Europol und europäischer Datenschutz*, eds. Wolter J, Schenke WR, Hilger H, Ruthig J & Zoller MA, C.F. Müller Wissenschaft, pp. 346-363.

Glüsing J, Poitras L, Rosenbach M & Stark H 2013, 'Fresh Leak on US Spying: NSA accessed Mexican President's email", *Spiegel*, 20 October. Available from <http://www.spiegel.de> [22 December 2014]

de Goede M 2012, 'The SWIFT Affair and the Global Politics of European Security', *Journal of Common Market Studies*, vol. 50, no. 2, pp. 214-230.

González Fuster G 2014, 'The emergence of personal data protection as a fundamental right of the EU', *Springer*, London.

Görlitz N 2013 'Le droit d'enquête du Parlement européen', *Cahiers de droit européen 49*, pp. 783-820.

Greenleaf G 2013, 'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?', *Computer Law & Security Review*, vol. 29, no. 4, July/August 2013, pp. 430-436.

Greenwald G 2014, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Hamish Hamilton, London.

Greenwald G & Ackerman S 2013, 'NSA collected US email records in bulk for more than two years under Obama', *The Guardian*, 27 June. Available from <http://www.theguardian.com> [5 November 2014].

Greenwald G & Aranda A 2013a, 'El CNI facilitó el espionaje masivo de EEUU a España', *El Mundo*, 30 October. Available from <www.elmundo.es> [6 November 2014].

Greenwald G & Aranda A 2013b, ' La NSA espió 60 millones de llamadas en España en solo un mes', *El Mundo*, 28 October. Available from <www.elmundo.es> [6 November 2014].

Guasch Portas V 2014, 'Las transferencias internacionales de datos en la normativa española y comunitaria', *Agencia Estatal Boletín Oficial del Estado*, Madrid.

Guzman AT & Meyer T 2011, 'International Soft Law', *UC Berkeley, Public Law and Legal Theory Research Paper Series*, Berkeley.

Hager N 1996, 'Secret Power - New Zealand's role in the International spy network', *Craig Potton Publishing*, New Zeland.

Hayes B 2004, 'From the Schengen Information System to SIS II and the Visa Information (VIS): the proposals explained', *Statewatch Analysis*. Available from <http://www.statewatch.org/news/2005/may/analysis-sisII.pdf> [1 November 2014].

Hayes B & Jones C 2013, 'Catalogue of EU Counter-Terrorism Measures Adopted since 11 September 2001', *SECILE: Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness*. Available from <secile.eu> [22 October 2014].

Hayes B & Vermeulen M 2012, *Borderline. The EU's new border surveillance initiatives assessing the costs and fundamental rights implications of EUROSUR and the "Smart Borders" proposals*, Heinrich Böll Foundation, Berlin.

Haaland Matlary J 2013, *European Union security dynamics. In the new national interest*, Palgrave Macmillan, London.

Hernanz N 2011, 'More surveillance, more security? The landscape of surveillance in Europe and challenges to data protection and privacy – Policy report on the proceedings of a conference at the European Parliament', *SAPIENT Deliverable 6.4*. Available from <http://www.sapientproject.eu/docs/D6.4-Policy-Brief-submitted-January-2012-29.pdf> [23 October 2014].

de Hert P & de Schutter B 2008, 'International transfers of data in the field of JHA: The lessons of Europol, PNR and Swift' in *Justice, Liberty, Security: New Challenges for EU External Relations, from Justice, Liberty, Security: New Challenges for EU External Relations*, eds. Bernd Martenczuk & Servaas van Thiel, VUBPress, Brussels, pp. 299-334.

de Hert P & Papakonstantinou V 2009, 'The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for', *Computer Law & Security Review*, vol. 25, pp. 403-414.

de Hert P & Papakonstantinou V 2009, 'The PNR Agreement and transatlantic anti-terrorism co-operation: No firm human rights framework on either side of the Atlantic', *Common Market Law Review 46*, pp. 885-919.

de Hert P & Papakonstantinou V 2013, 'Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN Agency?', *I/S: a Journal of Law and Policy for the Information Society*, vol. 9, no. 3, pp. 271-324.

de Hert & Bellanova R 2009, 'Data protection in the Area of Freedom, Security and Justice. A system still to be fully developed?', *European Parliament, Directorate General Internal Policies of the Union, Policy Department C, Citizens' Rights and Constitutional Affairs*, PE 410.692, pp. 1-32.

Heyder M 2014, ' The APEC cross-border privacy rules – Now that we've built it, will they come?', *Privacy perspectives*, 4 Septiembre. Available from <https://privacyassociation.org> [6 November 2014].

