Universidad Carlos III de Madrid
www.uc3m.es

TESIS DOCTORAL

INFORMATION EXCHANGE EFFICIENCY IN CRIMINAL INVESTIGATION IN EUROPEAN UNION

Autor:

Anna Fiodorova

Director/es:

Helena Soleto Muñoz

Tutor:

Helena Soleto Muñoz

DEPARTAMENTO DE DERECHO PENAL, PROCESAL

E HISTORIA DEL DERECHO

Getafe, noviembre 2015

Universidad Carlos III de Madrid
www.uc3m.es

TESIS DOCTORAL

Information Exchange Efficiency in Criminal Investigation in European Union

Autor: *Anna Fiodorova*

Director: **Helena Soleto Muñoz**

Firma del Tribunal Calificador:

Firma

Presidente:

Vocal:

Secretario:

Calificación:

Getafe, de de

INDEX OF CONTENT

INDEX OF TABLES

ABBREVIATIONS

AML/CFT – Anti-Money laundering/Counter Financing of Terrorism

ARO – Assets Recovery Office

AWF – Analytical Work File

CARIN – The Camden Assets Recovery Inter-Agency Network

CEPOL – European Police College

C-SIS – Central Schengen Information System

CISA – Convention implementing the Schengen Agreement of 14 June 1985 between the Government 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

EC – European Communities

EC3 – European Cybercrime Centre

ECHR – European Convention for the Protection of Human Rights and Fundamental Freedoms

ECtHR – European Court of Human Rights

EDPS – European Data Protection Supervisor

EEC – European Economic Community

EIS – Europol Information System

ENISA – European Network and Information Security Agency

EU – European Union

FIU – Financial Intelligence Unit

FRA – European Union Agency for Fundamental Rights

INTERPOL – International Criminal Police Organization

IOCTA – Internet Organised Crime Threat Assessment[1]

LIBE – Civil Liberties and Justice and Home Affairs Committee of the European Parliament

OCTA – Organised Crime Threat Assessment

SIRENE – Supplementary Information Request at the National Entry

SIS – Schengen Information System

SIS II – Second generation of the Schengen Information System

SOCTA – Serious and Organised Crime Threat Assessment

TEEEC – Treaty Establishing the European Economic Community

TE-SAT - Terrorism Situation and Trend Report

TEU – Consolidated version of the Treaty on European Union[2]

TFEU – Consolidated version of the Treaty on the Functioning of the European Union[3]

[1] At EU level, since 2004, Europol has produced comprehensive threat reports that include analysis of the current situation, both inside and outside the EU, and deduction of future threats to the EU's internal security.

[2] OJ C 83, 30.3.2010, p. 13-46.

[3] OJ C 83, 30.3.2010, p. 47-199.

INTRODUCTION

"It is a capital mistake to theorize before one has data.
Insensibly one begins to twist facts to suit theories,
Instead of theories to suit facts."
Arthur Conan Doyle, Sherlock Holmes

Information is a primary and indispensable background to any conclusions, whether of scientific research, business plans, political decisions or the performance of justice.

Except on those occasions when the offender is caught in the act, the starting point of any police investigation is obtaining information about the crime, and on this basis making, deductions, as glorified by Sherlock Holmes. It is also one of the main elements in crime prevention, given that its timely possession precludes damaging consequences and contributes to the security and protection of human rights and the legitimate interests of individuals and society.

Information is obtained from different sources, beginning with inquiries to victim and witnesses, and finishing with the inspection of crime scene, reviewing surveillance camera records and consulting data bases. It is very seldom that one piece of information is just one link in a chain, which guides competent authorities to the next links; and there is no certainty whether this chain will end in the same country where the investigation is taking place or not.

Cross-border information exchange became more relevant a few decades ago, when organised crime, moving "in the rhythm of time"[4], identified globalisation and the facilitated movement of persons as an opportunity for new criminal markets. It was especially perceived in the EU and the Schengen zone with the establishment of the free movement of persons, goods, capital and services, the

[4] STORBECK, Jürgen, "La cooperación policial europea", in MONTERO, Julián, ROMERO, Francisco and VALIENTE, Elena, *¿Hacia una Policía Europea?* (Madrid: Fundación Policía Española, 2002), p. 155.

abolition of internal borders and the introduction of a single currency in the majority of the Member States.

Notwithstanding, these negative side effects have not been led automatically by their antidote – the free movement of investigation and prosecution. Actions of law enforcement, prosecution and judicial authorities remained limited to state territory; this meant a high probability of impunity in the case of transnational crimes.

In these circumstances, when EU policies had endangered security by unintentionally giving wider possibilities to criminals than to prosecuting authorities, a need to introduce effective co-operation tools that would overcome the obstacle of the existence of border in investigation and prosecuting criminal deeds (including measures for information exchange) emerged.

As a result of this, as well as of some other particular incidents (such as terrorist attacks), the EU has developed a wide range of mechanisms for information exchange that include data bases, networks of experts or contact points, agencies and a purely legal basis for the information exchange process.

As shown by a study, carried out in 2009, by the International Centre for Migration Policy Development, countries exchanged approximately 13 million messages[5] (requests and transmissions of information) through INTERPOL and within five years, in 2014, this number increased to 17 million.[6] INTERPOL's data bases (such as those on suspected or wanted persons, on dactyloscopics, on DNA profiles, and stolen and lost travel documents) were consulted 1.7 billion times in 2014.[7]

Within the EU, in 2009, one quarter of all investigation information requests were sent to other Member States.[8] Comparing only information submitted to EIS in 2009 and 2014, a number of records were doubled.[9]

---

5 See INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT AND EUROPEAN PUBLIC LAW ORGANIZATION, "Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments", European Commission, 2010, p. 45, accessed February 20, 2013, http://ec.europa.eu/dgs/home-affairs/doc_centre/police/docs/icmpd_study_lea_infoex.pdf.

6 See INTERPOL, "Annual Report 2014", p. 13, accessed May 17, 2015, http://www.interpol.int/News-and-media/Publications.

7 Ibid, p. 14.

8 See INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT AND EUROPEAN PUBLIC LAW ORGANIZATION, "Study on the status of information…", loc. cit., p. 46.

9 Council document 8082/15, p. 42, 43.
As revealed by the International Centre for Migration Policy Development, the most frequent exchange data categories are:
"Data about persons; perpetrators, suspects, unidentified persons (name, date of birth, jobs, identification data of fingerprinted criminals for true identification, confirmation of identity,

Thus it became a very dynamic field of EU policy and new initiatives, but sometimes it lacked consistency and clear indications of use, and police officers faced plurality of legal basis, channels and procedures and different tools for different categories of information. In addition, the European legislator has established a variety of regulations on the storage of information, its transmission to third states and onward transmission, as well as on data subject rights towards the processing of their personal data.

For example, data such as fingerprints can be introduced and found in SIS, Europol's EIS, Europol's AWFs, national dactyloscopic data bases which are accessible on the basis of Prüm Decisions; but subjects' data and the purposes for which it is stored, can be different or overlapping. Information on suspicious financial transactions or bank accounts can be requested trough Europol, network of FIUs, bilaterally between competent authorities on the basis of Swedish Initiative, also found in AWFs.

It brings law enforcement officers to confusion, initially at the moment of requesting or submitting information: which mechanism should be used, how should it should be used, whether it will result only in cross-checks or direct access to information, how long can it take to get information, is it possible to request or submit information directly or shall it be done through the designated authority? Secondly, during the processing of such data and last but not least – at the moment of considering whether it is consistent with the due process.

Facing such babel, the aim of the thesis is to analyse: Which information exchange tools under which circumstances can be used? Do they overlap? How are they compatible with human rights?

Tools used in work as responsible as investigation, should result in a perfectly assembled puzzle, in which each piece corresponds to its due process.

---

residence, DNA, fingerprints, verification of personal data, criminal convictions, passports, IDs, photographs);
Data about vehicles; vehicles used to transport suspects, perpetrators; vehicles located at the crime scene or recorded by surveillance cameras, registration details, owner and operator of a vehicle, chassis numbers, purchase documents, export and import documents;
Financial data; company information, banking information, property relationship, bank accounts, transaction details, account holders, company board of directors, share capital, income and wealth information, unusual or suspicious money transactions, asset tracing data payment cards, data for POS terminal device;
Communication data; subscribers' details (particularly for mobiles), IT addresses, billing details, outgoing/incoming calls, emails, wiretapping, interceptions;
Data about objects, confiscated objects, objects related to committed crimes are often exchanged while data about firearms (licensing data, lost weapon, weapon used for crimes) and other "explanatory" data are seldom exchanged (e.g. interrogations, home searches, seizure of evidence, trends, statistics, customs documents, modus operandi, and fines)."
Source: INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT AND EUROPEAN PUBLIC LAW ORGANIZATION, "Study on the status of information…", loc. cit., p. 49.

Having said that, it is no less important to highlight the limits of this research; it addresses information exchange between law enforcement authorities while performing one of the core functions –the investigation of a crime. For the purpose of this work, information exchange in crime investigation will mean its processing in pre-trial investigation, operational activities, as well as within the stage of traditionally understood investigation, as a stage of the penal process when pieces of exchanged or transmitted data do not involve the authorisation of a judge or a prosecutor. It should also be pointed out that what is treated, as a general, rule as "police data" in some Member States can in fact belong to "judicial data"; for example, DNA data bases in Denmark.

In any case, information exchange between judicial authorities through Eurojust on the basis of rogatory letters, mutual recognition of evidence or other tools of judicial co-operation remains out of the scope of the thesis.

Summarising, it can be defined as analysis of the mechanisms to exchange "raw material" for police investigation, which at the latter stage, and when it is necessary and following relevant procedure, can be considered as evidence.

From geographical perspectives, it limits only to the EU tools and those applied to Schengen area, not entering in comparisons with international information exchange tools, first of all provided by INTERPOL.

The work is divided into three parts:

- The origins of transnational information exchange. Information use for law enforcement and fundamental rights;
- Pool of tools: development, application and problems associated with some information exchange instruments;
- Projects in the pipeline: reasons, content, problems, state of play.

The first part analyses circumstances that led to the necessity of law enforcement authorities to look for information beyond state borders, and how European politics evolved in this respect. It also scrutinises the impact of information exchange on fundamental rights and marks the difference between their limitation and violation. Special attention is drawn to the right to data protection and its regulation, as it is inalienable element of any piece of data and largely exposed to violation.

The second part is devoted to the analysis of different information exchange tools between law enforcement authorities. A selection of tools has been made, applying three criteria: to analyse each type of information exchange mechanisms, and

when there is more than one of each type, to analyse the most important or the most controversial one.

On this basis, SIS and SIS II have been chosen as the centralised data base, Europol as agency, Swedish Initiative as general the legal basis for any information exchange, FIUs and AROs as networks and Prüm Decisions as a decentralised data base with direct access.

A slight deviation from these criteria makes necessity to analyse the entire part of the CISA which corresponds to information exchange, i.e. Liaison officers, police and customs co-operation centres and general the regulation of cross-border assistance foreseen in Articles 39 and 46. This was carried out taking into account that not only SIS and SIS II, but all the mechanisms envisaged in CISA are compensatory measures for the abolition of internal borders within the Schengen area, and represented the first appearance of real police co-operation tools. Besides, study of the Swedish Initiative would not be comprehensive without its comparison with the regulation, foreseen on Articles 39 and 46 of the CISA.

The order of analysis is not random either, and it reflects the chronological evolution of the EU information exchange regulation. A partial discrepancy from this chain are FIUs and AROs networks, as FIUs were established before the adoption of the Swedish Initiative, but for the sake of the explanation of the functioning of ARO it was more convenient to discuss it later.

The third part presents new projects under development, but only those related to information exchange between law enforcement authorities, not entering into judicial co-operation and such initiatives as the establishment of the European Public Prosecutor's Office. The research is oriented to the identification of our level of need for them and coherence with the developed information management policy.

PART I:
THE ORIGINS OF TRANSNATIONAL INFORMATION EXCHANGE. INFORMATION USE FOR LAW ENFORCEMENT AND FUNDAMENTAL RIGHTS

CHAPTER 1:
POLICE AND INFORMATION EXCHANGE. EUROPEAN UNION INFORMATION EXCHANGE POLICY

Information is a raw material and an indispensable element of any investigation and with the developments of recent decades, its transmission and receipt "crossing" state borders has become vital in order to conclude successful legal action. Not to overlook unpunished crime whose detection and effective investigation would be impossible without cross-border information exchange.

Within such a framework, this chapter of research sets out to identify reasons for the outspread of "transnationality" of crime, to analyse the EU political developments in this respect, and specific steps carried out in this area.

1. Territorial limits of law enforcement institutions' competence and the need for co-operation

Guarantees of security (both internal and external) and justice are the core functions of any modern state[10] and so called state monopoly.[11] As in the case of any public institution within any state, the competence of law enforcement institutions is pre-established by national law and as a global rule "do not generally

[10] See ALMAGRO NOSETE, José; CÓRTEZ DOMÍNGUEZ, Valentín; GIMENO SENDRA, Vicente et al., *Derecho Procesal. Parte general proceso civil (1)* (Valencia: Tirant lo Blanch, 1989), p. 47; MONTERO AROCA, Juan, *Introducción al Derecho Procesal. Jurisdicción, acción y proceso* (Madrid: Tecnos, 1979), p. 18; MONTERO AROCA, Juan; GÓMEZ COLOMER, Juan Luís and BARONA VILAR, Silvia, *Derecho Jurisdiccional I. Parte General* (20th ed. Valencia: Tirant lo Blanch, 2012), p. 85; MITSILEGAS Valsamis; MONAR, Jörg and REES, Wyn, *The European Union and Internal Security: Guardian of the People?* (Hampshire: Palgrave Macmillan, 2003), p. 8.

[11] See DE LA OLIVA SANTOS Andrés and DÍEZ-PICAZO GIMÉNEZ, Ignacio, *Derecho Procesal. Introducción* (3rd ed. Madrid: Ramón Areces, 2004), p. 164-165.

transcend national borders."[12] It means that other persons or entities than the state constitute institutions (private parties or institutions of other states) are not allowed to implement law.[13]

There are not as many sources referring to territorial limits of law enforcement institutions' competence as those dedicated to the same topic in relation to judicial jurisdiction. In any case, the scope of competence of the law enforcement authorities in crime investigation is closely linked to the scope of jurisdiction as crime investigation does not have an end in itself, but is an indispensable step to perform jurisdiction.

The main elements that determine limits of jurisdiction and law enforcement competence are sovereignty and the principle of territoriality.

Penal law is an essential piece of classical understanding of sovereignty[14]. National sovereignty grants its jurisdiction exclusively to its Judicial Power and no other power (neither other branches of power, nor the judicial power of another state) can legitimately perform justice.[15] A judgment by a foreign tribunal admitted without any previous verification on the basis of the international agreement in force, would mean cession of sovereignty.[16] It also establishes what has to be treated as a criminal act on its territory and foresees sanctions. These limits are also reflected in crime investigation. That results in the principle of "no intervention" (or in other words non-application of national *ius puniendi*) in extra-territorial cases, as it would be an infringement of the sovereignty of another state.[17]

The principle of territoriality implies that judicial and law enforcement authorities are the only ones that are able to implement their judicial, administrative and coercive powers within the territory of the state to which they pertain, and, "Country borders normally provide a sufficient signal that one legal order is being left and another is being entered."[18] As judicial and law enforcement authorities

---

12 BANTEKAS Ilias and NASH Susan, *International Criminal Law* (2nd ed. Coogee: Cavendish Publishing Limited, 2003), p. 265.

13 See MONTERO AROCA, Juan, *Introducción al Derecho Procesal*…, op. cit., p. 35.

14 See ARNÁIZ SERRANO, Amaya, "Evolución de la Cooperación Judicial Penal Internacional: en especial, la Cooperación Judicial Penal en Europa" in CARMONA RUANO, Miguel; GONZÁLEZ VEGA, Ignacio U, and MORENO CATENA, Víctor, *Cooperación Judicial Penal en Europa* (Dykinson: Madrid, 2013), p. 10.

15 See GIMENO SENDRA, Vicente, *Manual de Derecho Procesal Penal* (Madrid: Colex, 2008), p. 9.

16 DE LA OLIVA SANTOS Andrés and DÍEZ-PICAZO GIMÉNEZ, Ignacio, *Derecho Procesal. Introducción,* op. cit., p. 165.

17 See AMBOS, Kai, *Temas de Derecho Penal internacional y europeo* (Madrid: Marcial Pons, 2006), p. 80.

18 DE HERT, Paul, "Division of Competencies between National and European Levels with regards to Justice and Home Affairs" in APAP, Joanna, *Justice and Home Affairs in the EU. Liberty and Security Issues after Enlargement* (Cheltenham: Edward Elgar, 2004), p. 57.

are submitted to their national law (with some exceptions foreseen in international conventions or agreements), their actions on the territory of another state would be lacking legality.[19]

Nevertheless, due to the facilitated movement of persons and goods in the last thirty years, as well as other factors that will be discussed in the following section, frequently investigative or preventive measures of one state require some investigative activities in another; or are related to an investigation held by competent authorities of another state as well. For instance, when a perpetrator has moved to another country or has contacts with its residents and they are suspected to be involved in the commission of or occultation of a crime or the laundering of criminal actives. The last well-known examples are the escape of Sergio Morate (a suspect in the murder of two girls) from Spain to Romania[20] and the dismantling of Chinese criminal network that was involved in smuggling illegal immigrants from China to Spain and then onwards to Canada, Switzerland, the United Kingdom and other countries.[21]

In both cases, internal security of Spain was affected, but bearing in mind the territorial limits of the competence, its law enforcement authorities had not been authorized to perform any investigative activities on the territory of other countries and therefore needed the assistance of Romania, China, Canada and other countries in order to apply Spanish *ius puniendi*. At the same time, the application of *ius puniendi* in Spain contributed to the security of those countries by allowing the prevention of the criminal activities of the above-mentioned persons on their territory.

In these examples, the countries involved could either have performed all the necessary actions themselves, or their national laws could have allowed Spanish competent authorities to act within their territory; this would have meant limiting their own sovereignty and permitting the expansion of Spanish sovereign powers on their territory. Any of the two options would first require contacts between competent authorities of the countries involved (providing information about committed crimes, movements of suspects, their detection on the territory of the other state) and then interaction in performing necessary procedural actions. All these elements together form a co-operation or engagement to assist.

---

[19] See GARCÍA BORREGO, José Antonio and FERNÁNDEZ VILLAZALA, Tomás, *Introducción al Derecho Procesal Penal* (Madrid: Dykinson, S.L., 2007), p. 21.

[20] See "La Justicia rumana aprueba la entrega definitiva a España de Sergio Morate", Europapress, September 3, 2015, accessed September 7, 2015, http://www.europapress.es/nacional/noticia-justicia-rumana-aprueba-extradicion-definitiva-espana-sergio-morate-20150902172359.html.

[21] See ORTEGA DOLZ, Patricia and CONGOSTRINA, Alfonso L., "Detenidas 80 personas de una red de tráfico ilegal de ciudadanos chinos", *El País*, May 4, 2015, accessed May 15, 2015, http://politica.elpais.com/politica/2015/05/04/actualidad/1430738360_410640.html.

The origins of co-operation can be found in the middle of the XIX century, with the aim of keeping travelling political agitators under surveillance. This intensified at the end of XIX century after the assassinations of the Russian Emperor Alexander II in 1881, the President of France, Sidi Carnot in 1894 and Austrian Empress Sissi in 1898.[22]

At the beginning of the XX century, the first attempts at legal regulation and institutionalisation took place. Thus in 1905, an International Police Convention between the authorities in Buenos Aires, La Plata, Montevideo, Rio de Janeiro, and Santiago de Chile was signed. In 1914 the first international police meeting in Monte Carlo took place, and an idea to establish a cooperation institution was raised. But due to the First World War it was not implemented until 1923, with the establishment of the International Criminal Police Commission that in 1956 was transformed into INTERPOL that nowadays counts with the membership of 190 states.

Currently, co-operation and its different mechanisms are widely used both at regional and global level and they cause the gradual softening of the principles of sovereignty and territoriality.[23]

2. Crimes and factors that gave rise for international police co-operation

As stated by Rebollo Delgado, regulation emerges from already existing conflict or social necessity.[24] Thus, the state's response to any new criminal phenomenon is also re-active, i.e. First it occurs and only then legal, organisational, technical and other necessary measures to combat it and to prevent its recurrence in society are taken. One of the latest examples in this respect is cybercrime that only originated with the introduction of the World Wide Web which besides leading to enormous facilitation of communications, became a tool of unfair trade, access to information or accounts belonging to other persons, radicalization and other criminal offences. [25] As stated in in the report published by the Computer Science and

[22] See MADSEN, Frank G., *Transnational Organised Crime* (New York: Routledge, 2009), p. 65.

[23] See LLORENTE SÁNCHEZ-ARJONA, Mercedes, *Las garantías procesales en el espacio europeo de justicia penal* (Valencia: Tirant lo Blanch, 2014), p. 76.

[24] See REBOLLO DELGADO, Lucrecio, *Vida privada y protección de datos en la Unión Europea* (Madrid: Dykinson S.L., 2008), p. 83.

[25] The first computer-related infringements of privacy appeared in the sixties, but were a matter of civil and public rather than criminal law. In the seventies computer manipulation, sabotage, espionage became known and in the eighties – illegal copies of soft-ware, music and movies. But the development of Internet computer networks in the nineties became really attractive for those offering illegal or harmful content, radicalisation, gambling, etc. See COUNCIL OF EUROPE, *Organised crime in Europe: the threat of cybercrime* (Strasbourg: Council of Europe Publishing, 2005), p. 84-85.

Telecommunications Board of the USA in 1991, "The modern thief can steal more with a computer than with a gun."[26]

The same philosophy can be applied to international co-operation, where first a need occurs and then corresponding measures are developed. Besides, such a need or a reason must be very significant and co-operation indispensable in order to convince independent countries to take common measures that could, to some extent, affect their sovereignty.

The most general clue about the reasons for co-operation tools is given by Albrecht who has stated that "First of all terrorism, then drugs and finally transnational or international crime gave an impulse to the demand to strengthen police co-operation."[27]

Before continuing the analysis, the terms "transnational" and "international crime" deserve a special mention. In this thesis the theory that transnational and international crime are different terms with different content will be followed.

Thus international crime will be understood as crime foreseen in the Rome Statute of the International Criminal Court,[28] i.e. Genocide, crime against humanity, war crime and crime of aggression.[29] The international community considers these crimes to be violations the highest values of mankind and expresses global interest to repress them. Some authors (Cassese, Vacas Fernández, Johnson, Sandoz, Bianchi, Naqui[30]) believe that some forms of terrorism and torture also have to be treated as international crime as they are included as subcategories of four international crimes covered by the Rome Statute.[31]

---

[26] COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, "Computers at Risk: Safe Computing in the Information Age", The National Academies Press, 1991, accessed January 21, 2015, http://www.nap.edu/openbook.php?record_id=1581.

[27] ALBRECHT, Hans-Jörg (translation GUERRERO PERALTA, Oscar Julián). *Criminalidad transnacional, comercio y lavado de dinero* (Bogota: Universidad externado de Colombia, 2001), p. 40.

[28] INTERNATIONAL CRIMINAL COURT, http://www.icc-cpi.int/NR/rdonlyres/ADD16852-AEE9-4757-ABE7-9CDC7CF02886/283503/RomeStatutEng1.pdf.

[29] See Article 5 of the Rome Statute of the International Criminal Court.

[30] See CASSESE, Antionio, *International Criminal Law* (2nd ed. New York: Oxford University Press, 2008), p. 11-13; BANTEKAS, Ilias and NASH, Susan, *International Criminal Law*, op. cit., p. 1-21; VACAS FERNÁNDEZ, Félix, *El terrorismo como crimen internacional. Definición, naturaleza y consecuencias jurídicas internacionales para las personas* (Valencia: Tirant lo blanch, 2011), p. 254–255; SANDOZ, Yves, "Lutte contre le terrorisme et droit international: risques et opportunités" in *Revue suisse de droit internationale et de droit européen*, 2002, No. 2, p. 347; PAULUSSEN, Christophe, "Impunity for international terrorists? Key legal questions and practical considerations" (research paper, International Centre for Counter-Terrorism, 2012), p. 7, accessed 21 January, 2015, http://www.icct.nl/download/file/ICCT-Paulussen-Impunity-April-2012.pdf.

[31] For instance torture as an element of crime against humanity (Article 7(1)f) as well as of crime of war (Article 8(2)a(ii). Terrorism is not directly mentioned in the Rome Statute, but Vacas

Besides negotiating the draft of the Rome Statute, the proposal to endow the International Criminal Court with jurisdiction on terrorism had been considered; but finally, due to strong opposition from some countries, Belgium, Brazil , France, the Netherlands, Norway, Spain, Sweden, the United States of America, for example, it was left aside.[32]

Some international treaties establish other crimes (explicitly providing with their elements) that have to be criminalised in the national law of participating states. One of the best known examples is organised crime established by the United Nations Convention against Transnational Organized Crime.[33] Some authors (like Bassiouni, Bantekas and Nash) ascribe them to international crimes, equally as those established by the Rome Statute[34]. Nevertheless, in this research they will be understood in line with Madson's explanation that those crimes that cross the border of one country are transnational (or cross-border) and require measures of global governance, but it does not convert them into international crimes in the sense of the Rome Statute.[35]

This research will focus on transnational or cross-border crime that affects more than one state by its preparation, direction or commission, by involvement of international organised crime[36] as well as by nationality of active and passive subjects or proliferation of the effects of crime.[37]

2.1. Reasons for the rise in co-operation within the European Communities

Although the original policies of the European Communities had not included security and justice topics and were purely oriented to post-war economic growth and the development of Europe, some global and regional factors as well as socially important events impelled its Members to start co-operation in these matters, and to adjust it to socially determined necessities. Over 40 years, an evolution took place from an informal agreement through an intergovernmental one and finally

Fernández understands that it could have consequences foreseen in its Article 7, for instance such as assassination, grave deprivation of liberty or other inhuman acts. See VACAS FERNÁNDEZ, Félix, *El terrorismo como crimen internacional..,* op. cit., p. 223.

32 Ibid, p. 60.

33 United Nations, http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.

34 BASSIOUNI, Cherif, *Introduction to International Criminal Law* (Ardsley, New York: Transnational Publisher, Inc., 2003), p. 114-118.

35 MADSEN Frank G., *Transnational Organised Crime*, op. cit., p. 95.

36 Article 3(2) of the United Nations Convention against Transnational Organised Crime provides with the comprehensive definition of transnational crime.

37 See PÉREZ MARÍN, María Ángeles, *La lucha contra la criminalidad en la Unión Europea* (Barcelona: Atelier, 2013), p. 204.

with the Treaty of Lisbon became supranational (for information in relation to the development of the European legal basis for co-operation, see the following subsection).

Circumstances that urged Member States of the European Community towards closer co-operation can be conditionally divided into three groups that are presented below.

2.1.1. Socially relevant milestones

The first informal and intergovernmental forum for co-operation on security between some Member States of the European Communities was created in 1975; this was as a consequences of the terrorist attack during the Olympic Games in Munich on 4th September 1972, and other threats of terrorism that had occurred in Europe: partly coming from the Middle East and partly activities of national-based terrorist groups. Even if the latest case seems to be a purely national problem, a tendency to co-operation among terrorist groups from different Western countries (France, Germany, Italy, Spain, the Netherlands, the United Kingdom) in sharing intelligence, preparing attacks, procurement of arms and even training had been observed.[38]

At the European Council of Rome on 1st–2nd December 1975, at the proposal of the United Kingdom, it was agreed that "Community ministers for the Interior (or Ministers with similar responsibilities) should meet to discuss matters coming within their competence, in particular with regard to law and order."[39]

This informal co-operation forum was named TREVI Group which is an acronym (in French) for terrorism, radicalism, extremism and international violence.[40]

In parallel, the President of France, Giscard d'Estaing, proposed the creation of an area of judicial co-operation in criminal matters, based on simplified extradition procedure, transmission of penal procedures, recognition of judicial decisions and common rules for transmission of detainees between the Member States. Since 1984 Ministers of Justice and Home Affairs have met twice a year to deal with

[38] See MITSILEGAS, Valsamis; MONAR, Jörg and REES, Wyn, *The European Union and Internal Security...*, op. cit., p. 22.

[39] Summary of the Conclusions of the Meeting of the European Council held in Rome on 1 and 2 of December, 1975, accessed September 20, 2013, http://aei.pitt.edu/1407/.

[40] In some sources TREVI firstly is associated with the famous Trevi fountain of Rome (where the Council took place). See MITSILEGAS, Valsamis; MONAR, Jörg and REES, Wyn, *The European Union and Internal Security...*, op. cit., p. 23.

matters of police, judicial and customs co-operation and free movement of persons.[41]

At the same time, Europe faced a problem of increased consumption of heroin, LSD and cocaine as a result of drug trafficking. This situation *per se* carried a cross-border element and needed a coordinated international response both within and outside the European Community.[42]

More than two decades later, other terrorist attacks (11th September 2001 in the United States, intensified after the attacks of 11th March 2004 in Madrid and 7th July 2005 in London) had created social and security shocks to both society and security organisations, and impelled a more active EU approach to the speeding up of judicial and police co-operation and information exchange.

2.1.2. Global factors facilitating criminal activities

Rapid development of financial markets became a great opportunity for many enterprises and entrepreneurs. But fast movement of big amounts of money around the world also meant great opportunities for rapid and well-masked money laundering with an estimation of one billion every day.[43]

Financial Action Task Force, founded in 1989 by G-7 estimated that in the late nineties, in the USA and Europe alone, laundered money accounted for around 2% of global GDP (US$ 0.34 trillion).

Almost ten years later, the International Monetary Fund calculated that money laundering accounted for between 2 and 5% of global GDP and had resulted in the following money equivalents: in 1996 between US$ 0.6 and 1.5 trillion; in 2005, between US$ 0.9 and 2.3 trillion and in 2009, between US$ 1.2 and 2.9 trillion.[44]

On the other hand, new technologies of transportation and political commitment to free or facilitated trade enabled organised crime to carry out its usual activity of

---

41 See G. VIADA, Natacha. *Derecho penal y globalización. Cooperación penal internacional* (Madrid: Marcial Pons, 2009), p. 118-119; MORENO CATENA, Víctor and CASTILLEJO MANZANARES, Raquel, *La persecución de los delitos en el Convenio de Schengen* (Valencia: Tirant lo Blanch, 1999), p. 13.

42 On international level co-operation in combatting drug trafficking began with the establishment of International Opium Commission in 1909. See more. MADSEN Frank G., *Transnational Organised Crime,* op. cit., p. 27-28.

43 VLASSIS, Dimitri, "The Global situation of transnational organized crime, the decision of the international community to develop an international convention and the negotiation process", in *Resource Material Series*, 2002, no. 59, p. 476.

44 See UNITED NATIONS OFFICE ON DRUGS AND CRIME, "Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes: Research Report (Vienna, October 2011)", p. 18-19, accessed September 20, 2013, www.unodc.org/documents/data-and-analysis/Studies/Illicit_ financial_flows_2011_web.pdf.

smuggling much more effectively and in more sophisticated ways; as Felsen and Kalaitzidis stated, "it heightened cross-border linkages and made national frontiers seem more permeable than ever."[45]

Taking advantage of this situation at the beginning of the 1990s organised crime changed significantly and became much more transnational in nature. As pointed out by Reinares and Resa, "This type of organised crime has three basic differences with respect to previous manifestations of the phenomenon: it tends to operate at a regional or global level, mobilizing extensive cross-border connections and, above all, has the ability to challenge both national and international authorities."[46]

Geopolitical changes caused by the end of the Cold War and the start of the Balkan War also had a significant influence on the augmentation of organised crime. These circumstances gave raise to new criminal organisations involved in illegal migration, the trafficking of human beings, illegal sale of arms as well as integration of criminal elements into politics and economies.[47]

Free movement not only has its physical dimension, but its virtual dimensions as well. As already mentioned, the last decades were marked with the development and increase in the use of cyber space for criminal purposes. In addition to commissioning such crimes as malware, phishing, data breach and network attacks, child sexual exploitation online, payment fraud, attacks on critical infrastructure, the Internet is used "as a communication tool, information source, marketplace, recruiting ground and financial service."[48] It facilitates authors of crimes to remain more anonymous, to conceal criminal deeds, to eliminate traces or evidences and to reduce investigative capacities of competent authorities.[49]

---

45 FELSEN, David and KALAITZIDIS, Akis, "A Historical Overview of Transnational Crime" in REICHEL, Philip, *Handbook of transnational crime and justice* (California: Sage Publications, Inc., 2005), p. 12.

46 REINARES, Fernando and RESA, Carlos, "Transnational organized crime as an increasing threat to the national security of democratic regimes: assessing political impacts and evaluating state responses", North Atlantic Treaty Organisation, 1997, p. 6, accessed February 1, 2015, http://www.nato.int/acad/fellow/97-99/reinares.pdf.

47 See FELSEN, David and KALAITZIDIS, Akis. "A Historical Overview of Transnational…", loc. cit., p. 13-15.

48 EUROPOL, "OCTA 2011: EU Organised Crime Threat Assessment", p. 45, accessed September 26, 2013, https://www.europol.europa.eu/content/publication/octa-2011-eu-organised-crime-threat-assesment-1465.

49 See exceptionally comprehensive information on this topic in VALLÉS CAUSADA, Luís Manuel, *La Policía judicial en la obtención de inteligencia sobre comunicaciones electrónicas para el proceso penal*. (PHd diss., National Distance Education University, 2012), p. 32-35, accessed March 20, 2015, http://e-spacio.uned.es/fez/eserv/tesisuned:Derecho-Lmvalles/Documento.pdf.

2.1.3. Side effects of the internal policies

Crime rates in the EU between 1990 and 2001 in the same number of Member States rose by 20.9% from 20,734,870 crimes to 25,061,214. Of course, part of this can be due to the changes of national Penal Codes and the criminalisation of some acts, but not to this extent.[50] Thus there are other factors influencing such a criminality rate.

Global factors related to free trade and open financial markets made even stronger influence in the European Communities due to the creation of the internal market and the introduction of the single currency. In this respect, Occhipinti states that "As European leaders hastened their preparations for "E-Day", so too did organized-crime groups, especially potential money launderers, armoured-car and safe robbers, and counterfeiters."[51]

The single currency eliminated a need to exchange money received from criminal activities in order to circulate said money in other Member States. Furthermore, the 500-euro note had become one of the highest-value internationally circulating notes and it facilitated cash laundering and, as indicated by Europol's EU Organised Crime Threat Assessment OCTA 2011, "Due to overwhelming evidence that the 500 euro note is almost exclusively the preserve of criminals, banknote wholesalers have stopped supplying the note in the UK: however, it remains legal tender."[52]

Abolishment of internal border controls and free movement of people and goods also meant the abolishment of obstacles and risks to moving criminal activities to other Member States, as well as allowing the free circulation of criminals, either to commit crime or to hide from the law enforcement and justice authorities of other Member States were crime had been committed. As defines Storbeck, the EU has become "fertilising territory for criminality".[53] In this way, at the beginning of the nineties a big "migration" of Italian organised crime was noticed in Germany and Austria. At the same time in Belgium, it was found that almost half of organised groups had contacts with organised crime in neighbouring countries.

---

50 See SERRANO GÓMEZ, Alfonso and Vázquez GONZÁLEZ, Carlos, *Tendencias de la criminalidad y percepción social de la inseguridad ciudadana en España y la Unión Europea* (Madrid: Edisofer S.L, 2007), p. 126.
Although Austria, Finland and Sweden joined the European Communities in 1995, the figures from 1990 include crime rates from these countries as well.

51 OCCHIPINTI, John D., *The Politics of EU Police cooperation. Towards a European FBI?* (Colorado, Lynne Rienner Publishers, Inc., 2003), p. 120.

52 EUROPOL, "OCTA 2011: EU Organised Crime…", loc. cit., p. 42.

53 STORBECK, Jürgen, "La cooperación policial europea", loc. cit., p. 156.

In addition to the internationalisation of organised crime, another phenomenon called mobile criminality arose as a result of the free movement of people and goods. Even if it made an impression of being less dangerous than organised crime, it directly affects the everyday life of European citizens and "There is an inverse correlation between the seriousness and the incidence of victimisation."[54]

A positive democratisation processes in Central and Eastern Europe had also had its negative effect on the European Communities as the restructuring of heavy industry, an "engine of communist block", had left a lot of people without work and vulnerable to criminal influence. That led to the gathering in organised groups, illegal entrance to the European Community or just tolerance of the black market. New democracies with new economic changes and imperfect laws also allowed assets of criminal activities to be laundered through the privatisation of public property and conversion into legal businesses, with the desire to set up them in more stable and safer European Communities. On the other hand, new states were also in need of foreign capital and this opportunity was widely used to legalise western criminal proceeds.

All these factors contributed to the establishment of international co-operation and of common measure within the Member States of the European Community (and later, the European Union) against terrorism and crime.

2.2. The current situation

Just as time and evolution do not stand still, crime phenomenon is also changing and transforming into more sophisticated forms and new threats. Consequently, it is analysed and evaluated by competent authorities: at international level, the United Nations Office on Drugs and Crime and in, the EU – Europol.

As revealed by Transnational Organised Crime Threat Assessment from 2010, trafficking in human beings annually means 70,000 victims and a profit of US$ 3 billion in smuggling migrants – US$ 6,75 billion, drug trafficking – US$ 105 billion, trafficking in natural resources – over US$ 3,5 billion, trafficking in arms –US$53 million, product counterfeiting –US$ 9,6 billion, maritime piracy - US$ 100 million, cybercrime – US$ 1,25 billion.[55]

---

[54] BENYON, John, "Policing the European Union: The Changing Basis of Cooperation on Law Enforcement" in *International Affairs (Royal Institute of International Affairs 1944-)*, July 1994, vol. 70, no. 3, p. 500.

[55] See UNITED NATIONS OFFICE ON DRUGS AND CRIME, "The Globalization of Crime. A Transnational Organized Crime Threat Assesment. 2010", p. 16-17, accessed September 27, 2013, https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.

As these criminal activities generate such high profits, they are under constant development: change *modus operandi*, use of new technologies and other opportunities. This means that they will not disappear, but become more elaborate.[56]

SOCTA 2013, reveals increasing internationality of organised crime and "Criminals act undeterred by geographic boundaries and can no longer be easily associated with specific regions or centres of gravity".[57] From an estimated 3,600 organised groups, 70% are multinational, and 30 % are involved in multiple crime areas.[58]

In comparison with the previous situation, this is a novelty, because even five years ago, organised crime in the EU was more of a regional phenomenon. Thus earlier Europol reports revealed the existence of regional hubs within the EU. For instance, Organised Crime Threat Assessment (OCTA) 2009 revealed 5 hubs: North-West, South-West, North-East, Southern, and South-East and their "specialisation" in some crimes.[59]

Among actual crime-relevant factors, SOCTA 2013 distinguished:

- The economic crisis (that does not increase crime rates, but transforms them into other types, such as counterfeiting of daily consumer goods).
- Social tolerance to some crimes, such as consumption of psychoactive substances, purchase of counterfeited goods.
- Transportation and logistical hotspots that facilitate any type of transportation both within and outside the EU.
- The use of diaspora communities across the EU to facilitate irregular migration, property crime as well as entrance into countries' markets and legal business.
- Corruption with attempts (and some of them successful) to infiltrate organised crime into public and private sectors, to obtain information and to make beneficiary manipulations.
- Internet and e-commerce as a place for the circulation of illicit commodities.[60]

[56] Ibid, p. 1.
[57] EUROPOL, "EU Serious Organised Crime Threat Assessment (SOCTA 2013)", p. 45, accessed September 30, 2013, https://www.europol.europa.eu/content/eu-serious-and-organised-crime-threat-assessment-socta.
[58] Ibid, p. 33.
[59] EUROPOL, "OCTA 2009: EU Serious Organised Crime Threat Assessment", p. 13-14, accessed September 30, 2013, https://www.europol.europa.eu/content/publication/octa-2009-eu-organised-crime-threat-assessment-1463.
[60] EUROPOL, "EU Serious Organised Crime…", loc. cit., p. 11-19.

With respect to terrorism, during recent years, the threat fostered by Al Qaeda became even stronger with the pronouncement of the Islamic State; as the threat is both outside and inside Western Countries, and as Jenkins reveals, "The current cohort of jihadist volunteers may differ from previous cohorts in the level of their commitment to jihadist ideology and their attraction to unlimited violence as a motive for volunteering, as well as in the level of military skills they may acquire."[61]

According to TE-SAT 2014 elaborated by Europol, "AQ [Al Qaeda] and IS [Islamic State] retained their capability to recruit jihadists from Europe, intensifying the threat posed to the EU. In 2014, Member States also reported an increase in women and children travelling to the region. This phenomenon may eventually lead to the emergence of a new generation of jihadist terrorists in Europe. The number of fighters that have returned to the EU has increased.[62]

It also indicates that the risk of being kidnapped (especially when travelling to West Africa or the Middle East) has increased, especially taking into account such declaration as those of Al Qaeda leader, Ayman al-Zawahiri that in 2012 encouraged the kidnapping of "British, French, Italian or US citizens [...] with a view to influencing negotiations regarding prisoners in Afghanistan."[63] In 2013, 22 EU citizens were kidnapped in risk areas, a third of them – journalists.[64]

An IOCTA carried out at the end of September 2015 by the European Cybercrime Center revealed that "Cybercrime is becoming more aggressive and confrontational. Various forms of extortion requiring little technical skills suggest changes in the profile of cybercrime offenders, and increase the psychological impact on victims."[65]

---

61 JENKINS, Brian Michael, "When Jihadis Come Marching Home. The Terrorist Threat Posed by Westerners Returning from Syria and Iraq" (Perspective, RADN Corporation, 2014), p. 2, accessed August 3, 2015, http://www.rand.org/pubs/perspectives/PE130-1.html.

62 EUROPOL, "EU Terrorism Situation and Trend Report 2015", p. 6, accessed August 10, 2015, https://www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015.

63 EUROPOL, "TE-SAT 2014 - European Union Terrorism Situation and Trend Report 2014", p. 24, accessed August 10, 2015, https://www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014.

64 Ibid.

65 EUROPOL, "The Internet Organised Crime Threat Assessment (IOCTA) 2015", p. 45, accessed October 9, 2015, https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.

3. The legal framework of police cooperation within the EU

Since its origin in 1975, police and judicial co-operation had been out of the formal framework of the European Communities for around 20 years.

For the first time, the notion of public security was mentioned in the Community legislation in the Solemn Declaration on the European Union[66], signed on 19th June 1983, including as one of its objectives (but still in the form of intergovernmental co-operation) "A common analysis and concerted action to deal with international problems of law and order, serious acts of violence, organized international crime and international lawlessness generally."[67]

Judicial and police co-operation has obtained greater relevance in the Single European Act since it was signed on 17th February 1986[68], when it received the role of compensatory measure for the establishment of the internal market of the Community.

As pointed out by Moreno Catena, the Treaty of Maastricht signed on 7th February 1992 had gone beyond the pure economic idea of the old European Economic Community, and bet on the integration policy, making the EU something more than a common market and including the Second and the Third Pillars (common security as well as police and judicial co-operation). [69] Different from the First Pillar (supranational nature of common market), the Second and the Third Pillars were driven by the principles of intergovernmental co-operation, meaning different legislation, supervision and implementation procedures.

The intergovernmental and non-supranational nature of these Pillars is related to their previously discussed relationship with sovereignty, and as explained by Walker, "The longstanding macro-political distinction between those who are more or less reluctant to cede authority to the European level tends to be reinforced and highlighted in a policy area – internal security – which is a traditional preserve of the state, and, indeed, which many would see as part of [...] the indispensable raison d'être – of state sovereignty."[70]

---

66 Bulletin of the European Communities, no. 6/1983, p. 24-29.
67 Ibid, p. 25.
68 OJ L 169, 29.6.1987, p. 1-19.
69 See MORENO CATENA, Víctor, "El cambio de paradigma d el principio de reconocimiento mutuo y sus implicaciones. Perspectivas del Tratado de Lisboa" in CARMONA RUANO, Miguel; GONZÁLEZ VEGA, Ignacio U. and MORENO CATENA, Víctor, *Cooperación Judicial Penal…*, op. cit., p. 43-44.
70 WALKER, Neil, "In Search of the Area of Freedom, security and Justice: A Constitutional Odyssey" in WALKER, Neil, *Europe's Area of Freedom, security and Justice* (Oxford University Press: Oxford, 2004), p. 16.

Thus according to Article K.3 (2), of the Treaty of Maastricht, Member States were enabled to propose joint positions or joint action and conventions to prevent and combat terrorism, unlawful drug trafficking and other serious forms of international crime. To ensure that none of the Member States can be overruled by the rest, a unanimous decision for all mentioned legal acts was required and in the case of conventions - also ratification by each Member State according to its national rules. The only exceptions to this rule are measures that implement conventions and they are adopted by the qualified majority of Member States (unless otherwise provided in the convention that is subject to implementation).

At that time, the role of the European Parliament in the Third Pillar was limited to consultation on the principal aspects of activities and taking its opinion "into consideration" by the Council of the EU.[71]

The Treaty of Maastricht has foreseen the minimum regulation of the Third Pillar and was quite insufficient in its proper development. It was criticised by WALKER as "the AFSJ [Area of Freedom, security and Justice], even if part of its initial Maastricht inspiration was the attempt to supply a menu of compensatory measures concerning the control of movements across the EU's external borders and the development of new capacities for the internal monitoring of populations [...], has no finalité other than continuing adherence to a highly abstract triumvirate of values."[72]

The Treaty of Amsterdam, signed on 2nd October 1997, introduced significant modifications to the Third Pillar that allowed progress in this area. As noticed Fazekas "A great leap forward has been taken in the area of cooperation. Perhaps not the legislative aspect is the most important outcome here, but the fact that a common way of thinking and acting became accepted at a Union level regarding issues of internal security."[73]

First of all, its scope in justice and home affairs was changed into a "broader project of establishing an area of Freedom, security and Justice (AFSJ) throughout the EU"[74] meaning the establishment of balance between security, justice and fundamental rights and freedoms.

Secondly, the former Third Pillar's areas of asylum, internal borders, migration and co-operation in civil matters were all moved to the First Pillar (i.e. Under

71 Article K.6 of the Treaty of Maastricht.

72 WALKER, Neil, "In Search of the Area of Freedom …", loc. cit., p. 5.

73 FAZEKAS, Judit, "Development of Justice and Home Affairs Cooperation between 2004 and 2009 in the European Union" in *European Integration Studies*, 2009, vol. 7, no 1, p. 8.

74 LONGO, Francesca, "Justice and Home Affairs as a New Dimension of the European Security Concept" in *European Foreign Affairs Review*, 2013, vol. 18, no. 1, p. 39.

supranational regulation), remaining under the intergovernmental co-operation of the Third Pillar only areas of police and judicial co-operation.

Thirdly, the legislative procedure of the Third Pillar underwent important modifications.

As had been foreseen in Article K.6 of the Treaty of Amsterdam, acting unanimously on the initiative of any Member State or of the Commission, the Council could adopt common positions, framework decisions,[75] decisions[76] and conventions. New regulation laid down that every draft framework decision, decision and convention should undergo consultation with the European Parliament, although in practice its opinion has been taken into account only few times. The Commission was given the right to take the initiative in developing policy in this Pillar.

The need for the Council's unanimity resulted in a loss of ambitious content of many legislative initiatives due to the different interests of Member States. In many cases, the initial legal drafts with comprehensive regulation for the European police and judicial co-operation at the end of consensus, were converted into "light" co-operation instruments, in order not to modify national legislations or to make minimum of them.[77]

The Third Pillar in general was without effective control of the European Commission and European Court of Justice, i.e., the European Commission did not have the competence to start infringement procedures for non-implementation or erroneous implementation by the Member States Communities' instruments; additionally, the Court of Justice had had very limited jurisdiction in this area. Thus Article K.3 (2)c of the Treaty of Maastricht foresaw the competence of the Court of Justice only to interpret provisions of conventions adopted within the EU, and to rule on any disputes regarding their application, but only if expressly foreseen in them.

Article K.7 of the Treaty of Amsterdam also previsedthe "peculiar ad hoc system whereby the member states had to opt in to judicial control by the ECJ"[78] meaning that any Member State could make a declaration to accept the jurisdiction of the Court of Justice in order to give preliminary rulings on the validity and

[75] In order to approximate laws and regulations of Member States.

[76] For any purpose consistent with judicial and police co-operation, excluding approximation of laws and regulations that shall take the form of framework decisions.

[77] See Chapter V "Swedish Initiative".

[78] GUILD, Elspeth and GEYER, Florian, "Introduction: The Search for EU Criminal Law – Where is it Headed?" in GUILD, Elspeht and GEYER, Florian (eds.) *Security versus Justice? Police and Judicial Cooperation in the European Union* (Hampshire: Ashgate Publishing Limited, 2008), p. 6.

interpretation of framework decisions.[79] Nevertheless, the question of what effect decisions of validity would have on other Member States which had not made such a declaration still stood. Could they apply a framework decision recognised as invalid and not applied in other Member State?

By the Treaty of Amsterdam, on the initiative of Member States (but not the Commission, as in other areas), the Court of Justice has been endowed to review the legality[80] of framework decisions and decisions in general, in order to solve disputes between Member States on the interpretation or the application of common positions, framework decisions, decisions and conventions as well as between Member States and the Commission in cases of application of conventions.