Heumann S & Scott B 2013 'Law and policy in Internet surveillance programs: United States, Great Britain and Germany', *Stiftung Neue Verantwortung,* vol. 25, no. 13, pp.1-17.

Hijmans H & Scirocco A 2009, 'Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?', *Common Market Law Review*, vol. 46, no. 5, pp. 1485-1525.

Hillebrand C 2012, *Networks in the European Union. Maintaining democratic legitimacy after 9/11*, Oxford University Press, Oxford.

Hillebrand C 2013, 'Guarding EU-wide counter-terrorism policing: The struggle for sound parliamentary scrutiny of Europol' in *European Security, Terrorism and Intelligence. Tackling New Security Challenges in Europe*, eds. Kaunert C & Léonard S, Palgrave Macmillan, pp. 96-124.

Hinarejos A 2009, 'Judicial Control in the European Union. Reforming Jurisdiction in the Intergovernmental Pillars', *Oxford Studies in European Law*, pp. 154-163.

Hinarejos A 2011, 'Law and order and internal security provisions in the Area of Freedom, Security and Justice: before and after Lisbon' in *Crime within the AFSJ*, eds. Christina Eckes and Theodore Konstadinides, Cambridge University Press, Cambridge, pp. 249-271.

Hinarejos A, Spencer JR & Peers S 2012, 'Opting out of EU Criminal law: What is actually involved?', *CELS Working Paper*, New Series, no. 1, Cambridge.

Hondius F.W. 1983, 'A Decade of International Data Protection', *Netherlands International Law Review,* pp. 103-128.

Hughes JT 2013, 'Bridging the EU-US privacy gap', *IAPP*, 22 April. Available from <https://www.privacyassociation.org > [23 November 2014].

Hustinx P 2012, 'Ensuring stronger, more effective and more consistent protection of personal data in the EU', *NewEurope*, 2 February. Available from <http://www.neurope.eu> [5 December 2014].

Inglis JC 2013, statement in 'Strengthening privacy rights and national security: Oversight of FISA surveillance programs: Hearing before the S. Comm. on the judiciary', 113th Congress.

Jones C 2011, 'Implementing the "principle of availability": The European Criminal Records Information System, The European Police Records Index System, The Information Exchange Platform for Law Enforcement Authorities', *Statewatch Analysis*. Available from <www.statewatch.com> [22 October 2014].

Jones C 2012, 'Complex, technologically fraught and expensive □ the problematic implementation of the Prüm Decision', *Statewatch Analysis*. Available from <www.statewatch.com> [31 October 2014].

Kamen A 2014, 'The NSA has a new, first time ever, privacy officer', *The Washington Post*, 28 January. Available from <www.washingtonpost.com> [5 November 2014].

Kaufmann S 2013, 'Europe, Lost on the Digital Planet', *The New York Times,* 14 October. Available from <www.nytimes.com> [6 November 2014].

Kaunert C 2010, 'Europol and EU Counterterrorism: International security actorness in the external dimension', *Studies in Conflict & Terrorism,* no. 33, pp. 652–671.

Kaunert C 2012 'Conclusion: assessing the external dimension of EU counter-terrorism –ten years on', *European Security*, vol. 21 no. 4, pp. 578-587.

Kaunert C, Léonard S & MacKenzie A 2012, 'The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT', *European Security*, vol. 21, no. 4, pp. 474-496.

Kaunert C & Zwolski K 2013, 'The EU as a global security actor: A comprenhensive analysis beyond CFSP and JHA', *Palgrave Studies in European Union Politics*, Basingstoke.

Khan Z 2006, 'The National Security Agency (NSA) eavesdropping on Americans. A programme that is neither legal nor necessary', *Utrecht Law Review*, vol. 2, no. 2, pp. 61-80

Kokott J & Sobotta C 2013, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law*, vol. 3, no. 4, pp. 222-228.

Korff D 2014, 'Expert Opinion prepared for the Committee of Inquiry of the Bundestag into the "5EYES" global surveillance systems revealed by Edward Snowden', *Committee Hearing, Paul-Löbe-Haus*, Berlin.

Koutrakos P 2013, 'The EU common security and defence policy', Oxford University Press, Oxford.

Kropf J & Crompton M 2013, 'The EU and APEC: A roadmap for global interoperability?', *IAPP*, 26 November. Available from <www.privacyassociation.org> [6 November 2014].

Kuner C 2013, 'The transatlantic divide over data privacy rights', *IAPP*, 20 May. Available from <www.privacyassociation.org> [23 November 2014].