Regarding information exchange, Article K.2(9) of the Treaty of Maastricht had only envisaged the creation of the Union wide information exchange system Europol. The Treaty of Amsterdam was more comprehensive on this issue, stating in Article K.2 that common actions within police co-operation should include "the collection, storage, processing, analysis and exchange of relevant information, including information held by law enforcement services on reports on suspicious financial transactions, in particular through Europol, subject to appropriate provisions on the protection of personal data."[81]

Thus the Treaty of Amsterdam had foreseen close co-operation with Europol in general, information exchange in particular and establishment within 5 years:

- Measures allowing the use of Europol's coordination and support capacity in specific investigative activities (such as joint investigation teams),
- Europol's right to ask Member States to conduct and coordinate their investigations when the case, the same organised group or other aspect involves investigations or operational activities of more than one Member State.
- Development of Europol's specific expertise to assist Member States in investigating cases of organised crime.

[79] See VILABOY LOIS, Lotario, "El sistema jurisdiccional comunitario". In MARIÑO, Fernando M.; MORENO CATENA, Víctor and MOREIRO, Carlos, *Derecho procesal comunitario* (Valencia: Tirant lo Blanch, 2001), p. 39-42.

[80] As a result of a lack of competence, infringement of an essential procedural requirements, infringement of this Treaty or of any rule of law relating to its application, or misuse of powers.

[81] OJ C 340, 10.11.1997, p. 17.

By the Protocol on the location of the seats of the institutions and of certain bodies and departments of the European Communities and of Europol[82] of the latter Treaty, political steps were taken by establishing Europol's seat in The Hague.

Articles K.15-K.17 of the Treaty of Amsterdam also envisaged a close co-operation procedure (as a tool to avoid the proliferation of cooperation outside the legal framework of the EU), that later was modified and developed by the Treaty of Nice[83] (signed on 26 February 2001) as enhanced co-operation.

Article 43a of the Treaty of Nice foresaw that "Enhanced cooperation may be undertaken only as a last resort, when it has been established within the Council that the objectives of such cooperation cannot be attained within a reasonable period by applying the relevant provisions of the Treaties."[84]

In such cases, a Member State could address a request to the Commission asking to submit a proposal of enhanced co-operation measure to the Council. If the Commission refused it, the proposal could be submitted to the Council by at least 8 Member States. The Council, acting by a qualified majority and after consulting the European Parliament, could grant authorisation of enhanced co-operation.[85]

The Treaty of Nice did not include any more novelties regarding police co-operation and information exchange, as its provisions were focused on ensuring smooth procedural and institutional functioning of the European Union after its significant enlargement by 10 new Member States in 2004.

Thus for the creation of the area of Freedom, security and Justice, not only legal, but also institutional resources were put in place[86] and as very well defined by Fijnaut, "The hard core of Member State Sovereignty was [...] gradually surrounded by the soft shell of the Community institutions."[87]

The Treaty of Lisbon was signed on 13th December 2007, raising the area of Freedom, Security and Justice to the level of supranational co-operation. It meant that the former Third Pillar reached its legal consolidation and became a part of the shared competence between the EU and Member States where Member States can only exercise the competence that is not assigned to the EU, or the latter has

82 OJ C 340, 10.11.1997, p. 112.
83 Articles 40-44 of the TEU.
84 OJ C 80, 10.3.2001, p. 12.
85 Since the Treaty of Lisbon, there is a requirement for at least o 9 Member States (instead of 8) for enhanced co-operation. It also modified a procedure of the authorisation of enhanced co-operation that foresees a need for the consent of the European Parliament instead of its pure consultation. See Article 329 of the TFEU.
86 See ARNÁIZ SERRANO, Amaya, *Evolución de la Cooperación Judicial...,* op. cit., p. 25.
87 FIJNAUT, Cyrille, "Police Co-operation and the Area of Freedom, security and Justice" in WALKER, Neil, *Europe's Area of Freedom…*, op. cit., p. 244.

decided to cease it execution.[88] As a consequence, the system of decision-making and implementation control was changing "making them subject to proper parliamentary and judicial control, in order to improve the balance between security and the judicial protection of citizens."[89]

Thus by means of the Treaty of Lisbon, the procedure of consultation in almost all areas was substitute by the ordinary procedure (also known as co-decision procedure) called by Peers "Two chamber legislation"[90], i.e. Approved by the European Parliament and a qualified majority of votes in the Council in the form of decisions, directives or regulations.

Articles 69 F and 69 H (Articles 87 and 89 of the consolidated version of the TFEU) of the Treaty of Lisbon maintains the procedure of consultation (renamed into special legislative procedure) for the measures concerning operational co-operation as well as for the establishment of the conditions and limitations under which the law enforcement authorities of the Member States may operate in the territory of another Member State. Article 69 B (article 83 of the consolidated version of the TFEU) foresees that acting unanimously, and after obtaining the consent of the European Parliament, the Council may establish minimum rules on the definition of criminal offences and sanctions in other areas of crime than those foreseen in the Article 69 B (1) part 2. [91]

Regarding the control system, Article 10 of the Protocol on Transitional Provisions of the Treaty of Lisbon[92] foresaw that not later than five years after the date of its entry into force, the Commission and the European Court of Justice should apply their full competence to the field of police co-operation and judicial co-operation in criminal matters, i.e. Infringement procedure and relative sanctions in cases of non-transposition, incorrect transposition or non-application of the EU legal provisions.[93] Thus since 1st December 2014, full EU control mechanism is applied to the transposition and implementation of the EU legal instruments.

---

88 See LLORENTE SÁNCHEZ-ARJONA, Mercedes, "La cooperación judicial penal en el Tratado de Lisboa" in DE LOS SANTOS MARTÍN OSTOS, José *El Derecho Procesal en el espacio judicial Europeo: estudios dedicados al catedrático Faustino Gutiérrez-Alviz y Conradi* (Barcelona: Atelier Libros S.A., 2013), p. 325.

89 PIRIS, Jean-Claude. *The Lisbon Treaty. A Legal and Political Analysis* (New York: Cambridge University Press, 2010), p. 178.

90 See PEERS, Steve, "Guide to EU decision-making and justice and home affairs after the Treaty of Lisbon" (Statewatch publication, December 2010), p. 3, accessed September 14, 2014. http://www.statewatch.org/analyses/no-115-lisbon-treaty-decision-making.pdf.

91 See PEERS, Steve, "Guide to EU decision-making and justice…", loc. cit., p. 3.

92 Protocol 36 of the consolidated version of the TFEU. OJ C 83, 30.3.2010, p. 322-326.

93 See PIRIS, Jean-Claude, *The Lisbon Treaty. A Legal and Political…*, op. cit., p. 188-189.

Nevertheless, as with previous Treaties, Article 240b[94] of the Treaty of Lisbon reiterates 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."[95]

Article 69 G[96] of the Treaty of Lisbon regulates Europol very comprehensively, i.e. By establishing its mission, excluding the application of coercive measures from its competence, foreseeing that its structure, operation, field of action, tasks, scrutiny of its activities shall be established within a new legal basis, adopted in accordance with ordinary legislative procedure.[97]

As evaluation of modifications introduced by the Treaty of Lisbon in relation to police and judicial co-operation, the following observations can be made:

- Changes in the Council's voting system can allow the approval of more ambitious co-operation instruments, even if not all Member States are in favour of them;
- The European Parliament's full participation in decision making introduces more transparency, although during the first years of its application, the European Parliament had been somehow "taking revenge" for its ignorance over the years in the process of consultation and blocked or delayed some initiatives.
- Application of control measures by the Commission and the Court of Justice of the EU ensures better implementation of EU instruments at national level.[98]

Summing up the trajectory of legal development of the area of Freedom, security and Justice and its growing importance, it can be said that it is no less an important issue than the introduction of Economic and Monetary Union and a Common Foreign and Security Policy.[99]

---

94 Article 276 of the consolidated version of the TFEU.
95 OJ C 306, 17.12.2007, p. 110-111.
96 Article 85 of the consolidated version of the TFEU.
97 More about the modifications introduced by the Treaty of Lisbon See MARISCAL, Nicolás, *Más allá de Lisboa: Horizontes europeos* (Técnos: Madrid, 2010), p. 174-177.
98 About unequal implementation read more in Section 2.4 of the Chapter V and "Swedish Initiative" and Section 2 of the Chapter VI.
99 See MITSILEGAS, Valsamis; MONAR, Jörg and REES, Wyn, *The European Union and Internal Security…*, op. cit., p. 6.

Nevertheless, some Member States still retain strong defence of sovereignty[100] and try to protect it with different means. For example:

- Protocols 21 and 22 of the Lisbon Treaty[101] entail that Denmark, Ireland and the United Kingdom will not take part in the adoption of measures within the area of Freedom, security and Justice and will not be bound by them. Ireland and the United Kingdom maintain the possibility of "opting-in" by notification addressed to the President of the Council, informing him / her of their wish to participate in the adoption of proposed measures within the area of Freedom, security and Justice. Such a declaration has to be submitted within 3 months of the presentation of the relevant proposal.
- Protocol 30[102] foresees that no court has competence to analyse whether Polish or British legal and administrative provisions are in accordance with the provisions of the of the Charter of Fundamental Rights of the European Union[103] (hereinafter – EU Charter).

The latest example of state self-protectionism is reflected in deliberations on the creation of the European Public Prosecutor's Office. Member States tend to endow it with competence only for the prosecution of criminal offences affecting the financial interests of the Union, and not those directly affecting EU citizens such as trafficking in human being, terrorism, cybercrime, drug trafficking and child pornography. This comes about due to the fear that the establishment of a powerful investigation entity would mean weakening the competences of each Member State.[104]

4. Principle of availability - the cornerstone of information exchange

In addition to the provisions of the primary EU law, establishing the main principles and aspects of EU politics, since 1999 the area of Freedom, Security and Justice has been developed by following the political guidelines of multiannual strategic programmes and their implementation plans.

After the entrance into force of the Treaty of Amsterdam, on 16 October 1999, the Presidency Conclusions "Towards a Union of Freedom, Security and Justice:

[100] See VON BOGDANY, Armin; CRUZ VILLALÓN, Pedro and M. HUBER, Peter, *El Derecho Constitucional en el espacio jurídico europeo* (Valencia: Tirant lo Blanch, 2013), p. 93.
[101] OJ, C 83, 30.3.2010, p. 295-303.
[102] OJ C 83, 30.3.2010, p. 313-314.
[103] OJ C 364, 18.12.2000, p. 1-22.
[104] See MORENO CATENA, Víctor, *Fiscalía Europea y Derechos fundamentales* (Valencia: Tirant lo Blanch, 2014), p. 13-14.

Tampere Milestones" (hereinafter - Tampere Conclusions) were adopted and became the first multiannual programme. Their "jewel in the crown" was the establishment of the principle of mutual recognition of judicial decisions and judgments as well as pre-trial orders. Besides, they also expanded the institutional background of the police and judicial co-operation foreseeing creation of:

- Eurojust – a unit with the mission to facilitate the coordination of national prosecuting authorities and to support criminal investigations of organised crime.
- European Police College (hereinafter – CEPOL) – a unit for the training of senior law enforcement officials.[105]

With regards to information exchange, it did not include any general guidelines, only stressing the need for its exchange between existing financial intelligence units and sending operational data from the Member States to Europol.

The importance of effective cross-border information exchange had become an object of political discussion after the terrorist attack of 11th September 2001 in the United States and intensified after the attack of 11th March 2004 in Madrid.[106] As Guile states, "These events have allowed many initiatives, which had previously encountered many difficulties in their development because of legal challenges, to see the light and be implemented in practice."[107]

Thus terrorism had been an accelerator for the constitution of the TREVI group in the 1970s' and after almost 30 years, gave a commencement to a new era of co-operation and "The "trigger" for formalising the "exchange" of information between law enforcement [...]"[108]

---

[105] Nowadays converted into a training unit for all law enforcement officials, not only senior ones.

[106] See GALÁN MUÑOZ, Alfonso, "La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea" in COLOMER HERNÁNDEZ, Ignacio and OUBIÑA BARBOLLA, Sabela. *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en al Unión Europea* (Navarra: Aranzadi, 2015), p. 45.
LEINIUS, Katharina, "An Imbalance between Security and Liberty? An Analysis of Cross-Border Information Exchange and Data Protection in the Context of the EU's Third Pillar since 9/11". (PhD diss, University of Twente, 2009), p. 9-10, accessed May 20, 2013, http://essay.utwente.nl/60243/1/BSc_K_Leinius.pdf; GUILLE, Laure, "Policing in Europe: An Ethnographic Approach to Understanding the Nature of Cooperation and the Gap between Policy and Practice", in *Journal of Contemporary European Research,* vol. 6, no. 2, 2010 p. 257, accessed January 30, 2013, http://www.jcer.net/index.php/jcer/article/view/192.

[107] GUILLE, Laure, "Policing in Europe: An Ethnographic Approach…", loc. cit., p. 257.

[108] BUNYAN, Tony, "The "principle of availability", Statewatch, December 2006, p. 2, accessed January 26, 2013, http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCEQFjAA&url=http%3A%2F%2Fwww.statewatch.org%2Fanalyses%2Fno-59-p-of-a-art.pdf&ei=7Jm_VLbDMYWuU9izgoAP&usg=AFQjCNFrlX_0fUkEc9zczWLutuiVFAblgA&bvm=bv.83829542,d.d24.

In less than one month after the attack of 11th March in Madrid, the European Council adopted a Declaration on combatting terrorism, emphasising among other measures:

- The simplification of the information and intelligence exchange between the law enforcement authorities of the Member States in as extensive manner as possible;
- Reinforcement of Europol;
- Focus on proactive intelligence;
- Bringing proposals on the retention of communication traffic data, on the exchange of DNA profiles and dactyloscopic data;
- The establishment of a European criminal records database.

In May-June of the same year, the Commission presented two communications: "Enhancing police and customs co-operation in the European Union"[109] and "Towards enhancing access to information by law enforcement agencies".[110]

In the first one, the Commission identified six general obstacles for EU wide police co-operation:

- Nature of police work – co-operation is possible as long as its arrangements do not encroach on national sovereignty and, as pointed out by Andersen, "Professional police agencies were an integral, and fundamentally important, part of the building of the sovereign nation state in Europe. For the police, whose function requires a simple focus of loyalty, this is a difficult legacy to eliminate."[111]
- Lack of strategic approach – as police and judicial co-operation had fallen under the Third Pillar, i.e. Intergovernmental co-operation, the Council's Presidency, changing every 6 months had been raising its own priorities without proper coherence with the previous or following Presidencies.
- Proliferation of Council conclusions and recommendations that have limited added value, and different interpretations on their obligatory nature.
- Decision making procedures in the Third Pillar – unanimity has made legislative process slow at all levels in the Council structures.
- Insufficient implementation of legal instruments at national level – the intergovernmental and not supranational nature of the Third Pillar has

[109] COM(2004) 376 final.
[110] COM(2004) 429 final.
[111] ANDERSON, Malcolm, "Trust and Police Co-operation", in ANDERSEN, Malcolm and APAP, Joanna, *Police and Justice Co-operation and the New European Borders* (The Hague: Kluwer Law International, 2002), p. 41.

excluded the application of control mechanisms that act as warranties of a correct and timely implementation of European instruments.

– Lack of empirical research in this area.[112]

The Commission outlined two axes to improve police and customs co-operation in the EU: the flow of information and actual cross-border co-operation.

Following this path in the following Communication ("Towards enhancing access to information by law enforcement agencies") specific obstacles for information exchange were described, for example "Compartmentalisation of information and lack of a clear policy on information channels."[113]

The Commission proposed establishing EU Information Policy for law enforcement based, first of all, on the improvement of information exchange and secondly to introduce the concept of intelligence-led law enforcement at EU level. In order to improve information exchange, a principle of equivalent access has been introduced as a right of "Access to data and databases within other EU Member States on comparable conditions as law enforcement authorities in that Member State. The corollary to that right is the obligation to provide access to law enforcement officials of other Member States under the same conditions as national law enforcement officials."[114]

Although in the introductory part of the communication "Towards enhancing access to information by law enforcement agencies", the Commission referred to the Council's Declaration on Combatting Terrorism, the proposed scope of the principle of equivalent access to information went beyond the fight against terrorists and includes serious and organised crime.[115] It can be explained by two reasons:

a) The high probability of links between terrorism and organised crime;

b) Reference to Article K.2 of the Treaty of Amsterdam to information exchange is not limited to fighting against terrorism, but to common actions on the collection, storage, processing, analysis and exchange of relevant information for law enforcement purposes.

The Commission's proposal "saw daylight" and political support in the second multiannual strategic programme – The Hague Programme that established the principle of information availability, applicable from 2008 onwards.

[112] COM(2004) 376 final, p. 36-40.
[113] COM(2004) 429 final, p. 3.
[114] COM(2004) 429 final, p. 7.
[115] And even more than that, the Commission has envisaged that "[...] it should be borne in mind that often criminal activity that would not appear to come within the category of "serious or organised" can well lead or be connected to it", COM(2004) 376 final, p. 4.

Equally to the principle of equivalent access, availability has converted the voluntary nature of transmitting of information into "Obligation to fulfil the information requests of other Member States."[116]

In this way it promoted a "space favouring the collectivisation of data"[117] as information became a property of all the authorities that need it in fighting criminal offences[118] and "the sociological norms regulating the practices of repressive authorities among themselves"[119] were changed.

Although, as Cabezudo Bajo points out, following the idea of the Commission, the principle of availability means direct on-line access to the information,[120] the Hague Programme does not mention it explicitly, leaving a question of access form open for further discussion.

Differently from the principle of equivalent access proposed by the Commission, the principle of availability is led by the list of conditions based on rational and necessary striking the balance between security and privacy. Thus The Hague Programme established that:

- Information is exchanged only in order to perform legal tasks of law enforcement;
- The warranty of the integrity of the exchanged data shall be applied;
- Protection of information sources and confidentiality of data at all stages of data processing shall be ensured;
- Common technical and access standards shall be introduced;
- Data protection shall be controlled;
- Protection of individuals from abuse of data shall be provided;

---

[116] ACED FÉLEZA, Emilio, "Principio de Disponibilidad y protección de datos en el ámbito policial" in *Noticias Jurídicas*, April 1, 2010, accessed September 25, 2013, http://noticias.juridicas.com:8080/articulos/15-Derecho-Administrativo/322-principio-de-disponibilidad-y-proteccin-de-datos-en-el-mbito-policial-.html.

[117] BIGO, Didier; BRUGGEMAN, Willy; BURGESS, Peter et al., "The principle of information availability", Challenge Liberty & Security, 2007, accessed January 26, 2013, http://www.libertysecurity.org/article1376.html.

[118] See BONN, Marjorie, "EL Programa de La Haya. El espacio de Libertad, Seguridad y Justicia en la Unión Europea" in ARROYO ZAPATERO, Luis and NIETO MARTÍN, Adán, *El Derecho Penal de la Unión Europea. Situación actual y perspectivas de futuro* (Universidad de Castilla-La Mancha: Cuenca, 2007), p. 34; BIGO, Didier; BRUGGEMAN, Willy, BURGESS, Peter et al. "The principle of information availability", loc. cit.; NIETO MARTÍN, Adán, "Modelos de organización del sistema europea de Derecho penal" in ARROYO ZAPATERO, Luis and NIETO MARTÍN, Adán. *El Derecho Penal de la Unión…,* loc. cit., p. 170.

[119] BIGO, Didier; BRUGGEMAN, Willy, BURGESS, Peter et al. "The principle of information availability", loc. cit.

[120] CABEZUDO BAJO, María José, "La protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal". In DE LA OLIVA SANTOS, Andrés (dir.); AGUILERA MORALES, Marien and CUBILLO LÓPEZ, Ignacio (coord.), *La Justicia y la Carta de Derechos Fundamentales de la Unión Europea* (Madrid: COLEX, 2008), p. 328.

– The right to seek correction of incorrect data shall be assured.[121]

The principle of availability became a cornerstone for police co-operation[122] in a similar manner to the principle of mutual recognition, established by the Tampere Conclusions, for judicial co-operation[123] and "The general political and practical guideline for the exchange of law enforcement information in the European Union."[124] Although some scholars, for example Ruggeri, say that availability derives from mutual recognition as free movement of data and information is a variation of the principle of mutual recognition.[125] In this respect, it can be said that both the principle of mutual recognition and the principle of availability have a common denominator – the free movement across state borders of elements. Which, during long periods of time, were considered as reflections of national sovereignty. Nevertheless, the nature of the recognition of judicial decisions in other Member States, and access to information, is different as in the first case, Member States are asked to recognise the results of foreign judicial processes and to execute them, and in the second case they are asked to "open" their deposits of information for foreign use.

For its implementation, the Commission has adopted an action plan "The Hague Programme: Ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice"[126] foreseeing fourteen measures for the improvement of information exchange, in particular: a general legal basis to implement the principle of availability, relevant data protection framework, mechanism on the use of passengers' data for law enforcement purposes (both at EU level as well as with the third countries, such as the United States of America, Canada, and so on), instruments on mutual consultation of DNA and fingerprint databases.

Despite the political boost for information exchange, two years later Bruggeman noticed that, "A lack of confidence [...] still blocks the exchange of information and raises questions concerning the protection of privacy in the use of the many electronic databases with personal data. Transnational crime often moves easily

[121] See OJ C 53, 3.3.2005, p. 8.
[122] See INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT AND EUROPEAN PUBLIC LAW ORGANIZATION, "Study on the status of information…", loc. cit., p. 35.
[123] Ibid.
[124] Council document 10333/12.
[125] RUGGERI, Stefano, "La transmisión de datos personales en cooperación judicial penal y policial en la UE. La perspectiva italiana" in COLOMER HERNÁNDEZ, Ignacio and OUBIÑA BARBOLLA, Sabela, *La transmisión de datos personales*…, op. cit., p. 280.
[126] COM(2005) 184 final.

across internal borders, while police and justice still hardly provide an effective and common approach."[127]

Five years later, the deadline of implementation of the principle of availability was not met because of the slow decision making process, delays with some proposals on the part of the Commission, information protectionism by some Member States, sensitivity to some issues.

Thus the principle of availability had not lost its relevance and was reiterated in later strategic documents:

- The Stockholm Programme of 2009 pointed out that the principle of availability will continue to give important impetus to the flow of information and acknowledged "the need for coherence and consolidation in developing information management and exchange."[128]
- The European Council Conclusions of 26-27 June 2014 (approved instead of new multiannual strategic programme)[129] reiterated that reinforced exchanges of information between the authorities of the Member States is required and that "intensifying operational cooperation while using the potential of Information and Communication Technologies' innovations, enhancing the role of the different EU agencies and ensuring the strategic use of EU funds will be key."[130]

According to the Stockholm Programme and Action Plan on its implementation,[131] the Commission had been tasked to evaluate the need of the European Information Exchange Model, and in 2012 came out with the conclusion that there was no need to propose any new instrument of initiative as "cross-border information exchange generally works well" and "a strong effort is still needed to ensure relevant

[127] BRUGGEMAN, Willy, "A Vision of Future Police Cooperation with Special Focus on Europol", in W. DE ZWAAN, Jaap and A.N.J. GOUDAPPEL, Flora, *Freedom, security and Justice in the European Union: Implementation of The Hague Programme* (Asser Press: The Hague, 2006), p. 207.

[128] OJ C 115, 4.5.2010, p.18.

[129] After the Treaty of Lisbon, Article 68 of the TFEU establishes that the European Council shall define the strategic guidelines for legislative and operational planning within the area of Freedom, Security and Justice. Notwithstanding, it does not foresee either term for which such guidelines shall be established nor obligation to approve them in the form of a programme. Thus in 2014, the European Council went back to the origins of strategic planning in the area of Freedom, Security and Justice and approved the strategic guidelines in the form of European Council Conclusions. In the area of security, it makes much more sense than a general programme, because almost in every area (for instance, drug trafficking, cybercrime, trafficking in human beings) there are individual multiannual programmes. And in case of the Stockholm Programme there was some overlapping and sometimes even contradiction to each other.

[130] Council document EUCO 79/14, p. 2.

[131] COM(2010) 171 final.

information is shared at Europol so as to create an EU-wide picture of cross-border criminality."[132]

In its Conclusions of June 2013[133], the Council agreed that there is no need for new legal instruments in this area, but better use of existing ones.

Besides multiannual strategies in the whole area of Freedom, Security and Justice, specialised strategies, such as "Information Management Strategy for EU Internal Security"[134] (hereinafter – IMS) and "Internal Security Strategy for the European Union. Towards a European security model" (hereinafter – ISS), also deserve a special mention.[135]

Thus in parallel with the development of the Stockholm Programme, in November 2009 the Council adopted the IMS that "aims to support, streamline and facilitate the management of information necessary for the competent authorities to ensure EU internal security, but excluding the responsibilities of Member States in safeguarding their national security."[136]

To this end, the IMS has foreseen eight steps in the planning and development of any new information exchange mechanisms:

a) To evaluate business needs and requirements, to analyse how existing solutions could be used for this purpose.

b) To follow already agreed law enforcement workflows and criminal intelligence models in new developments.

c) To ensure the balance between data protection requirements and business operational needs.

d) To ensure interoperability and co-ordination, both of business processes and technical solutions.

e) To share and re-utilise sustainable solutions whenever is possible.

f) To involve Member States from the very beginning of the process.

g) To establish clear responsibility for each part of the process.

h) To ensure multidisciplinary coordination within the Justice and Home Affairs area.

[132] Ibid, p. 14.
[133] Council document 7226/2/13, p. 2.
[134] Council document 16637/09.
[135] COUNCIL OF THE EUROPEAN UNION. "Internal Security Strategy for the European Union. Towards a European security model", accessed September 2014, https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf.
[136] Council document 16637/09, p. 6.

The IMS included a clause on its revision in 2014, and in November 2014 the Council re-affirmed the strategy and its implementation, introducing only minor wording changes and giving one new task to the Commission, "To examine the possibility of consolidating and increasing the efficiency of the existing legislation on law enforcement information exchange."[137]

In March 2010, ISS, foreseen in the Stockholm Programme, was approved with the aim of using a more integrated approach in tackling common threats and risks. With regard to information exchange, ISS has reiterated the Stockholm Programme, in relation to the need to strengthen mutual trust between competent law enforcement authorities, and use of the IMS for the development of the European Information Exchange Model.

As a continuation of ISS, in April 2015 the Commission approved "The European Agenda on Security"[138] which foresees better use of existing information exchange tools, such as the Schengen Information System, Prüm Decisions and Europol, as well as finding a political compromise on the European Passenger Name Records system.

Summing up the evolution of information exchange, we can refer to the reflexion of Leinius that "Security activity usually is characterized by a clandestine and insular thinking that makes cooperation even between different security actors of the same member state difficult; the principle of availability therefore is no less than revolutionary in its intention."[139]

It gave a political acceleration to development in this area, and served as a basis for numerous initiatives, some of which will be analysed in the following chapters. Nevertheless, its full and proper implementation took much longer than was forecast at the beginning and it is still in the process.

5. Information, intelligence and personal data

Although the title of the thesis only contains the term "information" and the above mentioned principle talks about availability of information, during the analysis of specific legal terms, "information", "intelligence" and "personal data" or "intelligence" will be frequently met. For example, legislation related to Europol includes all three terms and applies different regulations, the Swedish Initiative talks about information and intelligence, all mechanisms differentiate between

[137] Council document 15707/1/14, p. 9.
[138] COM(2015) 185 final.
[139] LEINIUS, Katharina, *An Imbalance between Security and Liberty?...,* op. cit., p. 15.

information in general, and personal data. Thus the principle of availability covers all three categories.

The most general and laconic explanation of information is knowledge of learned facts or details about something or someone.[140]

A more comprehensive definition is provided by the Business Dictionary, which understands information as "data that is accurate and timely, specific and organised for a purpose, presents within a context that gives it meaning and relevance and can lead to an increase in understanding and decrease in uncertainty".[141]

EU legislation on police and judicial co-operation does not foresee a definition of information with the exception of the Council Framework Decision 2006/960/JHA of 18th December 2006, on simplifying the exchange of information and intelligence between the law enforcement authorities of the Member States of the European Union (hereinafter –Framework Decision 2006/960/JHA).[142] Nevertheless, its Article 2.d gives a single definition to "information and/or intelligence", and describes it as "(i) any type of information or data which is held by law enforcement authorities; (ii) any type of information or data which is held by public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures, in accordance with Article 1(5)." Such a definition is erroneous as to determine the term "information" in its definition also include the term "information" and therefore cannot be used as a background for analysis.

In these circumstances, there is a need to establish the meaning of information within the context of police investigation, and it should be understood as a piece of data that allows the re-establishment of a wide picture of a crime, and all the related circumstances, and when necessary, to follow pre-established requirements to obtain consideration of evidence.

Unlike poor discussions on the term "information" within police investigation, much more attention is paid to the term "intelligence".

---

[140] See MacMillan Dictionary, http://www.macmillandictionary.com/dictionary/british/information; Oxford Dictionary, http://www.oxforddictionaries.com/definition/english/information.

[141] Business Dictionary. http://www.businessdictionary.com/definition/information.html#ixzz3orOh5ddk.

[142] OJ L 386, 29.12.2006, p. 89-100.

As the Spanish National Intelligence Centre explains, information is a news or a fact and is a starting element to develop intelligence that is considered as a result of evaluation, analysis, integration and the interpretation of information.[143]

But before defining criminal intelligence, two things should be pointed out. First of all, a difference should be made between "intelligence" as an element of the work of the national security services and "intelligence" in the meaning of police investigation. In cases of performing functions of national security services, it will be the analysis of "information related to capacities, intentions or activities of foreign governments as well as of organisations and persons that acts against national interests."[144] Thus, as pointed out by Bruggeman, "The term intelligence can be limited to authentic intelligence services or be understand broader and include all law enforcement authorities. CIA presents it in a very simple way: intelligence is knowledge and previous knowledge of the world that is surrounding us."[145] Secondly, it should be taken into account that the terms "information" and "intelligence" in road meaning are mostly used in common law countries, and in Eastern Europe, intelligence is very often still understood in a narrow way in association with national security services; criminal intelligence is referred to simply as the result of the analytical work of the criminal police.

A very comprehensive comparison between information and criminal intelligence is provided by Marica, who understands information as material that includes non-evaluated observations, communications, reports, rumours, images and sources from which criminal intelligence is made.[146] For example, when a competent authority asks for information about an organised group, it could include information (criminal facts, number of members, etc.) As well as intelligence (analysis of behaviour, probable future crimes, etc.).

Díaz-Pintado Moraleda explains intelligence simply as "mutation of information through the process of integration and interpretation."[147]

In the process of making intelligence, whether or not information has "material value or potential material value"[148] for the police or not is evaluated, and

[143] See CENTRO NACIONAL DE INTELIGENCIA, "¿Qué diferencia hay entre información e inteligencia?", accessed July 15, 2015, http://www.cni.es/es/preguntasfrecuentes/pregunta_010.html?pageIndex=10&faq=si&size=15.

[144] DÍAZ MATEY, Gustavo, "Hacia una definición de Inteligencia" in *Revista Inteligencia y Seguridad*, no. 4 (July – November 2008), p. 71.

[145] BRUGGEMAN, Willy, "Los procesos de construcción de una inteligencia europea" in MONTERO, Julián; ROMERO, Francisco and VALIENTE, Elena *¿Hacia una Policía Europea?*, op. cit., p. 215.

[146] See MARICA, Andreea, *Manual de Europol* (Navarra: Aranzadi, 2014), p. 121-122.

[147] See DÍAZ-PINTADO MORALEDA, Pedro, "El modelo de inteligencia en la organización policial" in MONTERO, Julián; ROMERO, Francisco and VALIENTE, Elena, *¿Hacia una Policía Europea?* op. cit., p. 231.

therefore it is considered that intelligence is qualitatively different from information.[149]As pointed out by O'Neill, "It should lead to "informed decision making", allowing for the "targeting of offenders" as the "best way to use our scarce police resources"."[150]

Notwithstanding, it does not mean that intelligence is necessarily more important than information. Sometimes there is no need of intelligence, but just information; for example, when there is a need to know a person's location at a certain moment or whether his or her mobile phone was switched on, or who is the owner of vehicle that was used to commit a crime, and so on.

The last example of information about the owner of the vehicle includes two types of information: information about the vehicle and information about the person. The last one is personal data and the object of stricter protection. Information about the color of the vehicle, its technical characteristics, or traces of accidents for example, will be general or depersonalised information and that about the owner, his or her driving license or address - will be personal data.

Unlike information and intelligence, personal data is defined by the European legislator in many legal acts; for example beginning with the Council Framework Decision 2008/977/JHA of 27th November 2008, on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (hereinafter – Framework Decision 2008/977/JAI)[151], the Council Decision 2009/936/JHA of 30th November 2009 adopting the implementing rules for Europol analysis work files[152] (hereinafter – Decision 2009/936/JHA), the Council Decision 2009/934/JHA of 30th November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information[153] (hereinafter –Decision 2009/934/JHA), Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generations Schengen Information System (SIS II)[154] (hereinafter – Decision 2007/533/JHA).

---

148 INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT AND EUROPEAN PUBLIC LAW ORGANIZATION, "Study on the status of information…", loc. cit., p. 16.

149 See DÍAZ-PINTADO MORALEDA, Pedro, "El modelo de inteligencia en la organización…", loc. cit., p. 231.

150 O'NEILL, Maria, "The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar", in *Journal of Contemporary European Research*, vol. 6, issue 2, 2010, p. 229, accessed July 15, 2014, http://www.jcer.net/ojs/index.php/jcer/article/view/264/206.

151 OJ L 350, 30.12.2008, p. 60-71. Also applied to Iceland, Ireland, Norway, Switzerland, Liechtenstein and United Kingdom.

152 OJ L 325, 11.12.2009, p. 14-22.

153 OJ L 325, 11.12.2009, p. 6-11.

154 OJ L 205, 7.8.2007, p. 63-84.

All of the above mentioned legal acts coincide in defining personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly".[155] All acts except Decision 2007/533/JHA specify that direct or indirect identification can be made "in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity".

Not all legal acts on information exchange that will be analysed regulate all three categories; but definitely in all of them, the difference between the processing of depersonalised and personal data is highlighted. The last one is always subject to stricter regulation, but the level of restriction varies depending on the information exchange mechanism.

[155] Article 2 of the Framework Decision 2008/977/JHA, Article 1 of Decision 2009/936/JHA, Article 1 of Decision 2009/934/JHA, Article 3 of the Decision 2007/533/JHA.

CHAPTER 2:
FUNDAMENTAL RIGHTS AND FREEDOMS UNDER CONSIDERATION

In the very recent European Data Protection Supervisor Strategy 2015-2019 is emphasised that "Our [EU] values and our fundamental rights are not for sale. The new technologies should not dictate our values, and we should be able to benefit both from new technologies and our fundamental rights."[156]

As stated in the "European Agenda on Security", reiterating case law of the European Court of Justice "Security and respect for fundamental rights are not conflicting aims, but consistent and complementary policy objectives."[157]

Security alone, has one of the aims to ensure full and free enjoyment of fundamental rights without fear that something like a terrorist attack or crime can impede it and deprive, for example, from the right to live, the right to physical or moral integrity. On the other hand, ensuring security legislators endows some institutions, including the judiciary and the police, with administrative power that comprises coercive or other measures over citizens that also leads to the limitation of some fundamental rights. Notwithstanding, such limitation of fundamental rights should be balanced and always subject to legitimacy, proportionality and some additional conditions.[158]

Nevertheless, Barona Vilar asserts that with the terrorist attack of 11th September, the "honey moon" between the world and fundamental rights came to an end.[159] Also Gascón Inchausti points out a tendency towards change in the penal process,

[156] EUROPEAN DATA PROTECTION SUPERVISOR, "The European Data Protection Supervisor Strategy 2015-2019", p. 11, accessed September 30, 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-02-26_Strategy_2015_2019_EN.pdf

[157] COM(2015) 185 final, p. 3.

[158] See for example GIMENO SENDRA, Vicente, *Manual de Derecho Procesal...*, op. cit., p. 46.

[159] See BARONA VILAR, Silvia, *Seguridad, celeridad y justicia penal* (Valencia: Tirant lo Blanch, 2004), p. 75.

from a process of "humanization" (based on warranties to the accused) into a process as an instrument for individual or collective security.[160] Although he makes general reference to "new techniques of investigation",[161] information exchange and its processing could be interpreted as such, due to the fact that all related measures were adopted as measures to increase security.

Therefore, this Chapter sets out to analyse existing interrelations and balance between security and fundamental rights, and freedoms in general, and to look in depth at rights directly related to information exchange in police investigation, i.e. Privacy and data protection.[162]

It should be taken into consideration that limitation of privacy occurs at the moment of data is obtained in one Member State or another, and is always subject to national regulation. Thus the question of the legality of limitation of privacy will be solved according to the legislation of that Member State and in cases of violation, the state will be responsible for its infringement. However, responsibility for data protection lies with every Member State or agency involved in its processing. For example, law enforcement or the justice institutions of one Member State are empowered to collect and further process data on a person's itineraries. This is the moment of interfering in privacy and, depending on the national legislation of the Member State that is interfering, can be treated as a valid limitation or a violation. Data obtained is subject to data protection that has to be applied during the entire processing procedure, both inside and outside of that Member State. Consequently, the greater part of this Chapter is dedicated to research on the data protection rules applied when personal data is "crossing the border".

In contrast to the other Chapters, where only the EU legal framework is analysed, this one will also include legislation and case law of the Council of Europe as:

- All Member States are part of the ECHR.
- Article 6(3) of the TFUE foresees that the Fundamental rights foreseen in the ECHR are treated as general principles of the EU.

[160] GASCÓN INCHAUSTI, Fernando, "Los procesos penales en Europa: líneas de evolución y tendencias de reforma", in *Revista de Derecho Procesal*, 2009, no. 1, p. 47.

[161] Ibid, p. 48.

[162] Of course, depending on information type, other fundamental rights can be under consideration, for example, in processing of DNA data questions about non-self-incrimination, non-incrimination of descendants or relatives, the right of children to personal development. See more: SOLETO MUÑOZ, Helena and FIODOROVA, Anna, "DNA and Law Enforcement in the European Union: Tools and Human Rights Protection" in *Ultrecht Law Review,* January 2014, vol. 10, issue 1, p. 154-158; SOLETO MUÑOZ, Helena, "DNA data in criminal procedure in the European fundamental rights context" in *Recent Advances in DNA and Gene Sequences*, 2014, 8(2), p. 91-97.

- Article 52(3) of the Charter envisages that when it and the ECHR establish the same rights, their meaning and scope shall be equal to the Convention, except where the Charter provides.
- Case law of the ECtHR shall be taken into account when interpreting the Charter.[163]

It has to be mentioned that Article 6(2) of the TEU (modified by the Treaty of Lisbon) establishes that "the Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties."

Nevertheless, the European Court of Justice in its opinion 2/13 came to the conclusion that "the agreement on the accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms is not compatible with Article 6(2) TEU or with Protocol (No 8), relating to Article 6(2) of the Treaty on European Union on the accession of the Union to the European Convention on the Protection of Human Rights and Fundamental Freedoms."[164] This conclusion was made due to the consideration that it will affect the specific characteristics of EU law and its autonomy, as well as the division of the power established in Article 344 of the TFEU. For example, there would be an overlap of the competence between the ECtHR and the European Union Court of Justice, in the case of the interpretation of human rights established in the ECHR and the EU Charter. [165]

1. Security deficit vs. democracy deficit

As revealed by a Eurobarometer survey carried out this year, "Europeans' attitude towards security", 79 % of the Europeans think that the EU is a safe place to live. But asked about the main challenges to security, people mostly mentioned terrorism, secondly, the economic and financial crisis and thirdly organised crime, corruption and poverty. Besides, both terrorism and organised crime are seen as increasing threats in the future.[166]

[163] COM(2015) 191, p. 11.

[164] Opinion of the Court of 18 December 2014, Opinion pursuant to Article 218(11) TFEU - Draft international agreement - Accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms - Compatibility of the draft agreement with the EU and FEU Treaties, ECLI:EU:C:2014:2475.

[165] See ETXEBERRÍA GURIDI, José Francisco. "Los derechos fundamentales en el espacio de libertad, seguridad y justicia penal", in *Revista Vasca de Administración Pública*. 2008, no. 82, 2, p. 160-163.

[166] EUROPEAN COMMISSION, "Special Eurobarometer 432. "Europeans' attitude towards security", April 2015, accessed July 10, 2015, p. 4, 6, 9, http://ec.europa.eu/public_opinion /archives/ebs/ebs_432_sum_en.pdf.

Threats to security mean threats to the enjoyment of all the freedoms and rights endowed on a person, and they cannot be prevented or combatted without social order that depends on effective policing[167] and as noted by Bruggeman "In order to safeguard the enjoyment of liberties and efficient protection, it is necessary, to obtain it, that those charged with that protection must be empowered with the adequate means and the possibility of action."[168]

As already mentioned, those necessary security tools sometimes mean limitations of human right and provoke a paradox: to guarantee the security to enjoying liberties and rights in general, there is a need to limit some fundamental rights. And in these circumstances, the question stands: what prevails? Where should we be able to find the limit or balance between the State's role as guardian of rights and arbiter in security? Or as pointed out precisely by Vallés Causada, "What fundamental rights would remain to people if the criminal tumor exceeded State's surgical capacities?"[169]

From first sight, it seems that there is no doubt about the priority of fundamental rights as they are a primary necessity,[170] but which fundamental rights? A person's right to life (in the case of a victim), or the right to privacy of communication (in the case of a suspect)? The right of hostages to live, or the right of the physical integrity of a kidnapper?

The answer to these questions will not be the same, not even when making comparisons among democratic states which strongly apply the Rule of Law. For example, in the case of Sweden or Norway, greater consideration would be given to rights of a suspect or kidnapper than in the United States of America or the United Kingdom where, in the light of new circumstances (basically the threat of terrorism), and the State's duty to protect residents (and first of all their right to live), the process of re-prioritisation of human rights takes place.[171] For example, after 11th September, on 19the November, the Parliament of the United Kingdom adopted the Antiterrorism, Crime and Security Act that foresaw a petition to the House of Commons to derogate Article 5 of the ECHR (the right to liberty and security), and established the possibility of indefinite detention of foreign suspects of terrorism who could not be expelled, and broader possibilities on intervention of communications or financial data, limited possibilities of a lawyer to receive

[167] See CRAWSHAW, Ralph; DEVLIN, Barry and WILLIAMSON, Tom, *Human Rights and Policing. Standards for Good Behaviour and a Strategy for Change* (Dordrecht: Kluwer Law International, 1998), p. 20.

[168] BRUGGEMAN, Willy, "Policing in a European Context" in APAP, Joanna, *Justice and Home Affairs…*, op. cit., p. 152.

[169] VALLÉS CAUSADA, Luís Manuel, *La Policía judicial en la obtención…,* op. cit., p. 84.

[170] See BARONA VILAR, Silvia.,*Seguridad, celeridad y justicial…,* op. cit., p. 78.

[171] See MCGHEE, Derek, *Security, Citizenship and Human Rights. Shared Values in Uncertain Times* (Hampshire: Palgrave McMilan, 2010), p. 60-61.

information about all evidences.[172] In the draft project it was also proposed to repeal Article 5 of the ECHR related to liberty and security.[173] The Act was in force until 2004 and was then substituted by a more flexible act, but one which still allowed the limitation of fundamental procedural rights. Such regulations tend to make a division between law for citizens and "law of enemies".[174] Biondo explains that such exceptional situations brought into question the efficiency of state institutions and constituted a threat to State sovereignty and therefore, as a consequence, fundamental rights and the system of warranties are challenged.[175]

On the other hand, in Norway, even after the massacre of Breivik on 22nd July 2011 legislative changes giving more powers to law enforcement authorities were not made; furthermore, "Terrorism legislation remains the same and there have been no special provisions made for the trial of suspected terrorists."[176]

The position of Norway is almost unique as many countries, even not directly affected by the terrorist attacks in the United States, Spain and the United Kingdom, have strengthened security measure that have resulted in bigger or broader restrictions of some fundamental rights.

With respect to human rights, the British Government's position in general deserves special attention. It underlines a deficit of public security and considers approval of a Modern Bill of Rights to define core values. As a consequence, the United Kingdom could stand back from the ECHR and the obligation to obey ECtHR judgments, as some of them have been found by the British authorities to misinterpret the ECHR, especially those on banning "sending home foreign criminals".[177]

---

[172] See JIMÉNEZ FORTEA, Francisco Javier, "La respuesta procesal penal al terrorismo en el marco de la Unión Europea: un ejemplo de cooperación judicial penal y policial" in CALDERÓN CUADRADO, Mº Pía and IGLESIAS BUHIGUES, José Luís, *El Espacio Europeo de Libertad, Seguridad y Justicia: Avances y Derechos Fundamentales en Materia Procesal* (Navarra: Aranzadi, 2009), p. 81.

[173] See JIMÉNEZ FORTEA, Javier, "De la restricción de derechos a un "derecho procesal del enemigo", in MASFERRER, Aniceto, *Estado de Derecho y derechos fundamentales en la lucha contra el terrorismo* (Navarra: Aranzadi, 2011), p. 616-617.

[174] See JIMÉNEZ FORTEA, Francisco Javier. *La respuesta procesal penal...,* loc. cit., p. 85-86.

[175] BIONDO, Francesco, "Emergencia y garantías (en el pensamiento jurídico de Luigi Ferrajoli)." In MASFERRER, Aniceto. *Estado de Derecho y derechos…*, op.cit., p. 516-517.

[176] GALPIN, Richard, "Norway prepares for killings anniversary", *BBC,* 20 July 2012, accessed July 22, 2012, http://www.bbc.com/news/world-europe-18791448.

[177] See MCGHEE, Derek, *Security, Citizenship and Human Rights…,* op. cit., p. 97, 99; "David Cameron: British bill of rights will 'safeguard legacy' of Magna Carta", *The guardian,* 15 June 2015, accessed September 8 2015, http://www.theguardian.com/law/2015/jun/15/david-cameron-british-bill-of-rights-safeguard-legacy-magna-carta; "David Cameron Won't Rule Out Ditching European Convention On Human Rights", *The Huffington Post,* 3 June 2015, accessed September 8 2015, http://www.huffingtonpost.co.uk/2015/06/03/prime-ministers-questions-human-rights-bill-of-rights-refuse-rule-out_n_7501460.html.

One of the judgments that urged the taking of such a decision was the case *Chahal v United Kingdom* in 1996. In this case the Government of the United Kingdom took a decision to deport Mr Chahal (who was a leader of the Sikh community, a separatist movement for independence in one of the regions of India – Khalistan) to India, as it had considered his behaviour "unconducive to the public good for reasons of national security, and other reasons of a political nature, namely the international fight against terrorism."[178]

The ECtHR (with 12 votes to 7), found that the right to not be subjected to torture or inhuman treatment (established in Article 3 of the ECHR) is absolute and therefore, the Government's decision on deportation to India was contrary to this Article, as there was a high probability that in India, Mr Chahal, being a separatist, would be subject to torture or inhuman treatment and "in these circumstances, the activities of the individual in question, however undesirable or dangerous, cannot be a material consideration."[179]

In respect to this and similar cases, a few aspects have to be highlighted:

- Decisions to expel are taken by the State's Executive Power and the Judicial Power cannot always overrule them (as in the quoted case).
- The deficit of security starts to prevail over the deficit of fundamental rights and liberties.
- Recognising the correctness of such ECtHR judgments, there is still a pending question: What should competent authorities do with respect to similar persons, bearing in mind their potential threat to the security and rights of other residents?

The British Conservatives also questioned ECtHR carrying out interpretations of the ECHR, making it a "live instrument" and considered this to be going far beyond the meaning that had been given to some rights. For example, with respect to prisoners' right to vote, the Conservatives declared "the issue of the franchise in elections was deliberately excluded from the text of the Convention. The Strasbourg Court has, however, now decided that it falls within the Convention's ambit."[180]

They also stated that "another clear example of 'mission creep' came in a 2007 ruling by the Court that required the UK Government to allow many more prisoners the right to go through artificial insemination with their partners, in

[178] ECtHR, *Chahal v the United Kingdom* [1996], paragraph 25.
[179] Ibid, paragraph 80.
[180] UK Conservatives, "Protecting Human Rights in the UK. The Conservatives' proposal for changing Britain's Human Rights Laws", p. 3, accessed August 13 2015, https://www.conservatives.com/~/media/files/downloadable%20Files/human_rights.pdf.

order to uphold their rights under Article 8. This is not what the originators of the Convention had in mind when they framed that article."[181]

After the re-election of the Conservatives in spring 2015, the question of a new British Bill of Rights has been raised again.

From first sight, it seems that possible "re-prioritisation" would limit the rights of suspects or convicted persons. Nevertheless, taking into account that the United Kingdom already applies the processing of passenger name records for security purposes (about PNR see section 3 of Chapter VIII), some limitation will cover all of society in general.

The position of the United Kingdom in relation to this and to other questions, including remaining or not in the European Union, can seem radical in comparison to the rest of Europe, but it is in fact something that could serve as a precedent in the future.

Nevertheless, going back to the majority of western countries, restriction of fundamental rights takes place within the limits established by international conventions and national Constitutions that are also justified by the ECtHR. Nevertheless, there are also signs of gradual expansion of purposes, categories of persons and facilitation of the procedure. For example, in France categories of crimes for which DNA profiles can be stored in national data base have been expanded from sexual offences to serious crimes and then less serious. Originally only DNA profiles of convicted persons were processed, but later legislator has permitted to process those of suspects. In Germany categories of data crimes also has been expanded and previous obligation of judicial authorisation has been made more flexible.[182] The key issue of limitations has to be respect to principle of proportionality that will be discussed later. For example, in the case of *B.B. v. France*, the ECtHR recognised that processing the data of a convicted sex offender interferes with the right to data protection, but with adequate data safeguarding, limited storage and access, the public interest in that data can be ensured.[183] Many European countries directly apply principles of proportionality, establishing that the limitation of fundamental rights can take place depending on the type of crime or punishment.[184]

---

[181] Ibid.