Kurowska X & Pawlak P 2009, 'Introduction: The Politics of European Security Policies', *Perspectives on European Politics and Society*, vol. 10 no. 4, pp. 474-485.

Kurth Cronin A & Ludes JM 2004, *Attacking terrorism: Elements of a grand strategy*, Georgetown University Press, Washington D.C.

Lavenex S & Wichmann N 2009, 'The external governance of EU Internal Security', *Journal of European Integration*, vol. 31, no. 1, pp. 83-102.

Ledgett R 2014, 'The NSA responds to Edward Snowden's TED Talk', *TED2014*. Available from <http://www.ted.com> [5 November 2014].

Lenoir F 2013, 'United States tracked Merkel's phone since 2002: report', *Reuters*, 26 October. Available from <www.reuters.com> [5 November 2014].

Leonard S & Kaunert C 2013, 'Introduction - Beyond EU Counter-terrorism Cooperation: European Security, Terrorism and Intelligence', *European Security, Terrorism and Intelligence. Tackling New Security Challenges in Europe*, eds. Leonard S & Kaunert C, *Palgrave Macmillan*, Hampshire, pp.1-14

Lewis P 2013, 'NSA denies discussing Merkel phone surveillance with Obama', *The Guardian*, 27 October. Available from <www.theguardian.com> [5 November 2014].

Lichtblau E & Risen J 2006, 'Bank data is sifted by U.S. in secret to block terror", *The New York Times*, June 23. Available from <www.nytimes.com> [21 November 2014].

Longo F 2013, 'Justice and Home Affairs as the new dimension of the European security concept', *European Foreign Affairs Review*, vol. 18, no. 1, pp. 29-46.

Lööf R 2008, *Defending liberty and structural integrity: a social contractual analysis of criminal justice in the EU*, Ph.D thesis, European University Institute, Florence.

Lowenthal M 1998, 'Open Source Intelligence: New Myths, New Realities', *Defense Daily International*, Special Reports. Available from <http://www.oss.net> [5 November 2014].

Luchtman M 2011 'Choice of forum in an area of freedom, security and justice', *Utrecht Law Review*, vol. 7, no. 1, pp. 44-101.

MacAskill E & Ball J 2013, 'Portrait of the NSA: no detail too small in quest for total surveillance', *The Guardian*, 2 November. Available from <www.theguardian.com> [6 November 2014].

MacAskill E, Borger J, Hopkins N, Davies N & Ball J 2013, 'Mastering the Internet: how GCHQ set out to spy on the world wide web' 23 June. Available from <www.theguardian.com> [6 November 2014].

MacKenzie A 2012, 'The external dimension of European homeland security', *European Homeland Security. A European strategy in the making?*, eds. Kaunert C, Leonard S & Pawlak P, Routledge, NYC.

Mackenzie A, Bures O, Kaunert C & Léonard S 2013, 'The European Union Counter-terrorism Coordinator and the External Dimension of the European Union Counter-terrorism Policy', *Perspectives on European Politics and Society*, vol. 14 no. 3, pp. 325-338.

Mangiaracina A 2014, 'A new and controversial scenario in the gathering of evidence at the European level: The proposal for a Directive on the European Investigation Order', *Utrecht Law Review*, vol. 10, no. 1, pp. 113-133.

Maier CS 1990, *Peace and security for the 1990s*. Unpublished paper for the MacArthur Fellowship Program, Social Science Research Council, NYC.

Mangold P 1990, *National security and international relations*, Routledge, NYC.

Matlary JH 2009, 'European Union security dynamics. In the new national interest', *Palgrave Macmillan*, Basingstoke.

Miller V 2014 'The UK block opt-out in police and judicial cooperation in criminal matters: recent developments', *House of Commons, International Affairs and Defence Section, Standard Note: SN/IA/6930,* 10.11.2014.

Mills M, Vermeulen M, Born H, Scheinin M, Wiebusch M & Thornton A 2011, 'Parliamentary oversight of security and intelligence agencies in the European Union', *European Parliament- Directorate General for Internal Policies, Policy Department c: Citizens' rights and Constitutional Affairs*, Brussels.

Moerel L 2014, 'SWIFT revisited- When do the Directive and the proposed Regulation apply' in *Data Protection anno 2014: How to restore trust. Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014),* eds. Hijmans H & Kranenborg H, Mortsel, pp.159-174.

Monar J 2005, 'The European Union and the challenge of September 11, 2001: Potential and limits of a "new" actor in the fight against international terrorism' in *September 11, 2001: A turning point in international and domestic law?*, eds. Eden P & O'Donnell, Transnational Publishers, Inc, Ardsley, NYC, pp. 387-419.