[182] See ETXEBERRÍA, GURIDI, José Francisco, "La identificación de personas mediante pruebas genéticas y bancos de perfiles de ADN: evolución normativa en el contexto europeo" in *Revista de Derecho y Genoma Humano*, 2014, extra ordinary issue, p. 140-142, 145, 150.

[183] ECtHR, *Affaire B.B. v France* [2009], paragraphs 61, 62, 70.

[184] MORENO CATENA, Víctor, "La garantía de los derechos fundamentales durante la investigación penal" in *LIDÓN, María José. Problemas actuales del proceso penal y derechos fundamentals,* 2010, ed. 7, p. 18.

With respect to EU policies, the security deficit felt after the terrorist attacks of 2001, 2004 and 2005 prevailed over the democracy deficit for some time and resulted in the adoption of different measures to combat terrorism and crime that intervene in fundamental rights, reducing their protection to secondary importance.[185] An attempt to re-establish the balance was made in the Internal Security Strategy by envisaging that freedom, justice and security policies would have to be developed, "Respecting fundamental rights, international protection, the rule of law and privacy."[186]

To end with this issue it would be biased not to mention the view of Vallés Causada, that judicial police activities reflect an adaptation of the complexity of the evolution of technology, and sometimes help us to assure less interference with fundamental rights than before; for example, using state-of-the-art metal detectors and scanners instead of carrying out intrusive searches.[187]

2. Information exchange and due process

Information exchange between law enforcement authorities for the purpose of crime investigation has another, wider aim – to contribute to the performance of justice. In this respect, each element of investigation and each piece of information has to be considered as a source of evidence in the judicial process. This circumstance approximates information exchange to procedural warranties, and allows the estimation of its impact on the due process, although their direct relationship is maybe not so clear.

To show the interrelationship between information exchange and the due process, there is a need for the analysis of the elements of the latter, which will gradually show its link to information exchange.

Firstly, the due process is a fundamental warranty for each person facing a judicial process, and it consists of presumption of the innocence, the inviolability of defence and pre-judgement.

[185] GALÁN MUÑOZ, Alfonso, "La protección de datos de carácter…", loc. cit., p. 48.

[186] COUNCIL OF THE EUROPEAN UNION "Internal Security Strategy…", loc. cit., p. 19.

[187] See VALLÉS CAUSADA, Luís M, "Usos delictivos no comunicativos de la telefonía móvil: una excepción a la protección del artículo 18.3 CE?" in PÉREZ GIL, Julio, *El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar y probar el delito* (Madrid: La Ley, 2012), p. 237.

Secondly, as indicated by López Ortega in the understanding of the classical school of Criminal Law, the presumption of innocence is the crucial element and starting point of the criminal process.[188]

Thirdly, every international and regional declaration of human rights considers that in order to abolish the presumption of innocence, "proof of guilt" is needed.[189] Thus it is directly related with evidence.[190]

Fourthly, proof of guilt or non-guilt is achieved by presenting evidence that demonstrates the truth. In the process, the truth has two sides: material and formal and therefore is called procedural truth,[191] i.e., in order to be admitted as evidence in a process, it is not enough to find out the truth, it has to be done according to legal requirements in order to ensure security of legal traffic.192 Therefore evidence is not just a truth, but also legal construction.193 Among requirements for truth it is foreseen that it cannot produce violations of fundamental rights, such as the right not to be tortured, to physical integrity, personal liberty, privacy or secrecy of communications.[194] That puts some limits of freedom of investigation by prohibiting or disregarding some means of evidence. Thus if evidence was collected and processed and fundamental rights were violated during the process, the evidence would be prohibited[195] and the collection violating procedural requirements – illicit.[196] In addition to elements of violation of fundamental rights in the collection of evidence, there has to be one more element – the connection between violation and collected evidence.[197]

In some countries (Canada, Italy, the Netherlands, Spain and United States) illicit evidence being will provoke a domino effect on other evidence that originating

---

188 See LÓPEZ ORTEGA, Juan José, "Los principios constitucionales del proceso penal", in *Derecho Procesal Salvadoreño* (San Salvador: Justicia de Pat, 2000), p. 84.

189 Article 11.1 of the Universal Declaration of Human Rights, Article 14.2 of the International Covenant on Civil and Political rights, Article 6.2 of the ECHR, Article 41.1 of the EU Charter.

190 GÓMEZ AMIGO, Luis and BLANCO SANTOS, Gemma, *Fuentes de prueba y nuevas formas de criminalidad* (Almería: Universidad de Almería. Servicio de Publicaciones, 2001), p. 53.

191 See GIMENO SENDRA, José Vicente, *Fundamentos del Derecho* (Procesal: Madrid: Civitas, 1981), p. 213.

192 Ibid, p. 214.

193 See ETXEBERRÍA GURIDI, José Francisco, "Los derechos fundamentales en el espacio...", loc. cit., p. 130.

194 In some countries, for example Italy, also called unconstitutional evidence. See MIRANDA ESTRAMPES, Manuel, "La prueba ilícita: la regla de exclusión probatoria y sus excepciones" in *Revista Catalana de Seguretat Pública*. Mayo, 2010, p. 132-134.

195 In Spain for the first time, illicit evidence was mentioned by the Constitutional Court in its judgment 114/1984 and then included into Organic Law won Judicial Power. See more. DE LA OLIVA SANTOS, Andrés, *Escritos sobre derecho, justicia y libertad* (México: Universidad Nacional Autónoma de México, 2006), p. 190-194.

196 See MORENO CATENA, Víctor, "La garantía de los derechos fundamentales…", loc. cit., p. 53.

197 See DÍAZ CABIALE, José Antonio and MARTÍN MORALES, Ricardo, *La garantía constitucional de la inadmisión de la prueba ilícitamente obtenida* (Madrid: Civitas, 2001), p. 22.

from it that will be disregarded as the "fruits of a poisonous tree".[198] Nevertheless, at least in Spain, beginning with judgment 81/1998 of the Constitutional Court, in order to follow this concept, there should be a connection of "anti-legality" between the original illicit evidence and the following.[199]

Such a limitation of liberty of evidence exists as a consequence of the application of Rule of Law, as in parallel to the function of *ius puniendi,* the state shall guarantee the fundamental rights of persons that are subject to trial.

Therefore, information that can be used in the future as evidence, has to be processed according to legal requirements and without violation of human rights. It is applied both to information processing at both national and transnational level.

Having said that, as a continuation it has to be said that despite the establishment of "proof of guilt", international instruments do not go into details of what is considered illegal or illicit evidence, leaving it to the national legislation of each country. In this manner, although the due process is guaranteed by every state that follows Rule of Law, and within the EU "All EU Member States have their own rules of evidence, governing fact-finding in criminal trials."[200]

Although the topic of licit evidence is directly related to the correct application of Article 6 of ECHR,[201] the latter does not regulate the admissibility of evidence or their evidential value.[202] ECtHR in its case law keeps silence about what has to be treated as illicit evidence and what consequences it can have on the process, precisely because evidential process is primarily regulated by domestic law.[203] And as Gless points out, "ECHR very often lacks an answer as to whether a certain piece of evidence – collected legally or illegally – in one country – may be admitted in a court in another country."[204]

---

[198] See MORENO CATENA, Víctor, "La garantía de los derechos fundamentales…", loc. cit., p. 146; LÓPEZ ORTEGA, Juan José. "Los principios constitucionales del proceso...", loc. cit., p. 146.

[199] GÓMEZ AMIGO, Luis and BLANCO SANTOS, Gemma, *Fuentes de prueba y nuevas formas de criminalidad* (Almería: Universidad de Almería. Servicio de Publicaciones, 2001), p. 64.

[200] GLESS, Sabine, "Mutual recognition, judicial inquiries, due process and fundamental rights", in VERVAELE, John A. E., *European Evidence Warrant. Transnational Judicial Inquiries in the EU* (Antwerpen: Intersentia, 2005), p. 124.

[201] See MILIONE, Ciro, *El Derecho a la tutela judicial efectiva en al jurisprudencia del tribunal Europeo de Derechos Humanos* (Valencia: Tirant lo blanch, 2015), p. 154.

[202] See LÓPEZ ORTEGA, Juan José, "Prueba y Proceso Equitativo. Aspectos actuales en la jurisprudencia del Tribunal Europeo de Derecho Humanos" in *Derechos y Libertades: revista del Instituto Bartolomé de las Casas*, 1993, I (2), p. 599; ECtHR, *Schenk v. Switzerland* [1988], paragraph 46.

[203] See MILIONE, Ciro, *El Derecho a la tutela judicial...,* op. cit., p. 154.

[204] GLESS, Sabine, *Mutual recognition, judicial...,* op. cit., p. 125.

The position of the ECtHR in relation to the evidential process is expressed in the judgment of a case *Kostovski v. The Netherlands*, "The admissibility of evidence is primarily a matter for regulation by national law [...] as a general rule it is for the national courts to assess the evidence before them."

Going back to the topic of the thesis, the following conclusion has to be made: as at some stage in the process, information exchanged can become evidence, it has to be processed according to legal requirements and respect for fundamental rights. As among all fundamental rights, the right to privacy and the right to data protection are the most exposed to be violated during information processing, they will be objects of further analysis.

3. Privacy

As mentioned, in order to use exchanged information as evidence, it has to be processed with respect for fundamental rights. The biggest risk in this respect is to privacy.

It is established in all international charters and declarations on fundamental rights, dating from the Universal Declaration of Human Rights of 1948[205] to the more recent Charter of 2000, which, along with the entrance into force of the Treaty of Lisbon in 2009, was granted the same legal values as those accorded to Treaties.[206]

3.1. Content of the right to privacy

According to international conventions, privacy is understood as the respect for private and family life, home and correspondence, respect for dignity, personal integrity or reputation. It derives from an understanding, developed at the end of XIX century,[207] that everyone has a right to share or not information about his/her private life, habits, acts, and relationships with others,[208] freedom from intrusion

[205] The same year, a right to privacy was established in the American Declaration of the Rights and Duties of Man.

[206] Article 6 of the TEU.

[207] Although some notions of privacy can be found earlier, but its full explanation was given by Samuel Warren and Louis Brandeis in 1890 in the article "The Right to Privacy" in *Harvard Law Review*, 1890, vol.4 no. 5, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

[208] GLANCY, Dotorhy J., "The invention of the right to privacy" in *Arizona Law Review*, 1979, vol. 21(1), p. 2.

and privacy of information,[209] and the right to know about and dispose of his/her personal data[210].

Santolaya and Lezertua defend that right to privacy as being equal to the right to intimacy established in Article 18 of the Spanish Constitution,[211] although other authors, for example del Castillo Vázquez, Murillo de la Cueva and Nogueira Alcalá defend that all intimate data is private data, but that not all private data is intimate.[212]

The Spanish Constitutional Court interprets personal and family intimacy as a personal area reserved from actions and knowledge of the rest,[213] or from those that fall outside of the area of trust of the person concerned and also covers some aspects of other people's lives. [214]

López Ortega states that due to technological developments, the right to privacy acquires new characteristics and nowadays, one of its varieties is informative privacy. If previously privacy was more understood as a person's right to decide to share or not to share information, and he or she could control it, with automated processing of information this control is lost, and privacy needs other measures of protection that prohibit the use of facilitated information.[215] This right derived from privacy is also known as the right to informative self-determination.[216]

Together with scientific developments, the right to privacy has given rise to the right to genetic privacy that has developed with the greater use of DNA, and the

[209] KINGSTON, Paul, "Personal information and Privacy" in HEFFERNAN, Liz, *Human Rights. A European Perspective* (Portland: The Round Hall Press, 1994), p. 155.

[210] GUTIÉRREZ ZARZA, Ángeles, "Conceptos básicos. Marco legal europeo sobre protección de datos en materia penal" in GUTIÉRREZ ZARZA, Ángeles, *Nuevas tecnologías, protección de datos personales y proceso penal* (Madrid: La Ley, 2012), p. 81.

[211] See SANTOLAYA, Pablo, "El derecho a la vida privada y familiar" in GARCÍA ROCA, Javier and SANTOYALA, Pablo, *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos* (Madrid: Centro de Estudios Políticos y Constitucionales, 2014, 3rd ed.), p. 430; DEL CASTILLO VÁZQUEZ, Isabel-Cecilia, *Protección de datos: cuestiones constitucionales y administrativas (el derecho a saber y la obligación de callar)* (Madrid: Civitas, 2007), p. 224.

[212] See DEL CASTILLO VÁZQUEZ, Isabel-Cecilia. *Protección de datos…,* op. cit., p. 224-225.

[213] See for example the sentence of the Spanish Constitutional Court 231/1988, paragraphs 3 and 4 of the legal basis.

[214] See ÁLVAREZ CARO, María, *Derecho al olvido en Internet: el Nuevo paradigm de la privacidad en la era digital* (Madrid: Universidad San Pablo, 2015), p. 43.

[215] LÓPEZ ORTEGA, Juan José, "La tutela de la intimidad genética en la investigación penal. A propósito de la STC 199/2013 y de la SAP Sevilla 650/2013" in CASADO, María and GUILLÉN, Margarita, *ADN forence: problemas éticos y jurídicos* (Barcelona: Universitat de Barcelona, 2014), p. 100-101.

[216] See SERRANO MAÍLLO, María Isabel, "Derecho al honor, a la intimidad y a la propia imagen" in SÁNCHEZ GONZÁLEZ, Santiago, *Dogmática y práctica de los derechos fundamentales* (Valencia, Tirant lo Blanch, 2006), p. 225-228.

need to give a data subject the right to determine conditions to access his or her genetic information.[217]

Ultimately, it is also interpreted as the right to be alone[218] and even the "right to be forgotten" and has a tendency to develop into a separate right.[219] The last point has witnessed an interesting development in case law of the European Courts of Justice. In its judgment in case C-131/12, where Google Spain SL and Google Inc. Were recognised as data controllers and as such responsible for data processing, although they are search engines and not databases. The Court's reasoning was the following: "The operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information, and does not distinguish between the latter and the personal data."[220] And, "it is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d)."[221]

Very recently, on 15th October 2015, the Spanish Supreme Court reiterated this judgment by saying that a publisher is responsible for the quality of information and has possibilities to eliminate it from search codes by using relevant protocols.

It declared that if data respects quality criteria, a publisher alone does not have an obligation to delete it, as it would mean a disproportionate limitation of liberty of information. Nevertheless, once the data subject asks for deletion, after reasonable time, the "right to be forgotten" has to be ensured, except in cases where data is of historic or public interest. [222]

---

[217] See ETXEBERRIA GURIDI, José Francisco, *Los análisis de ADN y su aplicación al proceso penal* (Granada: Comares, 2000), p. 61, 190; ETXEBERRÍA GURIDI, José Francisco, "La protección de los datos de ADN en la Unión Europea y en España", in CABEZUDO BAJO, María José. *Las bases de datos policiales de ADN ¿Son una herramienta realmente eficaz en la lucha contra la criminalidad grave nacional y transfornteriza?* (Madrid: Dykinson, S.L., 2013), p. 100.

[218] LÓPEZ ORTEGA, Juan José. "La tutela de la intimidad genética…", loc. cit., p. 100-101. WARREN, Samuel and BRANDEIS, Louis, "The Right to Privacy", loc. cit.

[219] See ÁLVAREZ CARO, María, *Derecho al olvido en Internet…,* op. cit., p. 72.

[220] Judgment of Court of Justice in *Google Spain SL, Google Inc. v Agencia Española de Protección de datos (AEPD), Mario Costeja Conzález*, C-131/12, ECLI:EU:C:2014:317, paragraph 28.

[221] Ibid, paragraph 33.

[222] Judgment of the Spanish Supreme Court of 15 October 2015 in case 545/2015.

Together with scientific developments, right to privacy had given the raise to right to genetic privacy that has developed with the greater use of DNA and the need to give a data subject the right to determine condition to access his or her genetic information.[223]

At European level, the right to privacy is established in the ECHR (that was opened to signature on 4th November 1950 and has been in force since 3rd September 1953) and since the Treaty of Lisbon also in the TEU, the TFEU and the EU Charter.

The ECHR in Article 8 envisages that "everyone has the right to respect for his private and family life, his home and his correspondence."

Even if the right to privacy is not directly written down, it derives from this provision, in particularly from the "private right", which, according to the ECtHR, "must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life".[224]

In the case of *Niemietz v Germany,* it also included the concept of labour environment[225] into the right to private life, and in the case *Perry v the United Kingdom,* the ECtHR declared that the use of cameras in public places for any purpose other than monitoring, is interference in privacy as well, and in this precise case, "There is no indication that the applicant had any expectation that footage was being taken of him within the police station, for use in a video identification procedure and, potentially, as evidence prejudicial to his defence at trial. This ploy adopted by the police went beyond the normal or expected use of this type of camera."[226]

3.2. Limitation of right of privacy

Right to privacy is not absolute right and Article 8(2) of the ECHR foresees the possibility of its restriction that according to Soleto Muñoz are quite wide and

[223] See ETXEBERRÍA GURIDI, José Francisco. *Los análisis de ADN…*, op. cit., p. 61, 190; ETXEBERRIA GURIDI, José Francisco, "La protección de los datos de ADN…", loc. cit., p. 100.
[224] ECtHR, *Amann v Switzerland* [2000], paragraph 65; *Rotaru v Romania* [2000], paragraph 43.
[225] ECtHR, *Niemetz v Germany* [1992], paragraph 29.
[226] ECtHR, *Perry v the United Kingdom* [2003], paragraph 41.

flexible. [227] It allows some level of national assessment to the fundamental right and legal establishment of its limitation according to national reality.[228]

In any case, according to Article 8(2) of the ECHR, restriction is possible only in cases where all three conditions listed below are fulfilled:

a) Restriction is established by law which is accessible to society, foreseeable229 and "formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[230]

b) It is established for the any of the following purposes:

- National security;
- Public safety;
- Economic well-being of the country;
- Prevention of disorder or crime;
- Protection of health or morals;
- Protection of the rights and freedoms of others.[231]

c) It is necessary for democratic society. Such necessity is measured by the principle of proportionality that includes:

- Necessity of restrictive measure in order to obtain the aim established by the law;
- Adequacy;
- "Cost-benefit" balance, i.e. The proportionality of the measure to the aim.[232]

From the ECtHR decision in the case of Peruzzo and Martens v Germany, a conclusion can be made that the law shall establish "appropriate safeguards against the blanket and indiscriminate taking and retention of DNA samples and profiles and adequate guarantees of the effective protection of retained personal data from misuse and abuse."[233]

---

[227] See SOLETO MUÑOZ, Helena, "Parámetros europeos de limitación de Derechos Fundamentales en el uso de datos de ADN en el proceso penal", article submitted for publication.

[228] See SANTOLAYA, Pablo, "Limitación de la aplicación de las restricciones de derechos. Art. 18 CEDH", in GARCÍA ROCA, Javier and SANTOLAYA, Pablo, *La Europa de los Derechos. El Convenio…*, op. cit., p. 658.

[229] See ECtHR, *Amann v Switzerland* [2000], paragraph 55.

[230] ECtHR, *Sunday Times v United Kingdom* [1979], paragraph 49.

[231] ECHR, Article 8(2).

[232] See ARENAS RAMIRO, Mónica, *El Derecho Fundamental a la protección de datos personales en Europa* (Valencia: Tirant lo Blanch, 2000), p. 121.

[233] ECtHR, *Peruzzo and Martens v. Germany* [2013].

In addition to the mentioned elements of the principle of proportionality, Gimeno Sendra adds necessity and motivation in each case of limitation of fundamental right.[234]

If the restriction does not meet any of these conditions, it becomes a violation of the right established in Article 8 of the ECHR.

Article 18 of the ECHR also entails that limitations can be applied only for the purpose that they have been established and their use for any other purpose will be treated as a violation.

In relation to limitation by law, such a limitation has to be very precise, for example the ECtHR recognised violation of Article 8 in the case of the French authorities which bugged a private flat because it had been out of the scope of the Criminal Procedure Code that only regulates the interception of telephone lines.[235]

In the case S and Marper v. The United Kingdom, the ECHR reiterated its previous judgments stating that the law shall have "clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness"[236] because it was "worded in rather general terms and may give rise to extensive interpretation."[237]

Article 7 of the EU Charter establishes the privacy of private and family life, home and communications without going into any details about its possible limitation, as Article 52(1) envisages possible restrictions on all rights that are not indicated in the Charter as absolute ones. Article 52(1) lays down the following requirements for limitation:

- Foreseen by law;
- Maintaining respect to the essence of the rights under consideration,
- Proportional;
- Protecting general interest or rights of others.

Thus compared with the ECHR, the Charter entails that in any case, the essence of right has to be maintained.

[234] See GIMENO SENDRA, Vicente, *Manual de Derecho Procesal..,* op. cit., p. 46.
[235] See ECtHR, *Vetter v. France* [2005], paragraphs 23, 24.
[236] ECHR, *S and Marper v. the United Kingdom* [2008], paragraph 99.
[237] Ibid.

The European Court of Justice pronounced that limitations are acceptable "as long as these limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union, or the need to protect the rights and freedoms of others."[238]

Regarding the balance between the well-being of a country and some aspects of privacy, Joined Cases C-465/00, C-138/01 and C-139/01 deserve some attention. In these cases the European Court of Justice recognised that information relating to salaries (including identification of persons), gathered by the public entity in order to ensure non-discrimination in salaries and appropriate use of public funds, falls within its scope and makes a justified element of the limitation of the right to privacy (although at the same time, necessity and proportionality also have to be taken into account).[239]

3.3. Privacy and electronic communications

Protection of privacy was directly established by the Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector[240] (hereinafter – Directive 2002/58/EC). On the one hand, Article 1 excludes from its scope activities related to public security and criminal law, but on the other hand, Article 15 allows the limitation of rights and obligations established by this Directive for the same purposes. The European Court of Justice in Case C-275/06 explained that it neither eliminates the possibility nor obliges the disclose of such data in civil processes,[241] but foresees that while transposing Directive 2002/58/EC, "Member States take care to rely on an interpretation [...] which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order."[242]

The Directive 2002/58/EC was amended by the Directive 2006/24/EC of the European Parliament and of the Council of 15th March 2006, on the retention of data generated or processed in connection with the provision of publicly available

[238] Judgment of the Court of Justice in *Volker und Markus Schecke GbR and Hartmut Eifert,* C-92/09 and C-93/09, ECLI:EU:C:2010:662, paragraph 50.

[239] See judgment of the Court of Justice in *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk*, C-465/00, C-138/01 and C-139/01, ECLI:EU:C:2003:294, paragraph 81.

[240] OJ L 201, 31.07.2002, p. 37-47.

[241] This precise case was about the infringement of rights to intellectual property.

[242] Judgment of Court of Justice in *Productores de Música de España (Promusicae) v Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54, paragraphs 54, 55 and ruling.

electronic communication services, or of public communication networks and amending Directive 2002/58/EC (hereinafter – Directive 2006/24/EC).

New legislation foresaw an obligation on the part of providers of communication networks and services to retain some categories of data, and to make it available for detection, investigation and prosecution of serious crimes. That meant storing data of every user despite its potential relationship or not with serious crime. The data retained[243] is data related to communication that allows identifying a person with whom communication took place, its time and location, but not its content or the information consulted.

As stated by the European Court of Justice, this data "taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[244]

Interpreting Article 52(1) of the EU Charter (possible limitation of fundamental rights), the Court came to the conclusion that as the content of the communications is not revealed, the essence of the right to privacy is not affected,[245] and as it is for the purpose of combatting serious crime, the interference is for general interest.[246]

But with respect to proportionality (understood as not exceeding the limits of appropriate and necessary interference), data retention was found to be a "valuable tool for crime investigation" and therefore an appropriate tool, but the question of necessity was raised as "Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a

[243] Data categories listed in Article 5 include: data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. See judgment of Court of Justice in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraphs 26.

[244] Ibid, paragraph 27.

[245] Ibid, paragraph 39.

[246] Ibid, paragraph 41, 44.

specific obligation on Member States to establish such rules has also not been laid down."[247]

On this basis, the Directive 2006/24/EC was recognised as a disproportionate measure and invalid as a whole. It was declared invalid without any temporary continuation of its application.

As is the case with every directive, Directive 2006/24/EC had to be transposed into national law and the term for that came to an end on 15th September 2007. That meant that between September 2007 and April 2012, according to Article 258 of the TFEU, the Commission was able to start infringement procedure for Member States that had not obeyed the obligation of the transposition. In effect such procedure had been started against Germany, but withdrawn due to the recognition of the directive as void. But in case of Sweden, the consequences were more serious as in 2010, the European Court of Justice had recognised Sweden's failure to carry out the transposition[248], and in 2013 ordered a lump sum payment of 3 million euros to be made.[249] After the judgment declaring the directive void, this fine was returned to Sweden.