Monar J 2012, 'The External Dimension of the EU's Area of Freedom, Security and Justice. Progress, potential and limitations after the Treaty of Lisbon', *Swedish Institute for European Policy Studies*, report no.1, Stockholm.

Moret Millás V 2005, 'El Centro Nacional de Inteligencia: Un aproximación a su régimen jurídico', *Foro Nueva época*, no. 2, pp. 249-295.

Mounier G 2009, 'Europol: A new player in the EU external policy field?', *Perspectives on European Politics and Society,* vol. 10, no. 4, pp. 582-602.

Navarro Bonilla D 2005, 'Introducción' in *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional,* Grupo de Trabajo número 5/04, Dirección General de Relaciones Institucionales de la Defensa. Instituto Español de Estudios Estratégicos, Madrid.

Neal RW 2013, 'Yahoo wins victory against PRISM: FISA court orders NSA to declassify documents', *Ibtimes*, 16 July. Available from <http://www.ibtimes.com> [5 November 2014]

Ni Loideain N 2011, 'The EC Data Retention Directive: Legal implications for privacy and data protection' in *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices,* eds. Akrivopoulou C & Psygkas A, IGI Global, Hershey, pp. 256-272.

Nichols M 2014, 'Germany, Brazil push the U.N. to be tougher on digital spying', *Reuters*, 6 November. Available from <www.reuters.com> [8 November 2014].

Nielsen N 2012, 'EU hands personal data to US authorities on daily basis', *EUobserver*, 22 June. Available from < http://euobserver.com/22/116719> [10 December 2014].

Nielsen N 2013, 'EU asks for answers on UK snooping programme', *EUobserver*, 26 June. Available from <http://euobserver.com/justice/120656> [6 November 2014].

Nielsen N 2015, 'No new mandate for EU intelligence centre', *EUobserver*, 6 February. Available from <https://euobserver.com/justice/127532> [18 February 2015].

Nino M 2010, 'The protection of personal data in the fight against terrorism. New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon', *Utrecht Law Review*, vol. 6 no. 1, pp. 62-85.

Noack N 2014, 'Yes, Berlin has its own spying scandals, but don't expect Germany to forgive the NSA', *The Washington Post*, 20 August. Available from <www.washingtonpost.com> [6 November 2014].

Occhipinti JD 2013, 'Availability by Stealth? EU information-sharing in transatlantic perspective', *European Security, Terrorism and Intelligence. Tackling New Security Challenges in Europe*, eds. Kaunert C & Leonard S, Palgrave Macmillan, Hampshire, pp. 143-184.

Oliveira Martins B & Ferreira-Pereira LC 2012a, 'Stepping inside? CSDP missions and EU counter-terrorism', *European Security*, vol. 21, no. 4, pp. 537-556.

Oltermann P 2014, 'NSA tapped German ex-chancellor Gerhard Schröder's phone – report', *The Guardian*, 4 February. Available from <http://www.theguardian.com> [22 December 2014]

Ondrejova A 2008, 'Implementation of the principle of mutual recognition in criminal matters', *European Criminal Law Academic Network*. Available from <www.eclan.eu/Utils/ViewFile.aspx?MediaID=542&FD=4E > [23 October 2014].

O'Brien KJ 2013, 'Europe weighs requiring to disclose data breaches', *New York Times*, 16 January. Available from <www.nytimes.com> [02.03.2015].

O'Neill M 2012, *The Evolving Counter-Terrorism Legal Framework,* Routledge Research in EU Law, New York.

Omand D 2010, *Securing the State (Intelligence and security)*, Oxford University Press, Oxford.

Ortiz C 2013, 'Security partnerships, intelligence and the recasting of the UK monopoly of violence in the 21st Century' in *Counter-terrorism and Intelligence in Europe,* eds. Kaunert C & Leonard S, Palgrave Macmiltan, Hampshire, pp. 215-228.

Padova Y 2014, 'PRISM scandal threatens EU-US 'Safe Harbour' agreement', *EurActiv*, 12 November. Available from <www.euractiv.com> [14 November 2014].

Paleri P 2008, 'National Security: Imperatives and Challenges', *Tata McGraw-Hill*, Delhi.

Pateraki A 2011, 'The Implementation of the Data Retention Directive' in *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices,* eds. Akrivopoulou C & Psygkas A, IGI Global, Hershey, pp. 317-328.

Pawlak P 2009a, 'The external dimension of the Area of Freedom, Security and Justice: Hijacker or hostage of cross□pillarization?', *Journal of European Integration*, vol. 31, no. 1, pp. 25-44.

Pawlak P 2009b, 'Network Politics in Transatlantic Homeland Security Cooperation', *Perspectives on European Politics and Society*, vol. 10 no. 4, pp. 560-581.

Pawlak 2012, 'Homeland security in the making American and European patterns of transformation', *European Homeland Security. A European strategy in the making?*, eds. Kaunert C, Leonard S & Pawlak P, Routledge, NYC, pp. 15-34.

Peers S 2012, 'Analysis. The Directive on data protection and law enforcement: A Missed Opportunity?', *Statewatch*. Available from <www.statewatch.com> [4 November 2014].

Peers S 2014, 'Are data retention laws within the scope of the Charter?', *EU Law Analysis. Blog about developments in EU Law*, 20.04.2014. Available from <http://eulawanalysis.blogspot.com.es> [2 November 2014].

Pell SK 2012, 'Systematic government access to private-sector data in the United States', *International Data Privacy Law*, vol. 2, no. 4, pp. 245-254.

Peral M 2013, 'La fiscal pide el documento del espionaje de la NSA en España', *El Mundo*, 5 November. Available from <www.elmundo.com> [6 November 2014].

Peterson A 2013, 'PRISM already gave the NSA access to tech giants. Here's why it wanted more', *The Washington Post*, 30 November. Available from <http://www.washingtonpost.com> [5 November 2014].

Piodi F & Mombelli Y 2014, 'L'affaire ECHELON. Les travaux du Parlement européen sur le système global d'interception 1998 – 2002', *EPRS Service de Recherche du Parlement européen*, PE 538.877, Brussels.

Polakiewicz J 2011, 'International Data Protection Conference Convention 108 as a global privacy standard', Speech in Budapest, 17 June Available from <www.coe.int> [6 November 2014].

Pop V 2011, 'Unhappy MEPs to approve passenger data deal', *EU Observer*, 11 November. Available from <http://euobserver.com/justice/114252> [21 November 2014].

Porter AL & Bendiek A 2012, 'Counterterrorism cooperation in the transatlantic security community', *European Security*, vol. 21, no. 4, pp. 497-517.

Powers T 2004, 'Intelligence wars: American secret history from Hitler to Al-Qaeda', *NYREV*, NYC.

Pulido Gragera J 2004, 'El papel de la inteligencia en la PESD', *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional*, Dirección General de Relaciones Institucionales de la Defensa. Instituto Español de Estudios Estratégicos, Grupo de Trabajo número 5/04, pp. 62-83.

Quesada Gámez M & Mincheva E 2012, 'No data without protection? Re-thinking transatlantic information Exchange for law enforcement purposes after Lisbon' in *EU external relations law and policy in the post-Lisbon era*, ed. Cardwell PJ, Springer, Berlin, pp. 287-312.

Randazzo V 2009, 'EU security policies and the pillar structure: A legal analysis", *Perspectives on European Politics and Society*, vol. 10, no. 4, pp. 506-522.

Rawlinson K 2013 'NSA surveillance: Merkel's phone may have been monitored 'for over 10 years', *The Guardian*, 26 October. Available from <www.theguardian.com> [6 November 2014].

Reding R 2013, 'Towards a more dynamic transatlantic area of growth and investment', SPEECH/13/867, 29 October.

Rees W 2011, '*The US-EU Security Relationship: The Tensions between a European and a Global Agenda'*, Palgrave Macmillan, Basingstoke.

Ribeiro J 2014, 'UN committee calls on countries to protect right to privacy', *Pcworld*, 25 November. Available from <http://www.pcworld.com>[26 November 2014].

Richards RJ 2014, 'NSA's civil liberties and privacy protections for targeted SIGINT activities under Executive Order 12333', *NSA Director of Civil Liberties and Privacy Office report*, 7 October.

Rifkind M 2014, '*Intelligence agencies in the Internet age - Public servants or public threat?*', Wadham College, Oxford.

Ripoll Servent A & MacKenzie A 2012, 'The European Parliament as a 'Norm Taker'? EU-US Relations after the SWIFT Agreement', *European Foreign Affairs Review*, vol. 17, Special Issue, pp. 71–86.

Ripoll Servent A & MacKenzie A 2011, 'Is the EP still a data protection champion? The case of SWIFT', *Perspectives on European Politics and Society*, vol. 12, no.4, pp. 390-406.

Rosenzweig R 2014, 'American privacy values vs. European perceptions', *The Business of General Technologies*, 8 August. Available from <http://fcw.com/> [23 November 2014].