The High Courts of Bulgaria, Cyprus, the Czech Republic, Germany and Romania have recognised the transposition laws of Directive 2006/24/EC in total (Romania[250]), or partially void (Bulgaria, Cyprus, Czech Republic, Germany).[251]They did not mention anything about the validity of the Directive, as they do not have jurisdiction to pronounce over EU law. But being in the same position, the courts of Ireland and Austria asked the European Court of Justice for a preliminary ruling in this respect.[252]

As a result of the judgment of the European Court of Justice, Constitutional Courts of Austria, Slovenia and Romania[253] declared national transposing laws void.

From these examples a few conclusions should be made:

---

[247] Ibid, paragraph 66.

[248] See judgment of Court of Justice in *European Commission v Kingdom of Sweden*, 185/09, ECLI:EU:C:2010:59.

[249] Judgment of Court of Justice in *European Commission v Kingdom of Sweden*. C-270/11, ECLI:EU:C:2013:339.

[250] See BOEHM, Franziska and COLE, Mark D., "Data Retention after the Judgement of the Court of Justice of the European Union" (study, Greens/EFA Group in the European Parliament, 2014), p. 16, accessed September 17 2014, http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf.

[251] Ibid, p. 15-18.

[252] In the case of Austria, actions before national courts were brought by more than 11 000 applicants. See judgment of Court of Justice in *Digital Rights Ireland Ltd...,* loc. cit., paragraph 19.

[253] After declaring the law void in 2009, a new one was adopted in 2012 and in 2014 also declared void.

- In the case of the infringement started against Sweden, the European Court of Justice took a technical decision, revising only the question of transposition of the Directive 2006/24/EC, but not its content.
- The courts of only two of the 27 Member States addressed this issue to the European Court of Justice, questioning the content and compatibility of the directive with human rights. The rest of the countries in the worst-case scenario transposed it automatically, and in the best-case scenario their high courts recognised transposing provisions as void. Thus Member States swear by the legality of European legislation.

Despite negative experience, electronic communication is so complex and overwhelming that it has to be compensated by appropriate procedural regulation to have benefits for investigation.[254]

4. Data protection

4.1. Relation between right to privacy and right to data protection

Although privacy and data protection are closely interrelated, their content is quite different.

It would be hard to find a better explanation of the interrelation between privacy and data protection than one provided by the European Data Protection Supervisor, "'Data protection' is broader than 'privacy protection' because it also concerns other fundamental rights and freedoms, and all kinds of data regardless of their relationship with privacy, and at the same time, more limited because it merely concerns the processing of personal information, with other aspects of privacy protection being disregarded."[255]

Thus the right to privacy protects persons against disclosure of personal information, and establishes some exceptions when they are allowed. Data

[254] See VALLÉS CAUSADA, Luís Manuel, "Usos delictivos no comunicativos...", loc. cit., p. 228.

[255] HUSTINX, Peter, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation" (article based on the course given at the European University Institute's Academy of European Law in July 2013), p. 5, accessed January 20, 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf. Similar explanation is given by KOKOTT and SOBOTTA, "The distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR", in *International Data Privacy Law*, 2013, vol. 3, no 4, p. 225, http://idpl.oxfordjournals.org/content/3/4/222.full.pdf+html as well as by GARRIGA DOMÍNGUEZ. See GARRIGA DOMÍNGUEZ, Ana, *Tratamiento de datos personales y Derechos Fundamentales* (Madrid: Dykinson, 2009, 2nd ed.), p. 24.

protection establishes rules for the use of all types of data, including the one already disclosed under the exception of privacy, or with the consent of the data subject.

The Spanish Constitutional Court defines data protection as a fundamental right to agree that a person's data would be collected, obtained, accessed and recently processed by the State or person.[256]

Looking at the content of the right to a private life and the right to data protection, the last one is not the only right to be defended, but also the right to demand certain action from others.[257] It includes not only the right not to disclose personal data, but also the right to be informed about its use, the right to access to such data and the right to correct or delete it.

Countries, as parties to numerous conventions, normally have developed both legislation protecting privacy and regulating data protection with special regulations in exceptional areas, such as the limitation of privacy for public security purposes, medical reasons, and so on.

At the beginning, the right to data protection was understood as an element of the protection of private life[258] and as a separate concept, was developed in the mid-sixties of the XX century as a consequence of the development of information processing technology.

The first laws on data protection are dated in the early seventies with the first law adopted by the German State of Hessen in 1971 and followed by the first state-wide law, adopted by the Swedish Parliament in 1972.

4.2. Origins and development of right to data protection

As already mentioned, data protection (also called *habeas data* or informative self-determination)[259] as an independent right started to develop in the United States in the sixties and in Europe, in the seventies. That is the reason why it is not included as a separate right in the ECHR.

Although the ECHR has a static nature, the ECtHR (and previously the European Commission of Human Rights) interprets its provision according to the current

[256] Judgment of the Spanish Constitutional Tribunal 292/2000.
[257] See ARENAS RAMIRO, Mónica, *El Derecho Fundamental a la protección*..., op. cit., p. 96.
[258] See REBOLLO DELGADO, Lucrecio, *Vida privada y protección de datos en la Unión Europea* (Madrid: Dykinson S.L., 2008), p. 55-56, 223.
[259] See DEL CASTILLO VÁZQUEZ, Isabel-Cecilia, *Protección de datos: cuestiones constitucionales...*, op. cit., p. 75.

social reality in a "progressive, evolutionary and teleological way, considering it as a "living instrument" that must be analysed according to the actual conditions".[260]

Within the context of the interpretation of the right to protection of private rights, data protection issues began to be addressed. For the first time, data protection was concerned in the case *X v the United Kingdom* in 1982. It was not mentioned directly as such, but with a reference to the need for protection of private life in relation to the development of new technologies. For the first time, data protection was recognized as a part of the right to private life in 1987 in the Judgment *Leander v Sweden*.[261]

Seeking to establish data protection rights as individual rights, the Committee of Ministers did not choose the possibility of signing additional protocol to the ECHR, but opted for an individual convention, despite close links of this right with the right of protection of private and family life.[262]

Thus with the technical developments and increased processing personal data, the Committee of Ministers recognised the necessity of its regulation and on 28th January 1981, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter – Data Protection Convention) was opened for signature and came into force on 1st October 1985.

Though the Data Protection Convention does not explicitly exclude the processing of data by the police, in 1983 the Committee of Ministers established a working party to elaborate specific recommendations for the police on use of personal data. The Committee of Ministers finally adopted them on 17th September 1987 as Recommendation No. R (87) 15 of the Committee of Ministers to Member States, regulating the use of personal data in the police sector (hereinafter – Recommendation R (87)15).[263]

Within the European Communities, the process of regulation of data protection can be defined as bottom-up, because firstly, it was regulated by the secondary law and in primary law it was just mentioned. It was included in the Charter in 2000, but as all rights became obliged to respect only with the entrance into force of the Treaty of Lisbon in 2009 that, as already mentioned, equalized its status to that of a Treaty.

---

[260] THE LISBON NETWORK, "The Right to a Fair Trial: Analysis of the Condemnations of the Portuguese State due to the Violation of Article 6 of the European Convention on Human Rights", Council of Europe, 2008, accessed October 30, 2014, http://www.coe.int/t/dghl/cooperation/lisbonnetwork/Themis/ECHR/Paper4_en.asp.

[261] ECtHR, *Leander v Sweden* [1987].

[262] See DEL CASTILLO VÁZQUEZ, Isabel-Cecilia, *Protección de datos: cuestiones…*, op. cit., p. 87.

[263] "Data protection", Compilation of Council of Europe texts, accessed October 30, 2014, http://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf.

In this way data protection has been transformed from an element of harmonization of the single market regulated by the secondary law, into a fundamental right.[264]

Article 16 of the TFEU directly establishes the individual right to personal data protection and specifies that relevant EU level rules have to be approved and applied by the EU institutions and entities as well as by the Member States, while transferring such data and performing activities within the scope of EU law. It also includes institutional provision, establishing that the accomplishment of this regulation has to be controlled by independent authorities.

Article 8 of the EU Charter envisages that personal data can be processed only with the consent of the subject of the data or on the basis specifically established by the law and in any case it is possible only for specific purposes. The consent has to be explicit or tacit, reasonably concrete, given by a person with legal capacity, without pressure and with information relating to the consequences. [265] Equally, as in the case of privacy, some legal limitations of the right to data protection are possible according to Article 52(1). Thus, for example, in case C-291/12, the European Court of Justice explained that both the right to privacy and the right to data protection "are not absolute rights, but must be considered in relation to their function in society".[266] In the same judgment it was stated that taking both face images and fingerprints for the issuing of identity documents is proportional to the objective of preventing the falsification of passports, and does not mean bigger interference in the right to privacy and to data protection.[267]

Establishment of the fundamental right to data protection at EU level means an obligation to assess it (as any other fundamental right) before adopting any European legislation. For this purpose the Commission has elaborated "Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments."[268]

According to López Guerra, with the changes brought by the Treaty of Lisbon, rights established in the Charter became obligatory to call upon in the

[264] PARIENTE DE PRADA, Iñaki. "La reforma de la protección de datos en el ámbito europeo" in GOIZUETA VÉRTIZ, Juana; GONZÁLEZ MURUA, Ana Rosa and PARIENTE DE PRADA, Iñaki, *El Espacio de Libertad, Seguridad y Justicia: Schengen y Protección de Datos* (Navarra: Aranzadi, 2013), p. 127.

[265] See EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE, *Handbook on European Data Protection Law*, 2014, p. 56, accessed October 30, 2014, http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law

[266] Judgment of Court of Justice in *Michael Schwarz v Stadt Bochum*, C-291/12, ECLI:EU:C:2013:670, paragraph 33.

[267] Judgment of Court of Justice in *Michael Schwarz v Stadt…,* loc. cit., paragraph 41, 50.

[268] SEC(2011) 567 final.

implementation of EU Law and can be voluntary applicable in any area of national competence.[269]

The following subsections are dedicated to European legal instruments applicable to data processed by the police, and therefore they do not include the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter – Directive 95/46/EC) in which Article 3(2) foresees exclusion of areas of public security and activities related to criminal law.

4.3. European legal framework for right to data protection

4.3.1. European Convention on Data Protection (CETS 108)

The Data Protection Convention was the first obligatory data protection instrument establishing its basic principles, but on the other hand, it is criticised for being a legal basis with indirect application that needs further development at national level. [270]

Its Article 1 envisages that data protection is a warranty of respect for human rights and fundamental freedoms, including privacy. It goes in line with the previously quoted European Data Protection Supervisor that the scope of data protection is broader than privacy.

Article 2 entails the scope of the Data Protection Convention as "Automated personal data files and the automatic processing of personal data in the public and private sectors."[271] Implementing it at national level, the States' parties have the possibility:

- To limit this scope;
- To expand it to groups of persons, companies, etc. Despite the fact whether they have a status of legal person or not;
- To apply it to non-automated data processing.

[269] LÓPEZ GUERRA, Luís María, "Derechos e integración europea" in UGARTEMENDÍA ECEIZABARRENA, Juan Ignacio and JÁUREGUI BERECIATU, Gurutz, *Derecho Constitucional Europeo* (Valencia: Tirant lo Blanch, 2011), p. 24-25.

[270] GUASCH PORTAS, Vicente, *Las transferencias internacionales de datos en la normativa española y comunitaria* (Madrid, Agencia Española de Protección de Datos, Agencia Estatal Boletín Oficial del Estado, 2014), p. 25.

[271] "Details of Treaty No. 108", Council of Europe, accessed November 3, 2014, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

Article 5 foresees the main principles – the conditions for automated data processing:

- Accuracy – a controller must have reasonable certainty about data quality and reliability. For example in the case *Khelili v Switzerland* the ECtHR recognised that inclusion of the definition of "prostitute", only on the basis of deduction from information on a calling card[272], is not a sufficient background for its maintenance in the data base and "could damage Ms Khelili's reputation and make her day-to-day life more problematic, given that the data contained in the police records might be transferred to the authorities. That was all the more significant because personal data was currently subject to automatic processing, thus considerably facilitating access to, and the distribution of, such data."[273]
- Lawfulness –law (in a clear and comprehensive manner)[274] has to envisage data processing. It must be subject to necessity[275] and done for a legitimate aim (to protect the general interest or rights of others).[276]
- Specified and legitimate purposes – as explained in the Handbook on European Data Protection Law, "Every new purpose for processing data must have its own particular legal basis and cannot rely on the fact that the data were initially acquired or processed for another legitimate purpose."[277]
- Relevancy – amount of data and their categories have to be proportionate to their purposes, without including unnecessary data.
- Limited storage – only for the time that is necessary for the purpose for which it was collected. Additionally, data storage has to be proportional to the purpose for which it was collected and in any case there shall be time limit.[278]

[272] "Nice, pretty woman, late thirties, would like to meet a man to have a drink together or go out from time to time. Tel. no. …"

[273] ECtHR, *Khelili v Suisse* [2012], paragraph 63-64.

[274] ECtHR in case *Rotaru v. Romania* concluded that the law shall define the type of information, categories of peoples and circumstances that allows limitation. See ECtHR, *Rotaru v. Romania* [2000].

[275] In case *Leander v. Sweden* the ECtHR recognised proportionate secret check of persons to be employed in posts related to national security. See ECtHR, *Leander v. Sweden* [1987].

[276] In case *Peck v. the United Kingdom*, CCTV camera fixed an attempt to suicide and the police after rescuing of the applicant, passed video information to the media. That was recognised by the ECtHR as lack of legitimate aim and a need of person's consent was declared. See ECtHR, *Peck v. the United Kingdom* [2003].

[277] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, COUNCIL OF EUROPE, *Handbook on European Data…*, op. cit., p. 68.

[278] See ETXEBERRÍA GURIDI, José Francisco, "La protección de los datos de ADN…", loc. cit., p. 114.

- Fair processing – society, in reasonable terms, shall be provided with information about lawful and transparent data processing and with a copy of the file concerned.[279]
- Depersonalisation - when it is no longer required for the purposes that it was stored, and for proper data control.

A very important article is Article 6, which permits the processing of special data categories (racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sex life and criminal convictions), but only with safeguards established in national law.

Comparing the possibilities of derogations from the Data Protection Convention established in its Articles 5, 6 and 8 (a person's access to his or her data) and the limitation of the right to privacy, envisaged in Article 8(2) of the ECHR, some of the bases coincide and some are different.

Derogation from Article 5, 6 and 8 of the European Data Protection Convention	**Limitation of the right to privacy of the ECHR**
National security	
Public safety	
Protection of the rights and freedoms of others	
Economic well-being of the country	Monetary interests of the State
Prevention of disorder or crime	Suppression of criminal offences
Protection of health or morals	Protecting the data subject

Table 1: Derogations from the right to data protection according to the European Data Protection Convention and the ECHR.

As a result of this comparison, it can be said that the scope of limitations of data protection is more narrow than that of limitations of privacy; as in the case of data protection only monetary interests figure instead of the broad concept of economic well-being; and instead of the prevention of disorder or crime only the suppression of criminal offences.

Article 12 is very important in relation to the topic of this analysis; this article establishes, as a general rule, no limitation of cross-border information transmission between parties to the Data Protection Convention. Only two exceptions from this right are foreseen:

- When some categories of data are subject to specific protection by national law;
- In the case of onward transmission from a receiving party to a third state.

[279] See ECtHR, *K.H. and Others v. Slovakia*, [2009], paragraph 47.

Article 2 of the 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[280], establishes the possibility of data transfer to a third state only if it ensures satisfactory data protection level, and envisages the following exceptions of that rule: the interests of either the subject of the data or public interests; special arrangements between the data controller and the receiving authority on application of adequate data protection.

Article 3 of the Data Protection Convention does not directly envisage that it is applied to data automatically processed by police and judicial authorities, but on the other hand, it foresees its application both for private and public authorities. As no exception is established in respect to application for police and judicial authorities, it can be presumed that without a special declaration of derogation from the State Party, the Data Protection Convention will be applied to those authorities.[281]

4.3.2. Recommendation R (87)15

A working group consisting of experts from Belgium, France, Italy, the Netherlands, Portugal, Sweden, Switzerland and the United Kingdom elaborated the recommendations adopted on 17th September 1987 at the 410th meeting of the Ministers' Deputies as Recommendation R (87)15.

It established that, "The expression "for police purposes" covers all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order." Thus it also covers information processing and exchange.

Equally, as in Data Protection Convention, Recommendation R (87)15 foresees the possibility of extending the application of the Recommendation to non-automated data processing as well as to groups of persons, associations, and so on, despite having legal personality or not.

Recommendation R (87)15 established 8 principles of data protection:

[280] Opened for signature on 8th November 2001 and came into force on 1st July 2004. Not signed by Azerbaijan, Malta, San Marino and Slovenia. Not ratified yet by Belgium, Greece, Iceland, Italy, Norway, Russia, Turkey, the United Kingdom. See "Details of Treaty No. 108", loc. cit.

[281] Similar conclusion is made in the Explanatory Memorandum to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, Council of Europe, accessed October 13, 2014, https://wcd.coe.int/ViewDoc.jsp?Ref=ExpRec(87)15&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

- The Independent supervisory authority has to control data processing. Its consultation before introducing new automatic processing methods and notification about automated databases kept.
- Data can be collected only in order to prevent real danger or to suppress specific criminal offences and, as an exception, for other purposes foreseen by national law. Data collection on the basis of specific data (except when it is necessary for a particular inquiry) is prohibited, expect when it is indispensable for specific inquiry.
- Only accurate and necessary data has to be stored. While storing data, it has to be categorized by degree of reliability.
- It can be used exclusively for police purposes.
- Data can be transmitted to other police institutions only on the basis of a legitimate interest. Its transmission to other public bodies and private parties is subject to special conditions. International transmission is permitted only to police bodies and on the basis of national or international legal provisions or for the prevention of imminent danger or suppression of serious crime, and having reasoned request. Interconnection of data bases is allowed under provisions of national legislation in general, or permission of the supervisory body for a particular case.
- To provide public information about the existence of data bases and the right to access, rectification and appeal.
- The storage period cannot be longer than is necessary for the purpose for which the data was stored.
- Proper secure measures of access, storage, communication and other processing shall be applied.

It reiterates some principles of the Data Protection Convention (such as definition of personal data, principle of data quality, use of special categories of data, data subject right to access, etc.) As it was thought that those members of the Council of Europe that had not ratified the Convention could be interested in joining and implementing this Recommendation.[282] Currently, the only such country is Turkey, but at the moment of the adoption of Recommendations Data Protection Convention, it was in force only in France, Germany, Norway, Spain, Sweden and very close to entry into force in the United Kingdom.[283]

On the other hand, being *soft law,*[284] Recommendation R(87)15 established a more ambitious data protection system, going beyond the European Convention on Data

[282] See GUTIÉRREZ ZARZA, Ángeles, "Conceptos básicos. Marco…", loc. cit., p. 78.
[283] See "Details of Treaty No. 108", loc. cit.
[284] LÓPEZ GUERRA describes "soft law" as international instruments that multilaterally are not binding, but in which parties express wishes or proposals how to regulate certain issues in the

Protection and already being established in 87 supervising authorities that was only introduced to the Convention with the Additional protocol in 2001.

Although, as mentioned, Recommendation R(87)15 is *soft law*, ECtHR gives it *ratio decidendi* in the case *S. And Marper v the United Kingdom* and states that principles foreseen in the European Convention on Data Protection and Recommendation R(87)15 are "core" and have to be "Consistently applied by the Contracting States in the police sector."[285]

4.3.3. Council Framework Decision 2008/977/JAI

Although police and judicial co-operation, including information exchange in the EU, can be counted for a few decades, general data protection rules in this area were approved only in 2008, as Framework Decision 2008/977/JAI.

As pointed out by Gutiérrez Zarza, the importance of this legislative act is great as , "no other rules are limiting the powers of law enforcement authorities to ensure the protection of the fundamental rights of the individuals concerned by the access, processing, exchange [...] of police information."[286]

4.3.3.1. Scope of application

It received a lot of criticism due to being very watered down, with a limited application and leaving a patch system because at the very beginning of the text, in its recital 39, it is recognised that it shall not affect data protection provisions of the European Police Office, Eurojust, the Schengen Information System, Customs Information System and information exchange under Council Decision 2008/615/JHA of 23rd June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (hereinafter –Decision 2008/615/JHA) and some other instruments. It is declared that the above mentioned instruments have completed a coherent set of rules on data protection.

At the same time, data protection rules for other co-operation mechanisms are considered as not exhausted and can be applied only when they establish more restrictive rules than the Framework Decision 2008/977/JHA.[287]

---

future. See LÓPEZ GUERRA, Luis, "*Soft law* y sus efectos en el ámbito del Derecho Europeo de los Derechos Humanos", in *Teoría y derecho. Revista de pensamiento jurídico*, 2012, 11, p. 151.

[285] ECtHR, *S and Marper v United Kingdom* [2008], para 107. See LÓPEZ GUERRA, Luis, "*Soft law* y sus efectos…", loc. cit., p. 157-158.

[286] GUTIÉRREZ ZARZA, Ángeles, *Exchange of Information and Data Protection in Cross-Border Criminal Proceedings in Europe* (Berlin: Springer, 2015), p. 158.

[287] See recital 40 of the Framework Decision 2008/977/JAI.

One more exception is found in Article 1(4) where it is stated that it does not interfere in cases related to national security.

As stated by O'Neill, "Council Framework Decision 2008/977/JHA appears to give a unitary response to the issue of data protection for EU law enforcement activities, but its provisions are subject to so many exceptions that the question does arise as to its actual applicability."[288]

Besides, the Council of the European Union has decided that it will be applied only to cross-border information exchange (between the Member States, Member States and EU authorities or information systems), but not to information exchange between competent authorities within one Member State. On the one hand, it allows application within Member States at a higher level of data protection (where it exists), but does not require raising it where the safeguards are lower.

As pointed out by Oubiña Barbolla, it gives double vision on the same data depending on its national or cross-border processing, and complicates the work of law enforcement officers who have to be always aware of which data protection rules have to be applied and makes protection weaker.[289]

4.3.3.2. Principles applied to data protection

Article 3(1) of the Framework Decision 2008/977/JHA establishes principles of lawfulness, proportionality and purpose for information transmission and processing, saying that, "Personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected."[290] But as Etxeberría Guridi noticed, no criteria to measure proportionality are included.[291]

Thus, on the one hand, it envisages a strong relationship between data collection and processing, but on the other hand. Article 3(2) foresees very flexible deviation from this general rule by permitting its processing to any purpose that is not incompatible with the original one, its proportional and competent authority is

[288] O'NEILL, Maria, *The Issue of Data Protection and Data...,* op. cit., p. 218.

[289] See OUBIÑA BARBOLLA, Sabela, "Cambio de enfoque en la cooperación judicial penal y policial en la UE en relación con la transmisión de datos personales: las nuevas propuestas normativas y la STJUE de 8 de abril de 2014", in COLOMER HERNÁNDEZ, Ignacio, OUBIÑA BARBOLLA, Sabela, *La transmisión de datos personales…,* op. cit. p. 83.

[290] OJ L 350, 30.12.2008, p. 65.

[291] ETXEBERRÍA GURIDI, José Francisco, "Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo" in *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, 2009, no 23, p. 365.

authorised by the law.[292] Article 11 specifies three circumstances of further processing[293] of data, and foresees the fourth one as open to any other purposes, but with the requirement of the prior consent of the transmitting party or the subject of the . Article 12 establishes the obligation of the receiving Member State to follow restrictions on data processing that are established in the national law of the transmitting Member State, and about which it has previously been informed. On the other hand, the transmitting Member State cannot ask for restrictions that would not be applied to its national competent institutions. Here, we can find d indirect allusion to the principle of availability that can be interpreted as the right to process received data equally to the scope of processing that would be applied in the transmitting Member State. But in reality it goes far beyond the principle of information availability that establishes equal access to information, but not its transmission.

Thus exceptions that seem to be very limited finally convert into almost infinite possibilities of data transmission and, as noticed by Oubiña Barbolla, totally disrespect principles of purpose.[294]

Quoted Article 3(1) enters, to some extent, into contradiction with Article 1 as it foresees the application of principles for information collection and not only its transmission and further processing. Principles established in Article 3(1) could be for information that is collected for transmission to other Member States. But what if it has been collected for national use and then, just by coincidence, another Member States asks for it? In this case, collection for internal purposes falls out of the scope of the Framework Decision 2008/977/JHA according to its Article 1. Thus application of the principles of the Article 3 should be more precise, making emphasis on the collection of personal data with the purpose of its transmission.

4.3.3.3. Regulation of data storage

Regulation of data storage is very diluted as in Article 5, a general rule of "appropriate time limits" is established; this indeed does not provide any clarity or safeguard. In Article 9 a little more detail can be found:

[292] Data can be also used for historical, statistical and scientific purposes once it is depersonalised (made anonymous).

[293] "1. The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which they were transmitted or made available;
2. Other judicial and administrative proceedings directly related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
3. The prevention of an immediate and serious threat to public security."
OJ L 350, 30.12.2008, p. 67.