Rozée S, Kaunert C & Léonard S 2013, 'Is Europol a Comprehensive Policing Actor?', *Perspectives on European Politics and Society*, vol. 14 no. 3, pp. 372-387.

la Rue, F 2013, 'Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', *General Assembly of the United Nations*, A/HRC/23/40.

Ruiz Miguel C 2007, 'Problemas actuales del derecho de los servicios de inteligencia', *Inteligencia y Seguridad: Revista de Análisis y Prospectiva,* no. 2, pp. 13-46.

Ruthig J 2008, 'Rechtliche Rahmenbedingungen der Tätigkeit von Europol – Bestandaufnahme Ausblick', *Alternativenentwurf Europol und europäischer Datenschutz*, eds. Wolter J, Schenke WR, Hilger H, Ruthig J & Zoller MA, C.F.Müller Wissenschaft, pp. 97-124.

Salmi I 2014, 'Multilateral intelligence cooperation in the EU', *Gnosis Rivista italiana di Intelligence*, no. 2. Available from <http://gnosis.aisi.gov.it/Gnosis/Rivista39.nsf/ServNavig/24> [28 October 2014].

Sarkesian SC, Allen Williams J & Cimbala SJ 2008, 'National Security. Policymakers, processes and politics', *Lynne Rienner Publishers*, Boulder, CO.

Sayare S 2013, 'France Broadens Its Surveillance Power', *The New York Times,* 14 December. Available from <www.nytimes.com> [6 November 2014].

Sayers D 2011, 'The European Investigation Order Travelling without a 'roadmap'', *CEPS Paper in Liberty and Security in Europe*, pp. 1-25.

Scheinin, M 2009, 'Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', *General Assembly of the United Nations*, A/HRC/10/3, NYC.

Scheinin, M 2013, 'LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens Hearing', European Parliament, 14 October.

Scheinin M 2014, 'To the Extent the ICCPR has Extraterritorial Effect, the Right to Privacy Is Not an Exception', written statement for *Privacy and Civil Liberties Oversight Board*'s hearing on 19.03.2014 Washington, D.C.

Scherrer A, Jeandesboz J & Guittet EM 2011, 'Developing an EU internal security strategy, fighting terrorism and organised crime'. *European Parliament, Directorate*

*General for Internal Policies. Policy Department C: Citizens' rights and Constitutional Affairs. Civil Liberties, Justice and Home Affaires*, Brussels.

Schroeder UC 2009, 'Strategy by Stealth? The Development of EU Internal and External Security Strategies', *Perspectives on European Politics and Society*, vol. 10 no. 4, pp. 486-505.

Schwartz PM 2012, 'Systematic government access to private-sector data in Germany', *International Data Privacy Law*, vol. 2, no. 4, pp. 289-301.

Schwartz PM 2014, 'Differing privacy regimes: A mini-poll on mutual EU-US distrust', *IAPP*, 22 July. Available from <https://privacyassociation.org> [23 November 2014].

Shenon P 2003, 'Two years later: The borders; new passport rules to fight terrorism are put off for a wear', *New York Times*, 9 September. Available from <www.nytimes.com> [22 November 2014].

Smith J.C. 2003, 'The USA Patriot Act: Violating reasonable expectations of privacy protected by the fourth amendment without advancing national security' , *82 North Carolina Law Review*, pp. 412-455.

Soleto Muñoz H & Fiodorova A 2014, 'DNA and law enforcement in the European Union: Tools and human rights protection', *Utrecht Law Review*, vol. 10, no. 1, pp. 149-162.

Stessens G 2008, 'The EU-US Agreements on extradition and on mutual legal assistance', *Justice, Liberty, Security: New Challenges for EU External Relations,* eds. Martenczuk B & van Thiel S, VUBPress, Brussels, pp. 341-366.

Suda Y 2013, 'Transatlantic politics of data transfer: Extraterritoriality, counter-extraterritoriality and counter-terrorism', *Journal of Common Market Studies*, vol. 51 no. 4, pp. 772–788.

Sullivan B 2006, ''La difference' is stark in the EU, US privacy laws', *NBC News*, 1 October. Available from <www.nbcnews.com> [23 November 2014].

Svenden ADM 2011, 'On a "continuum with expansion"? Intelligence cooperation in Europe in the early 21st Century', *Journal of Contemporary European Research*, vol. 7, no. 4, pp. 520-538.

Taplin W L 1989, 'Six general principles of intelligence', *International Journal of Intelligence and Counterintelligence*, vol. 3, no. 4, pp. 475-491.