[294] See OUBIÑA BARBOLLA, Sabela. "Cambio de enfoque en la cooperación …", loc. cit., p. 87-88.

- The transmitting authority can indicate storage time, which can be extended by the receiving Member State if it is still needed for on-going investigation, prosecution or enforcement of criminal penalties.
- If the transmitting authority does not give any indication, data can be stored according to the national provisions of the receiving Member State.

With the last provision, European legislators seem to accept the refutable approach of the transmitting Member State, allowing that it does not indicate rules on personal data storage. The European law should not establish such provision that permits negligence in data transmission. What should be done is to impose an obligation on the transmitting Member State, to indicate storage and processing conditions and national provisions for the receiving Member State. The regulation of receiving Member State should be applied only when it foresees a shorter storage term. If such obligation would be a disproportionate burden to provide such information with every data transmission, a handbook with relevant data relating to all Member States could be drafted.

4.3.3.4. Special categories of data and onwards data transmission

Another watered down provision of Framework Decision 2008/977/JHA is the related processing of special categories of data[295] that, according to Article 6, is allowed when it is strictly necessary and with adequate safeguards of national law. It would be understandable, to some extent, if Framework Decision 2008/977/JHA would be applicable to Europol instead of its own data protection regulation and the legislator would like to maintain already applicable provision on the possibility of including sensitive data into analysis work files. But as mentioned in subsection 5.3 of the Chapter II, Framework Decision 2008/977/JHA is not applicable to Europol. In these circumstances, such a provision in *lex generalis* of data protection raises a lot doubts. Besides, both expressions "strictly necessary" and "adequate safeguards" ideally need to be more precise and descriptive as data concerned can be the background for violation of the fundamental right of non-discrimination, and effectively mean the breach of the principle of legality.[296] Besides, in Europol's regulation of sensitive data, its processing is allowed only in indispensable cases and with a previous existence of other data on that person in the AWF, i. E. It is forbidden to start collecting special data without having previously collected general data.

[295] Racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and the processing of data concerning health or sex life.

[296] See EUROPEAN ASSOCIATION FOR THE DEFENSE OF HUMAN RIGHTS AND EUROPEAN DIGITAL RIGHTS, "Report on Privacy and Personal Data Protection in the European Union", December 2009, p. 10, accessed October 13, 2014, http://www.ldh-france.org/IMG/pdf/legislation_Europeenne.pdf.

Council Framework Decision 2008/977/JHA also allows controversially treated onwards data transfer to third states, or to international bodies and to private parties. On the one hand, the fact that this issue is not left without regulation can be valued positively; but then the question about necessity arises. As will be explained later, onward data transmission is permitted within the framework of Europol, i.e. Europol can transmit information received from Member State onward to third parties. Transmission is restricted only to third parties with whom Europol has an operation agreement that allows personal data exchange and establishes at least basic data protection warranties.[297] Thus the question stands whether it is really indispensable to allow broader data transmission outside the EU. Of course it makes sense in other areas to which Directive 95/46/EC is applied.[298] Leaving aside this question, Article 13 of the Council Framework Decision 2008/977/JAI establishes 4 conditions for onward data transmission:

a) Purpose limitations – equal to general purpose of this legislative act, i.e. "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties."

b) Receiving authority is responsible for such a purpose;

c) Consent of Member State of data origin according to its law;[299]

d) Adequate level of data protection in the third party.

The notion of adequacy time was undefined for a long, but the Advocate General Yves Bot, in Case C-362/14 considered that, "Although the English word 'adequate' may be understood, from a linguistic viewpoint, as designating a level of protection that is just satisfactory or sufficient, and thus as having a different semantic scope from the French word 'adéquat' ('appropriate'), the only criterion that must guide the interpretation of that word is the objective of attaining a high level of protection of fundamental rights, as required by Directive 95/46. Examination of the level of protection afforded by a third country must focus on two fundamental

[297] See Subsection 2.2 of the Chapter IV.

[298] In this case, information can be transmitted to the State when a relevant decision on adequate data protection level is approved by the Commission. For the time being, the Commission has recognised the following states as having such an adequate data protection level: Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, United States of America, Uruguay and Switzerland. See GUASCH PORTAS, Vicente, *Las transferencias internacionales de...,* op. cit., p. 22, 81-84. This statement is not applied so much to the area of police and judicial co-operation as in general.

[299] Article 13(2) foresees an exception to this condition in cases "Essential for the prevention of an immediate and serious threat to public security of a Member State or a third State or to essential interests of a Member State and the prior consent cannot be obtained in good time".

elements, namely the content of the applicable rules and the means of ensuring compliance with those rules."[300]

Although this Case C-362/14 is based on Directive 95/46/EC and data transfer to the United States under the Commission Decision 2000/520/EC of 26th July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles, and related frequently asked questions issued by the US Department of Commerce[301] (hereinafter – Decision 2000/520/EC), it is also interesting in the context of this research because it reveals the position of the Advocate General and the European Court of Justice on "(un)limited" personal data use for law enforcement. Thus even as a general rule, safe harbour principles have to be applied to data transferred from the EU to the US for commercial purposes; national law has "primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them"[302] and therefore, entities that possess information are obliged to share it with intelligence and law enforcement institutions. Additionally, there are no effective supervisory mechanisms to ensure proper use of transferred information.

In these circumstances the Advocate General understands that such data transfers can cover "in a generalised manner, all persons and all means of electronic communication and all the data transferred, including the content of the communications, without any differentiation, limitation or exception according to the objective of general interest pursued"[303] and is totally contradictory to the right to privacy and right to data protection.

Going back to the Framework Decision 2008/977/JHA, closer analysis deserves exceptions from the requirement of the ensuring of an adequate level of data protection. Such exceptions refer to the national law of the data transmitting authority; national law; not to the law of the Member State where the data was obtained. Thus Article 13(3) establishes that if the third party does not have relevant data protection legislation, data can be transmitted if, according to the law of the transmitting Member State, it is necessary to protect the data subject's interests or public interests, and furthermore, that the receiving state provides data safeguards (but not stable legislation) which is acceptable by the transmitting

[300] Opinion of the Advocate General in *Maximillian Schrems v Data Protection Commissioner,* C-362/14, ECLI:EU:C:2015:627, paragraphs 142, 143.
[301] OJ L 215, 25.08.2000, p. 7-47.
[302] Judgment of the Court of Justice in *Maximillian Schrems v Data Protection Commissioner,* C-362/14, ECLI:EU:C:2015:650, paragraph 86.
[303] Opinion of the Advocate General in *Maximillian Schrems v Data…,* loc. cit., paragraphs 198, 200.

Member State. It means that Member States where information was obtained would face the situation that their data will be transmitted to third parties without adequate levels of protection and with assessments made on the basis of the law of the transmitting one, will totally lose control of protection of data.[304] Such a regulation can be assumed to be redundant and lacking logic. It should be the Member State where data has originated which decides on the sufficiency of safeguards in the third party, and makes assessment according its national law.

Article 14 of the Framework Decision 2008/977/JHA foresees onward transmission to private parties, but does not specify whether they can be only within the transmitting Member State or outside as well.

Article 14(1)c(ii)-(iv) entails transmission of data to private bodies when necessary for crime prevention, investigation, prosecution or execution of criminal penalty, protection of public security from imminent threat or individual rights from serious damage. Data transmission in such situations is justifiable. But it is not clear why data obtained by the competent authorities for crime prevention, investigation or prosecution purposes can be forwarded to private entities in order to perform their lawfully assigned tasks as established in Article 14(1)c(i).

4.3.3.5. Other particularities

Framework Decision 2008/977/JHA does not mention any difference in treatment and processing of different categories of persons, such as convicted persons, suspects, witnesses, victims and others. The processing of data of different categories of persons should be subject to different rules, especially in such questions as its storage or onward transmission to third or private parties.[305]

In respect of the control of data protection, application of relevant national provisions has to be supervised by the independent supervisory authorities of each country. Such authorities shall have powers to investigate, intervene and participate in legal proceedings. In this regard, O'Neill makes a very precise observation that supervisory authorities shall have security clearances as data exchanged that is subject to control, can be classified or belong to special categories.

[304] BOSCH MOLINÉ, Alba, "La dimensión exterior de Europol desde el punto de vista de la protección de datos. El caso del acuerdo TFTP" in PI LLORENS, Montserrat and ZAPATER DUQUE, Esther, *La dimensión exterior de las agencias del espacio de libertad, seguridad y justicia* (Madrid: Marcial Pons, 2014), p. 134.

[305] For critics of the Council Decision 2008/977/JAI also see GUASCH PORTAS, Vicente, *Las transferencias internacionales de datos…*, op. cit., p. 290-292.

Summing up weak points of the Framework Decision 2008/977/JHA, it is the example of the result of legislative procedure under the Third Pillar, where the unanimity of all Member States was required, and when final the result seems to be more of a "wish list" of exceptions and flexible provisions than aspiration to proper and comprehensive data protection.

As pointed out, the European Data Protection Supervisor in the Third opinion of the European Data Protection Supervisor of the Proposal on the draft of this Framework Decision, "The decision-making procedure cannot justify a lowest common denominator approach that would hinder the fundamental rights of EU citizens as well as hamper the efficiency of law enforcement."[306] and "In many aspects the revised proposal even falls below the level of protection afforded by Convention 108. It is thus both unsatisfactory and will even be incompatible with international obligations of the Member States."[307]

But even this absolutely weak data protection regime had not been implemented in every country by the end of 2014, when there were still nine Member States that had not notified the Commission or the Council about transposition measures.[308]

With the entrance into force of the Treaty of Lisbon, the Commission took the initiative to revise the European data protection system and in 2012, presented a package of measures that have to substitute current weak regulations. New regulations for the area of police and judicial co-operation in criminal matters will be discussed in the part, "Projects in the pipeline".

5. Brief summary and evaluation

Side or negative effects of globalization, technological progress, terrorism, liberties of movement that came out in the form of crime, resulted in the need to abolish borders in such purely national function as *ius puniendi* and to introduce and

[306] OJ C 139, 23.6.2007, p.3.

[307] OJ C 139, 23.6.2007, p.2.
In the same opinion, a very valuable example of the patchwork system created by the Council Framework Decision 2008/977/JHA is given:
"[...] a law enforcement body at national or EU level, when dealing with a criminal file — consisting of information originating from various national, other Member States' and EU authorities — would have to apply different processing rules for different pieces of information depending on whether: personal data have been collected domestically or not; each of the transmitting bodies has given its consent for the envisaged purpose; the storage is compliant with time limits laid down by applicable laws of each of the transmitting bodies; further processing restrictions requested by each of the transmitting bodies do not prohibit the processing; in case of a request from a third country, each transmitting body has given its consent according to its own evaluation of adequacy and/or international commitments. In addition, citizens' protection and rights will vary enormously and be subject to different broad derogations depending on the Member State where processing takes place."

[308] Council document 11902/15, p. 4.

prosecution some elements of free transnational movement to investigation as well.

Within the EU, it has resulted in a separate area of policy – Freedom, Security and Justice that with the entrance in force of the Treaty of Lisbon, has been transformed from intergovernmental co-operation into supranational policy, subject to the control of the European Court of Justice and infringement procedure.

In the field of information exchange, a crucial stimulus to establishing the principle of information availability were the terrorist attacks at the beginning of millennium.

As stated by the European Parliament, after the terrorist attacks of 11th September, two tendencies in information processing and exchange can be distinguished, "Data processing in EU internal security policies is increasingly moving towards mass processing [...] Automated processing and datamining with the aim of profiling categories of person."[309]

It has shaken the sensitive balance between security and fundamental rights, moving towards the overweighting of security. Some fundamental rights can be indirectly affected by this tendency, but on the right to data protection it can have a direct effect

In these circumstances effective data protection systems have even greater importance, including at least common minimum standards applied in all states under consideration as well as independent and effective supervision systems.

Both have been attempted within the frameworks of the Council of Europe and of the European Union. Bearing in mind the wide membership of the Council of Europe, regulation does not reach much farther than the establishment of general principles. On the other hand, the European Union has intended to carry this out with more precise obligations, although the final result approved by Member States is quite perfunctory.

Nevertheless, one of the last political declarations of JHA Council on this topic allows us to expect better regulation in the future because it states that, "Privacy and security are possible and that there is no need to choose between being free

[309] EUROPEAN PARLIAMENT, Directorate General for Internal Policies, "Developing an EU Internal Security Strategy, fighting terrorism and organized crime" (study, 2011), p. 102, accessed August 13, 2015, http://www.europarl.europa.eu/document/activities/cont/201206/20120627ATT47777/20120627ATT47777EN.pdf.

and being safe and that the necessary and appropriate processing of personal data is vital in keeping the public safe."[310]

And as pointed out by Mitsilegas, "The development of the right to a privacy – linked to autonomy, freedom, dignity and personhood – has the potential to raise standards by placing the individual and the Self at the heart of protection."[311]

[310] Council conclusions on the Communication from the Commission to the European Parliament and the Council - A comprehensive approach on personal data protection in the European Union 3071st JUSTICE and HOME AFFAIRS Council meeting Brussels, 24 and 25 February 2011.

[311] MITSILEGAS, Valsamis, *EU Criminal Law* (Portland: Hart Publishing, 2009), p. 279.

PART II:
POOL OF TOOLS: DEVELOPMENT, APPLICATION AND PROBLEMS ASSOCIATED WITH SOME INFORMATION EXCHANGE INSTRUMENTS

CHAPTER 3:
INFORMATION EXCHANGE UNDER SCHENGEN ACQUIS

The Schengen area is a symbol of liberty of movement with checks on common borders abolished.[312] The political will of free movement existed since the Treaty establishing the EEC was signed in Rome on 25th March 1957. Its Article 3 foresaw the abolition of obstacles to the freedom of movement for persons, services and capital. But due to the difficulties in reaching agreement between all the Member States, firstly it was put into practice by the multilateral agreement and not by communitarian legislation.

Opening of the internal borders carried some risks to security and therefore it was accompanied by compensatory measures, part of whose were dedicated to fluent information exchange between law enforcement authorities.

This Chapter presents the analysis of the SIS and its second generation, functioning of police and customs cooperation centres, role of liaison officers as well as of general legal basis for cross-border information exchange envisaged in Articles 39 and 46 of the CISA.

1. From multilateral Agreement to Schengen Acquis

Despite the general EEC commitment to create the area of free movement, some Member States had not been able to agree on the abolition of checks on common borders for more than 25 years and it impelled intergovernmental initiatives out of the EEC framework. On 13th July 1984, France and Germany signed the

[312] In the Schengen Agreement and the CISA term "common borders" is used, but in the EU law, especially Treaties, more frequent term "internal borders" is met.

Experimental Convention of Saarbrücken.[313] As the Benelux countries (Belgium, Luxemburg and the Netherlands) had created a Customs Union and had abolished checks at their borders in 1962, on 12th December 1984, the Governments of the Benelux Economic Union signed a Memorandum expressing interest in the Experimental Convention of Saarbrücken. Thus it was rewritten and it resulted in the Agreement 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 (hereinafter – the Schengen Agreement), signed on 14th June 1985 in Schengen –a Luxembourg border town with France and Germany. According to Hreblay, these five countries wanted to give a very strong political signal demonstrating the real image of a united and free Europe.[314] According to Moreno Catena and Castillejo Manzanares, it was the fruit of pragmatism that allowed the creation of the true free movement of persons.[315]

The Schengen Agreement was largely negotiated by the ministers of transport and foreign affairs. However, an envoy from the German Ministry of Interior raised the question of compensatory measures for security in the case of abolition of internal borders that were part of the security mechanism.

Article 9 of the Schengen Agreement establishes that in the short term, "Parties shall reinforce cooperation between their customs and police authorities, [...]. To that end and in accordance with their national laws, the Parties shall endeavour to improve the exchange of information and to reinforce that exchange where information which could be useful to the other Parties in combating crime is concerned. Within the framework of their national laws the Parties shall reinforce mutual assistance in respect of unauthorized movements of capital."

Different opinions can be found in this respect. For example, Parkin believes that the broad police and justice cooperation measures foreseen in the CISA have secondary meaning and are exaggerated.[316] Nevertheless, other authors like Alvargonzáles San Martín and Luengo Alfonso, have stated that weakness on

[313] See CALESINI, Giovanni, *European Police Law Handbook* (Roma: Laurus Robuffo, 2007), p. 20-21; SCHATTENBERG, Bernd, "Schengen Information System: Privacy and Legal Protection" in SCHERMERS, Henry G.; FLINTERMAN, Cees; KELLERMANN, Alfred E. et al. *Free Movement of Persons in Europe* (Dordrecht: Martinus Nijhoff, 1993), p. 43; DONAIRE VILLA, Francisco Javier, *La Constitución y el Acervo de Schengen* (Valencia: Tirant lo Blanch, 2002), p. 44.

[314] HREBLAY, Vendelin, *Les accords de Schengen: Origine, Fonctionnement, Avenir* (Brussels: Bruylant, 1998), p. 15.

[315] MORENO CATENA, Víctor and CASTILLEJO MANZANARES, Raquel, *La persecución de los delitos en el Convenio...,* op. cit., p. 11.

[316] See PARKIN, Joanna, "Difficult Road to the Schengen Information System II: the legacy of 'laboratories' and the cost for fundamental rights and the rule of law" (report, Centre for European Policy Studies, 17 June 2011), p. 3, accessed September 9, 2013, http://www.ceps.eu/book/schengen-information-system-and-eu-rule-law.

interior borders can result in a rise in illegal migration, evasion of national legislation and crime.[317]

Talking about long-term measures that allow total abolition of internal border controls, Article 18 of the Schengen Agreement foresaw that "parties shall open discussions, in particular on the following matters, account being taken of the results of the short-term measures: (a) drawing up arrangements for police cooperation on crime prevention and investigation; (b) examining any difficulties that may arise in applying agreements on international judicial assistance and extradition, in order to determine the most appropriate solutions for improving cooperation between the Parties in those fields; (c) seeking means to combat crime jointly, inter alia, by studying the possibility of introducing a right of hot pursuit for police officers, taking into account existing means of communication and international judicial assistance."

Long-term measures were supposed to be in force and applied by 1st January 1990; [318] but due to the merging of the Federal Republic of Germany and the German Democratic Republic, and the opening of their inner borders on 9th November 1989, the signing of the CISA had been postponed[319] and eventually took place after the foreseen deadline on 19th June 1990. On 25th June 1991, Portugal and Spain also joined the Schengen Agreement and the CISA.

Implementing the CISA, checks at common borders was finally abolished on 26th March 1995.

In parallel, the signing of the Schengen Agreement was immediately echoed at the Fountainebleau European Council on 25th-26th June 1985, asking the Council and the Member States to study the measures for the abolition of "all police and customs formalities for people crossing intra-Community frontiers".[320]

Further steps towards the abolition of checks on internal borders of EEC were made with the Single European Act[321] signed on 17th[322] and 28th[323] February 1986. It supplemented the TEEC by the new Article 8A, foreseeing that the area without internal frontiers had to be established over a period expiring on 31st

[317] See ALVARGONZÁLES SAN MARTÍN, Fernando, "Hacia un nuevo escenario de cooperación en asuntos de justicia e interior". In MINISTERIO DEL INTERIOR, *El espacio europeo de libertad, seguridad y justicia* (Madrid: Secretaría General Técnica, 2000), p. 16*;* LUENGO ALFONSO, Luis, "Cooperación Policial y Europol" in ibid, p. 103.

[318] See DONAIRE VIILA, Francisco Javier, *La Constitución y el Acervo de Schengen*, op. cit., p. 46.

[319] See SCHATTENBERG, Bernd, "Schengen Information System…", loc. cit., p. 44.

[320] Conclusions of the European Council 22/84, Fontainebleau, June, 28, 1984.

[321] OJ L 169, 29.6.1987, p. 1-19.

[322] Signed by Belgium, Germany, France, Ireland, Luxembourg, Netherlands, Portugal, Spain and United Kingdom.

[323] Signed by Denmark, Greece and Italy.

December 1992. The Justice and Home Affairs policy introduced by the Maastricht Treaty meant that real free movement would be reached with the accompanying measures in this area.[324]

But it was not enough, and finally a Protocol of the Amsterdam Treaty, signed on 2nd October 1997, incorporated the Schengen acquis[325] into the EU legal system. That meant the application of the existing regulation of the Schengen area to all of the EC and putting all future measures related to the Schengen area under EU decision-making procedures.[326] The Schengen acquis[327] became a part of EU law on 1st May 1999 with the coming into force of the Treaty of Amsterdam.

Notwithstanding, membership of the EU did not mean automatic membership of the Schengen area. According to Art. 2.2 of the Protocol integrating the Schengen acquis into the framework of the EU, EU Member States not signatories to the Schengen Agreement and the CISA could become members of the Schengen area only after a unanimous decision of the Council. Such a decision was (and still is) based on evaluations of the conditions that every country has to meet before joining the Schengen area: application of common visa issuing policy; common asylum granting policy; operational readiness of N-SIS and its interoperability with C-SIS; police cooperation; protection of external land, sea and air borders and data protection.

Going back to compensatory measures, the CISA foresaw a long list of security measures applied together with the abolishment of common borders, most of them in the Title III "Police and Security":

---

[324] See ALVARGONZÁLES SAN MARTÍN, Fernando, "Hacia un nuevo escenario de cooperación…", loc. cit., p. 15.

[325] According to the Annex of the Protocol integrating the Schengen acquis into the framework of the European Union of the Amsterdam Treaty, Schengen acquis consists of:
- "the Schengen Agreement,
- the CISA,
- Agreements on Accession,
- Decisions and declarations of Executive Committee, acts adopted for the implementation of the Convention by the organs upon which the Executive Committee has conferred decision-making powers."

[326] At the time of the adoption of Schengen acquis (due to the existence of the three pillars system abolished by the Lisbon Treaty) different EU / ECC decision-making processes were applied. The Schengen acquis provisions on free movement of persons fell under the Community decision-making (former First Pillar) and supposed to be regulated by the TEEC and the police and judicial cooperation fell intergovernmental cooperation (former Third Pillar) and supposed to be regulated by the TEU. Precise EU / ECC legal basis for the different provisions of the Schengen acquis was determined by the Council Decision 1999/436/EC determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the Schengen acquis, OJ L 176, 10.7.1999, p. 17-29.

[327] The Schengen Acquis as referred to in Article 1(2) of Council Decision 1999/435/EC of 20 May 1999, OJ L 239, 22.9.2000, p. 1-473.

- Information exchange and or police assistance (Art. 39, 46);
- Cross-border surveillance (Art. 40);
- Cross-border pursuit (Art. 41);
- Liaison officers (Art. 7, 47);
- Supplement to the existing acts on mutual assistance (Art. 48-53);
- Application of ne bis in idem (Art. 54-58);
- Supplement to the existing acts on mutual assistance (Art. 59-66);
- Transfer of the enforcement of criminal judgments (Art. 67-69);
- Cooperation in combating drug trafficking (Art. 70-76);
- Cooperation in control firearms and ammunition (Art. 77-91).

Although from the title, a conclusion that only police measures were envisaged can be drawn, the content also included instruments of judicial co-operation as well. But due to the quick development of the cooperation in the area of justice in the last 15 years, the CISA's provisions related to mutual assistance, enforcement of criminal judgements, combating drug trafficking and controlling firearms and ammunition were derogated by more comprehensive and modern EU legislation.[328]

Another and more important compensatory measure, the SIS, was established in Title VI of the CISA. SIS was described as a system of obligatory use on external borders and a direct tool for the law enforcement authorities and for criminal investigation.

The following parts of this chapter will be dedicated to the analysis of those compensative measures used for information exchange among law enforcement authorities: SIS, Art. 39 and 46 and their relation with the aforementioned Framework Decision 2006/960, liaison officer corps as well as police and customs cooperation centres.

But before that, let's have a look at membership of the Schengen area, as it deserves some attention and at least a basic explanation, given its geographical difference from the EU membership area.

[328] Articles 59–66 were replaced by the Council Framework Decision 2002/584/JHA o the European arrest warrant and the surrender procedures between Member States (hereinafter – Framework Decision 2002/584/JHA), OJ L 190, 18.7.2002, p. 1-18. Articles 77 to 81 and Articles 83 to 90 of the implementing Convention have been superseded by the Council Directive 91/447/EEC on control of the acquisition and possession of weapons, OJ L 256, 13.9.1991, p. 51-58, with the following amendments (OJ L 179 of 8.7.2008, p. 5-11). Articles 49(a), 52, 53 and 73 by the Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ L 197, 12.7.2000, p. 3-23.

Currently, the Schengen area consists of 26 countries: 22 EU Member States and 4 non-Member States and with the special partial Schengen acquis application to Ireland and specific to the United Kingdom and access of Bulgaria and Romania to SIS II, but for the moment without abolishment of the control on internal borders.

EU Member State	Member of Schengen Area
Austria	
Belgium	
Bulgaria[329]	
Croatia	
Cyprus	
Czech Republic	
Denmark	
Estonia	
Finland	
France	
Germany	
Greece	
Hungary	
Ireland[330]	
Italy	
	Iceland[331]
Latvia	
	Liechtenstein[332]

[329] But already using SIS II.