Tene O 2014, 'The U.S.-EU privacy debate: Conventional wisdom is wrong', *Privacy Perspectives*, 4 March. Available from <https://privacyassociation.org> [23 November 2014].

Töpfer E 2011, 'Europe's emerging web of DNA databases", *Statewatch Journal*, vol. 21 no. 1. Available from <http://database.statewatch.org/article.asp?aid=30566> [23 October 2014].

Trauner F & Carrapiço H 2012, 'The External Dimension of EU Justice and Home Affairs after the Lisbon Treaty: Analysing the Dynamics of Expansion and Diversification', *European Foreign Affairs Review*, vol. 17, no. 2/1, pp. 1-18.

Travis, A 2011, 'US to store passenger data for 15 years', *The Guardian*, 25 May. Available from <www.theguardian.com> [21 November 2014].

Tzanou M 2011, 'Data protection in EU Law: An analysis of the EU legal framework and the ECJ jurisprudence' in *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices,* eds. Akrivopoulou C & Psygkas A, IGI Global, Hershey, pp. 273-297.

Tzanou M 2012, *The added value of data protection as a fundamental right in the EU legal order in the context of law enforcement*, Ph.D thesis, European University Institute, Florence.

Vaas L 2013 'Infosec pros give verdict on EU's new cybersecurity strategy: Nice try', *Naked Security*, 8 February. Available from <http://nakedsecurity.sophos.com/2013/02/08/eu-cybersecurity-strategy/> [2 November 2014].

Van den Hoven van Genderen R 2008, 'Cybercrime investigation and the protection of personal data and privacy', *Council of Europe, Directorate General of Human Rights and Legal Affairs*, 25 May.

Van Elsuwege P 2014, 'The interface between the Area of Freedom, Security and Justice and the Common Foreign and Security Policy in the European Union: Legal constraints to political objectives' in *Freedom, Security and Justice in the European Union. Internal and External Dimensions of Increased Cooperation after the Lisbon Treaty*, eds. Holzhacker RL & Luif P, Springer, Berlin, pp. 119-135.

Vermeulen M & Wills A 2011, 'Parliamentary oversight of security and intelligence agencies in the European Union', *European Parliament, Directorate General for Internal Policies, Policy Department C, Citizens' rights and Constitutional Affairs*, Brussels.

Vernimmen-Van Tiggelen G & Surano L 2008, 'Analysis of the future of mutual recognition in criminal matters in the European Union', *Institute for European Studies*, *Université Libre de Bruxelle, ECLAN Report*. Available from <http://ec.europa.eu/justice/criminal/files/mutual_recognition_en.pdf> [23 October 2014].

Warner M 2002, 'Wanted: A Definition of "Intelligence". Understanding our craft', *Studies in Intelligence*, vol. 46, no. 3. Available from <https://www.cia.gov> [5 November 2014].

Watson SR 2011, 'Google sets sail: Ocean-based server farms and international law', *Connecticut Law Revie*w, vol. 43 no. 3, pp. 709-751.

Webb DC 2008, *ECHELON and the NSA*, IGI Global, Hershey, PA.

Wesseling M 2014,'Evaluation of EU measures to combat terrorist financing', *European Parliament, Directorate General for Internal Policies, Policy Department C, Citizens' rights and Constitutional Affairs*, Brussels.

Wesser RA 2010, 'Cross-pillar Mixity: Combining Competences in the Conclusion of EU International Agreements' *in Mixed Agreements Revisited. The EU and its Member States in the World,* eds. Hillion C & Koutrakos P Hart Publishing, pp. 30-55.

Wesser RA, Marin L & Matera C 2011, 'The external dimension of the EU's Area of Freedom, Security and Justice' in *Crime within the Area of Freedom, Security and Justice. A European Public Order*, eds. Eckes C & Konstadinides T, Cambridge University Press, Cambridge, pp. 272-300.

Wiese Svanberg C 2014, 'The questionable legality and practicality of the EU's proposed anti-FISA clause', *Privacy Perspective*, 16 January. Available from <https://privacyassociation.org> [6 November 2014].

Whitehead T & Porter A 2010, 'Britons to be spied on by foreign police', *Telegraph*, 26.07.2010. Available from <http://www.telegraph.co.uk/news/uknews/law-and-order/7909314/Britons-to-be-spied-on-by-foreign-police.html>[24 October 2014].

Wolff S, Wichmann N & Mounier G 2009, 'The external dimension of justice and home affairs: A different security agenda for the EU?', *European Integration* vol. 31, no. 1, pp. 9-23.

Wolf S 2009, 'The Mediterranean Dimension of EU Counter-terrorism', *European Integration*, vol. 31, no. 1, pp. 137–156.

Wolf C & Maxwell W 2012, 'So close, yet so far apart: The EU and U.S. visions of a new privacy framework', *Antitrust,* vol. 26, no. 3, pp. 8-13.

Wolf C 2013, 'Is personal data better protected from government surveillance in Europe than the U.S.? Maybe not, *IAPP*, 20 June. Available from <https://www.privacyassociation.org > [5 November 2014].

Wright D & de Hert P 2012, 'Privacy Impact Assessment', *Springer*, Berlin.

Wright S 2005, 'The ECHELON trail: An illegal vision', *Surveillance & Society,* vol. 3 no. 2/3, pp. 198-215.

# ANNEX 1

[redacted]

September 11, 2014

Dear Mr. [redacted],

Your FOIA request has been closed as insufficient for **one or more of the following reasons**:

- Your FOIA request is a third party request and did not include authorization that information on this individual can be released to you. All third party FOIA requests must include a signed G-28 or G-639 form, or a signed statement from the individual verifying that his/her information may be released to you.

- **Did not include a date of birth.**

- Did not include a full name (and aliases as appropriate) of the individual in which you are seeking records

- Did not include a death certificate (or other proof that the subject is deceased)

- Did not include a clear and detailed description of the records being requested.

Please resubmit your FOIA request, along with the required information, by logging into your existing FOIAonline account or go to https://foiaonline.regulations.gov to create an account.

Thank you,

FOIA Division

Sincerely,

Trible D. Greaves
U.S. Customs and Border Protection

# ANNEX II

| | |
|---|---|
| IAT_Traveller_ID | [redacted] |
| Birth_Date | [redacted] |
| Sex_Code | M |
| Family_Name | [redacted] |
| Given_Names | [redacted] |
| Travel_Doc_ID | [redacted] |
| Travel_Doc_Dept_Country_Code | ESP |
| Route_ID | EK413 |
| Local_Port_Code | SYD |
| Local_Scheduled_Date | 13/03/2013 |
| Direction_Code | O |
| Actual_Movement_Message_ID | A0380206357 |
| Movement_Date | 13/03/2013 |
| Movement_Status_Code | A |
| Movement_Time | 41:42.0 |
| Visa_Identifying_NBR | 5781075473 |
| Visa_Sub_Class_Code | 570 |
| Passenger_Crew_Code | P |
| Travel_Doc_Type_Code | FP |
| Travel_Type_Code | AI |
| Local_Scheduled_Date | 13/03/2013 |
| Movement_Race_ID | D30 |
| Movement_Status_Code | A |
| Passenger_Crew_Code | P |
| Related_Visa_ID | [redacted] |
| User_ID | [redacted] |

# ANNEX III



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

March 4, 2015



Agencia de Protección de Datos
C/Jorge Juan, 6
28001 Madrid

Dear Sir or Madam,

This letter is in response to your constituent's request for access to records (EU DPA Case Number ES-0001-TFTP; U.S. Treasury Department Case Number 2014-06-013), which you transmitted on behalf of your constituent and which the U.S. Treasury Department Office of Privacy, Transparency & Records received via electronic mail on May 12, 2014, pursuant to Article 15 of the *Agreement between the United States and the European Union on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program* ("Agreement"), and related authorities. Your constituent seeks records that may exist as part of the Terrorist Finance Tracking Program.

After conducting a thorough review of this request and receiving all necessary verifications, I confirm that your constituent's data protection rights have been duly respected in compliance with the Agreement. In particular, I verify and confirm that no processing of your constituent's personal data has taken place in breach of the Agreement.

The Department has reviewed the request for access to records and has determined that we are unable to confirm or deny the existence of any responsive records. Disclosure of such information could identify subjects of ongoing counterterrorism investigations and thereby impair the prevention, detection, investigation, or prosecution of criminal offenses, and could harm public or national security. This information would also be exempt from disclosure under the Freedom of Information Act. *See*, 5 U.S.C. § 552(b)(1) and/or (b)(7)(E) and Article 15(2) of the Agreement.

You may transmit an appeal of this decision on behalf of your constituent within 35 days from the date of this letter, using the same process and forms as the Article 15 access request. The appeal should specify the date of the initial request, the date of this letter, and contain the reasons your constituent believes the decision is in error. Please refer to the Case Numbers (EU DPA Case Number ES-0001-TFTP; U.S. Treasury Department Case Number 2014-06-013) in the appeal request and add the words "DPA Appeal" to the front of the envelope. Please address the envelope to:

DPA Appeal
Deputy Assistant Secretary for Privacy, Transparency, and Records Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220