[330] According to Article 4 of the *Protocol integrating the Schengen acquis into the framework of the European Union of the Amsterdam Treaty*, Ireland is not bound by the Schengen acquis, but has a right at any time to request partial or entire participation in it. Such participation has to be approved by the unanimity of the Council (OJ C 340, 10.11.1997, p. 95). According to the requests of the Government of Ireland, of 16th June 2000 and 1st November 2001, to participate in certain provisions of the Schengen acquis and the *Council Decision 2002/192/EC concerning Ireland's request to take part in some of the provisions of the Schengen acquis* it is participating in the police and judicial cooperation established by the Schengen acquis, except cross-border hot pursuit and surveillance (OJ L 64, 7.3.2002, p. 20-24). Never less those provisions of the CISA are still not applicable in Ireland.

[331] On 12th July 1957 Iceland, Norway, Sweden, Finland and Denmark signed Convention on the Abolition of Passport Controls at Intra-Nordic borders and created Nordic Union of Passports. As Sweden, Finland and Denmark joined the EU and the Schengen area, in order to assure further functioning of the Nordic Union of Passport, on 19th December 1996, the Agreement between the thirteen Member States of the European Union, signatories to the Schengen Agreements and the Republic of Iceland and the Kingdom of Norway was signed. Therefore, Article 6 of the Protocol integrating the Schengen acquis into the framework of the European Union of the Amsterdam Treaty established that Iceland and Norway shall be associated with the implementation of the Schengen acquis and its further development. It was reflected in the Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis (OJ L 176, 10.07.1999, p. 1-16).

[332] On 28 February 2008 a Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the

Lithuania		
Luxembourg		
Malta		
Netherlands		
		Norway
Poland		
Portugal		
Romania[333]		
Slovakia		
Slovenia		
Sweden		
		Switzerland[334]
United Kingdom		

Table 2: Belonging to EU and Schengen Area.

In the same way as Ireland, according to Article 4 of the Protocol integrating the Schengen acquis into the framework of the European Union of the Amsterdam Treaty, the United Kingdom was not bound by the *Schengen acquis*, but had a right at any time to request partial or entire participation in it.

According to the request of 22nd May 1999 (and its further modifications on 9th July and 6th October) and to the Council Decision 2000/365/EC concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the *Schengen acquis,* the United Kingdom participates in police and judicial cooperation established, except cross-border hot pursuit.[335] On 22nd December 2004, the Council Decision 2004/926/EC on putting into effect of parts of the Schengen acquis by the United Kingdom of Great Britain and Northern Ireland was adopted.[336] Partial participation in the application of the CISA also entailed the United Kingdom in the participation of the SIS, with regard to criminal law and policing information; but due to the difficulties with N.SIS, it was decided to wait until the second generation of the SIS is created and to join that.[337] The United Kingdom became operational in April 2015 and was granted temporary access to SIS II as a Council Decision with regard to evaluation is still

Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis was signed (OJ L 160, 18.6.2011, p. 21–36).

333 But already using SIS II.

334 On 26 October 2004 Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis was signed (OJ L 53, 27.2.2008, p. 52-79).

335 OJ L 131, 1.6.2000, p. 43-47. See FERNÁNDEZ-PITA Y GONZÁLEZ, Rafael, "El Tratado de Amsterdam y el Acervo de Schengen" in MINISTERIO DEL INTERIOR *El espacio europeo de libertad...,* op. cit., p. 93.

336 OJ L 395, 31.12.2004, p. 70-80.

337 See HOUSE OF LORDS, EUROPEAN UNION COMMITTEE "Schengen Information System II (SIS II)" (Report with Evidence, 2007), p. 12-14, accessed January 18, 2013, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldeucom/49/49.pdf.

pending. As it does not apply *Schengen acquis* with respect to free movement, it has not abolished its border controls.

2. Schengen Information System

Before abolishment of the control of common borders, each country was responsible only for its own security and chose who it was going to send information about real or potential threats to.[338] But within the obligation to contribute to the security of all the Schengen area, as noticed by Hreblay, the privileged partner does not exist anymore as all of them have be equally aware of all threats and receive the same information.[339]

With the abolishment of common borders, more thorough control of persons and goods and additional measures were moved to the external border. The tool that is obligatory in the protection of external borders (land, air and maritime) and issuing visas for the Schengen area is SIS. It can also be used in internal checks performed by the law enforcement agencies when a person or an object raises suspicions.

SIS is one of very few centralized systems[340] of the EU and the biggest in terms of content. It allows the sharing of information about persons that can be a threat to internal security or need special attention and he objects of crime or investigation in the form of alerts among all Schengen Member States.

The core element of the SIS is alert – a set of data on a person or object that requires special attention from the authorities performing the check. An alert sent by one country is automatically seen by the rest of the partners.

Nowadays, SIS is an information exchange tool used most widely within the Schengen area.[341]

On 31st December 2013 SIS II contained 50 279 389 alerts with the following "Top 5" of the countries entering alerts: Italy (32.2% of all alerts), Germany (15%), the Netherlands (7.9%), Spain (7.8%) and France (5.5%).[342]

Since the beginning of the functioning of SIS II (9th April 2013) until 31st December 2013, SIS II was consulted 1 284 512 470 times. The countries that

338 See HREBLAY, Vendelin, *Les accords de Schengen: Origine*…, op. cit., p. 149-150.
339 Ibid.
340 Apart from the Eurodac and the Visa Information System (VIS).
341 See COM(2015) 185 final, p. 4.
342 See EUROPEAN AGENCY FOR THE OPERATIONAL MANAGEMENT OF LARGE-SCALE IT SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE. "SIS II – 2013 Statistics" (Report, June 2014), p. 9, accessed July 16, 2014, http://www.eulisa.europa.eu/Pages/SIS-II-statistics.aspx.

more often consulted the system were Spain(26.75%), Germany(18.62%), Poland (10%), Romania (5%) and Czech Republic (3.89%).[343]

2.1. From reporting to investigation

At the moment of its establishment in the nineties SIS was viewed as a "form of computerized cooperation – a novelty in the international field",[344] a "vertebral column"[345] of free movement of people within the Schengen area.

As i mentioned before, looking structurally at the CISA, the provisions on SIS are laid out in the Title IV, i.e. Separately from the provision on police and judicial cooperation laid out in the Title III. First of all, it was seen as a tool for police controls on external borders and for the administration of foreigners[346]

Nevertheless, let's analyse it from different perspectives:

- Primary legal regulation: Article 93 of the CISA foresaw that the purpose of SIS is to maintain public order and safety, including State security, and to implement the provisions on the movement of persons in the territory of the Member States, but it did not make direct reference to police and judicial cooperation.
- The EU political approach: after transposing the Schengen acquis into EU legal framework, the European Commission considered SIS as "a vital factor in the smooth running of the Schengen frontier-free area and indispensable both in applying the Schengen arrangements on the movement of persons and in ensuring police and judicial cooperation in criminal matters"[347] and move "from a reporting system to a reporting and investigation system"[348].
- Practical implementation: granting the right of the access (although it is not yet in use) to the United Kingdom and Ireland which at the beginning applied only the part of Schengen acquis related to police and judicial cooperation and called data stored in it "policing and criminal data"[349] also shows that the SIS was not only a tool for external border controls and the assurance of free movement of persons.

[343] Ibid, p. 7.
[344] SCHATTENBERG, Bernd, "Schengen Information System…", loc. cit., p. 47.
[345] ALVARGONZÁLES SAN MARTÍN, Fernando, "Hacia un nuevo escenario de cooperación …", loc. cit., p. 20.
[346] See DONAIRE VILLA, Francisco Javier, *La Constitución y el Acervo de Schengen*, op. cit., p. 114.
[347] COM(2001)720, p. 3.
[348] Ibid, p. 7.
[349] HOUSE OF LORDS, EUROPEAN UNION COMMITTEE "Schengen Information System II (SIS II)", loc. cit., p. 12.

- Scholar opinions: Peers describes SIS as the system firstly used by law enforcement institutions for checks at external borders or within Schengen states;[350] Recuero indicates that SIS was established to improve coordination between police, customs and judicial services;[351]Hayas states that it is a powerful apparatus for surveillance and control.[352]
- Current legal regulation of SIS II: Art. 2 of the Decision 2007/533/JHA says that the information exchange tools are in place for the purpose of police and judicial cooperation in criminal matters.

Thus it could be concluded that a lot of indications demonstrate the use of SIS as a tool for the police and justice cooperation, although it was only established directly in the EU regulation in 2007 with the approval of the legislation for SIS II.

2.2. From SIS to SIS II

The SIS is based on interaction of the central system C.SIS[353] and national systems N.SIS of every Schengen area state.

Competent authorities of the countries insert alerts on persons or goods into their N.SIS from where they are transmitted to C.SIS that has a mirror reflection of all existing alerts of the States. Other countries, performing checks, directly consult the C.SIS (and not the N.SIS of other countries) and see all alerts issued in the Schengen area. When a performed check of a person or object results in a match with the alert (a so called "hit"), the system automatically informs that issuing country and national SIRENE[354] offices of the searching and issuing State's exchange. SIRENE offices continue with the exchange of all additional information (confirmation of its existence and actuality, additional information that could help to identify the person or object).

Information exchange through the SIS started in 1995 between seven countries: Belgium, France, Germany, Luxembourg, the Netherlands, Portugal and Spain.

---

350 PEERS, Steve, *EU Justice and Home Affairs Law* (New York, Oxford University Press Inc., 2011), p. 908.

351 RECUERO, Paz, "La protección de datos y Schengen: Una visión desde la experiencia española" in GOIZUETA VÉRTIZ, Juana; GONZÁLEZ MURUA, Ana Rosa and PARIENTE DE PRADA, Iñaki (directors), *El Espacio de Libertad, Seguridad...,* op. cit., p. 198.

352 HAYES, Ben, "SIS II: fait accompli? Construction of EU's Big Brother database underway" (Statewatch Analysis, May 2005), p. 1, accessed October 14, 2013 http://www.statewatch.org/news/2005/may/sisII-analysis-may05.pdf.

353 It is located in Strasbourg (France) with the back-up system in Sankt Johann im Pongau near Salzburg (Austria).

354 SIRENE - Supplementary Information Request at the National Entries, Supplément d'Information Requis a l'Entrée Nationale.

Since then, the SIS has technically been extended to SIS I+ in order to cope with the connection of eighteen States. In 2000 fifteen countries[355] were connected, with the perspective to connect United Kingdom, Ireland and keeping one extra connection. The accession of 10 new countries to the EU in 2004 also meant the future extension of the Schengen area and a need for a technical solution for the connection of new countries to the SIS.[356]

On 28 September 2001, the Commission decided to take responsibility both for the funding of SIS II and for the development work carried out under Community funding.[357]

Council Decision 2001/886/JHA of 6th December 2001 on the development of the second generation Schengen Information System (SIS II)[358] foresaw a deadline for the development of the SIS II - December 2006. Besides the technological development of the central system and the need to adjust or to create new N.SIS, there was a need to adopt new legislation under the EU decision-making process in order to replace Articles 92-119 of the CISA.

The legislative basis for the operation of the SIS II were adopted in 2006 (Regulation (EC) No 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II)[359] (hereinafter – Regulation 1987/2006)) and Decision 2007/533/JHA.

Art. 1 of the above mentioned legal instruments establishes that the purpose of the SIS II is "to ensure a high level of security within the area of Freedom, security and Justice of the European Union including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States [...]."

Although SIS II legal bases were adopted with only a slight delay, the technical development of the SIS II faced much bigger problems and setbacks. As noticed by the European Court of Audits, "The delay and overspending resulted partly from the challenging governance context which limited the Commission's ability to

[355] Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Italy, Luxembourg, The Netherlands, Norway, Portugal, Spain and Sweden.
[356] The idea of the SIS II was already raised in 1997 in the Decision of the Executive Committee of 7 October 1997 on the development of the SIS (SCH/Com-ex (97) 24) (OJ L 239, 22.9.2000, p. 442).
[357] COM(2001)720 final, p. 4.
[358] OJ L 328, 13.12.2001, p. 1-3.
[359] OJ L 381, 28.12.2006, p. 4-23.

address operational issues and partly from weaknesses in the Commission's management."[360]

This delay meant keeping EU "newcomers" outside the Schengen area and created a two speed EU. Nevertheless, the Presidency Conclusions of the European Council held on 15th and 16th June 2006 expressed a political commitment to enlarge the Schengen area in April 2007.[361]

In mid-2006, the future Portuguese Presidency of the Council of the European Union[362] came up with the proposal of an interim solution to use a clone of the Portuguese system to connect new countries to SIS and then make the transition of all to SIS II.

On 5th December 2006 the Council adopted the Conclusions on the SIS II, the SIS 1+ and the enlargement of the Schengen area.[363] It was agreed to apply the intermediate solution proposed by Portuguese experts, "A clone of the Portuguese national system and developed by experts from Portugal's Border and Foreign Service of the Ministry of Internal Affairs, relied upon extending the current version of the SIS to enable access by the new member states"[364] named "sisone4all". It allowed nine newcomers to the EU (Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia) to lift checks on their internal borders.[365]

As pointed out by BERTOZZI, "Adding another difficult task such as the development of a parallel system to the workload of member states and the Commission hardly makes things easier - but the Portuguese idea immediately

---

[360] EUROPEAN COURT OF AUDITS, "Lessons from the European Commission's development of the second generation Schengen Information System (SIS II)" (Special Report, 2013), p. 6, accessed July 16, 2014, http://www.eca.europa.eu/Lists/ECADocuments/SR14_03/SR14_03_EN.pdf.

[361] Council document 10633/1/06, p. 2.

[362] Art. 16(9) of the Treaty on European Union establishes that the Presidency of Council configurations, other than that of Foreign Affairs (which means General Affairs Council, Economic and Financial Affairs Council, Justice and Home Affairs Council, The Employment, Social Policy, Health and Consumer Affairs Council, Competitiveness Council, Transport, Telecommunications and Energy Council, Agriculture and Fisheries Council, Environment Council, Education, Youth, Culture and Sport Council), shall be held by Member State representatives in the Council on the basis of equal rotation. Thus every 6 months, the presidency of the Council of the European Union is taken over by another Member States. The second semester of 2015 is presided by Luxembourg. From January 2016, the presidency will be respectfully held by the Netherlands, Slovakia, Malta, United Kingdom, Estonia, Bulgaria, Austria, Romania, Finland. See Council Decision 2009/908/EU laying down measures for the implementation of the European Council Decision on the exercise of the Presidency of the Council, and on the chairmanship of preparatory bodies of the Council establishes presidencies' rotation until 2020 (OJ L 322, 9.12.2009, p. 28-34).

[363] Council document 16391/1/06.

[364] PARKIN, Joanna, "Difficult Road to the Schengen…", loc. cit., p. 6

[365] The only "newcomer", Cyprus, declared that its national N.SIS would not be ready for 2007, and it would join SIS II directly.

gained strong currency with the new member states, who decided to throw themselves behind what y considered to be a timely and sensible solution. Thanks to the Portuguese idea, mutual distrust and anger did not degenerate into outspoken hostility to Schengen enlargement, which would have created an irreparable rift between the old Schengen member states and "Schengen candidates".[366]

As a result of this solution, the integration of the new Member States into the SIS 1+ through the sisone4all was accomplished by the end of 2007.[367] On 6th December 2007, the Council Decision 2007/801/EC on the full application of the provisions of the Schengen acquis in the Czech Republic, the Republic of Estonia, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic[368] was adopted. It allowed their internal land and sea borders to be abolished on 21st December 2007 and air borders on 30 March 2008.

SIS II finally became operational on 9th April 2013[369] with a 6 year delay and exceeding the primary budget 8 times.[370]

2.3. Content and functionalities of SIS II

Both the CISA, regulating SIS, and Regulation 1987/2006 and Decision 2007/533/JHA, regulating SIS II foresee 6 categories of alerts that can be inserted and consulted in the system:

- Alerts on persons wanted for arrest for extradition / surrender purposes;
- Alerts on refusing the entry of aliens;
- Alerts on missing persons, including those that need special protection:
- Alerts on persons sought to assist with a judicial procedure;
- Alerts on persons and objects for discreet or specific checks;

366 BERTOZZI, Stefano, "Schengen: Achievements and Challenges in Managing and Area Encompassing 3.6 million km^2" (Working document no. 284, Centre for European Policy Study, 2008), p. 16-22, accessed October 2, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1337624

367 See Council document 13540/06.

368 OJ L 323, 8.12.2007, p. 34-35.

369 It was established in the Council Decision 2013/157/EU fixing the date of application of Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 87, 23.3.2013, p. 8-9), and Council Decision 2012/158/EU fixing the date of application of Regulation (EC) No 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 87, 23.3.2013, p. 10-11).

370 Final budget was around 500 million euro for the whole project, including 189 million euro for the new C.SIS II instead of initially estimated 23 million euro. See European Court of Audits, "Lessons from the European Commission's…", loc. cit., p. 33-49.

- Alerts on objects for seizure or use as evidence in criminal proceedings.

On the basis of the experience from SIS, new legislation foresees some improvements related to the content or issuing of alerts, as well as some new functionalities and rights of access:

- Direct insertion of the European Arrest Warrant;
- The possibility of including not only alphanumeric, but also biometric data (photographs and fingerprints);
- Extension of the list of objects that can be subject to alert (aircrafts, boats, industrial equipment, etc.);
- Possibility to make a link between different alerts;
- Access of Eurojust and vehicle registration service providers.

2.3.1. Alerts: content and issuing rules

As mentioned before, SIS contains alerts on persons and objects that are somehow linked to the alternation of internal security. That shows erroneous judgement in the common understanding that SIS contains information about everyone. It is true that everybody can be subject to alert, despite having citizenship, but a person has to be linked to some police investigation or judicial procedure, violation of rules allowing entrance into the Schengen area or in need of special attention due to his/her age or physical or mental state.

Additionally, as stated in the report of the European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (hereinafter - eu-LISA) about SIS II content in 2013, "Alerts on persons represented 1.71% (861,900 alerts) of the content of SIS II. The biggest category of alert is represented by issued documents (such as passports, identity cards, driving licenses, residence permits and travel documents which have been stolen, misappropriated, lost or invalidated) with 79.23% (39,836,478 alerts) of the total amount of alerts."[371] Therefore the remaining 19.06 % alerts are on other objects.

The first type of alerts in SIS II is on persons wanted for arrest for extradition or surrender purposes. The difference between regulation of the CISA and the Decision 2007/533/JHA is that in the CISA, only extradition procedure was mentioned and in the Decision 2007/533/JHA both extradition and surrender under the European Arrest Warrant are foreseen. Despite this change, the factual content of this category of alerts remains the same.

[371] See EUROPEAN AGENCY FOR THE OPERATIONAL MANAGEMENT OF LARGE-SCALE IT SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE. "SIS II – 2013 Statistics", loc. cit., p. 9.

During the drafting and approval of the CISA, the process known as extradition procedure was based on the principle of mutual assistance between involved states and meant the application of the complicated national process of making a decision to surround a person wanted by another country[372] (involving judicial authorities and authorities of the executive power[373]). The evolution of judicial cooperation in the EU resulted in moving from the principle of mutual assistance to mutual recognition[374]; that means recognition of the judicial decision of other EU Member States without complicated internal procedure.[375] The first instrument of practical implementation of the mutual recognition was the Council Framework Decision 2002/584/JHA of 13th June 2002 on the European arrest warrant and the surrender procedures between Member States (hereinafter – Decision 2002/584/JHA)[376], adopted on 13th June 2002 and applied instead of the extradition procedure among EU Member States since 1st January 2004. Due to that Chapter V of the Council Decision 2007/533/JHA refers to the persons wanted for arrest for surrender (among the EU Member States members of Schengen area) or extradition purposes (when one of the parties (issuing or requested) is a member of the Schengen zone, but not one applying the Framework Decision 2002/584/JHA, i.e. Norway, Iceland, Switzerland, Liechtenstein).

In both cases, the basis for the alert is a decision of the judicial authority. The novelty is that according to Article 27 of the Decision 2007/533/JHA, in the case of surrender on the basis of the European Arrest Order, an alert issuing Member State is also obliged to enter in the SIS II a copy of the original of the European Arrest Warrant.

---

[372] As extradition very often is accompanied by the detention of a wanted person, it is always based on a judicial decision.

[373] Such as Ministries of Justice or even Ministries of Foreign Affairs or governmental committees or councils.

[374] As mentioned before, for the first time mutual recognition was established by the Tampere Conclusions of the Tampere European Council 15th-16th October 1999 that were adopted in order to implement measures of the judicial and police cooperation established by the Amsterdam Treaty:
"Enhanced mutual recognition of judicial decisions and judgements and the necessary approximation of legislation would facilitate co-operation between authorities and the judicial protection of individual rights. The European Council therefore endorses the principle of mutual recognition which, in its view, should become the cornerstone of judicial co-operation in both civil and criminal matters within the Union. The principle should apply both to judgements and to other decisions of judicial authorities. [...] the formal extradition procedure should be abolished among the Member States as far as persons are concerned who are fleeing from justice after having been finally sentenced, and replaced by a simple transfer of such persons [...]".

[375] Although it is not an automatic recognition of a foreign judicial decision, but it does mean the application of simplified checking procedure by the national judicial authority (only judicial, without involving of the Executive Power) if a foreign judicial decision is not opposed to national judicial system and legislation.

[376] OJ L 190, 18.7.2002, p. 1-18.

For example, border guards or police authorities perform checks in the airport and detects that a person is a subject to alert on surrender or extradition. A copy of the European Arrest Warrant permits immediate access to both information on crime committed, and the judicial authority issuing the European Arrest Warrant. The issuing country will receive a notification that its alert resulted in a hit in another country and SIRENE offices of both of them will exchange all necessary information for the decision on further actions. If the issuing state confirms its need for a person's surrender or extradition, then execution of the European Arrest Order or extradition request, according to the national law of the requested state, will take place.

In the case of alerts on surrender, it is very important to take into consideration the principle *non bis in idem.* According to the European Court of Justice the same act is not understood as the same legal classification, but as "Identity of the material acts, understood as the existence of a set of concrete circumstances which are inextricably linked together."[377]

As a general rule, Member States assess the existence of *non bis in idem* only at the stage of the authorisation of surrender procedure to the requesting Member State, i.e. When a person is detected and possibly detained on the basis of alert. Nevertheless, this assessment should take place at the moment of appearance of the alert in the system, i.e. Member States receiving a new alert through SIS II should check whether a person was already convicted or acquitted for the same act on their territory. This would allow many inconveniences and violations of fundamental rights of the person concerned to be avoided.

The second category of alerts is on refusing the entrance of third-country nationals to the Schengen area based on the decision of the competent administrative or judicial authority of one the members of Schengen area. Only third-country nationals can be subject to this category of alert, i.e. According to Article 3 (d), "Any individual who is neither citizen of the European Union within the meaning of Article 17(1) of the Treaty nor a national of a third country who, under agreements between the Community and its Member States on the one hand, and these countries, on the other, enjoys rights of free movement equivalent to those of citizens of the European Union."

This is the only category of alerts regulated by the Regulation 1987/2006 as they are directly related to the free movement of persons (former First Pillar of the EU) and not to compensatory measures and police cooperation.

[377] Judgment of Court of Justice in *Jean Leon Van Straaten v Staat der Nederlanden and Republiek Italië*, ECLI:EU:C:2006:614, C-150/05, paragraph 48; in *Criminal proceedings against Leopold Henri Van Esbroeck*, ECLI:EU:C:2006:165 C-436/04, paragraph 36.

According to Article 27 of the Regulation 1987/2006, besides police, customs and judicial authorities, "The right to search data under this category of alert may be exercised by the authorities responsible for issuing visas, the central authorities responsible for examining visa applications and the authorities responsible for issuing residence permits and for the administration of legislation relating to third country nationals in the context of the application of the Community acquis relating to the movement of persons."

As previously mentioned, this category of alerts and related information exchange do not fall under strict understanding of the police cooperation, and is outside of police cooperation in crime investigation and, therefore, will not be analysed in depth.

The third category of alerts is on missing persons, including those that need special protection (as minors or persons who have to be interned).

In case of this category of alert, regulation foreseen in the CISA and the Decision 2007/533/JHA is slightly different in terms but not in content. Article 97 of the CISA entails that the basis for alert is a decision of the competent authority or competent judicial authority, while Article 32(1) of the Decision 2007/533/JHA refers to the request of the competent national authority without emphasising judicial ones. Alerts on missing persons can be issued despite their nationality, and special attention is paid to missing minors.

Article 33 deserves special observation; this article foresees that information found on an adult missing person (if he/she is not a minor and does not need special protection) can be transmitted to others, apart from competent authorities, (e.g. His/her family) only with his/her consent. But competent authorities are allowed to communicate to the person who reported the disappearance the fact that the alert has been erased due to the missing person's appearance.

The following categories of alerts are on persons sought in order to assist with a judicial procedure. According to the Article 34 of the Decision 2007/533/JHA those are:

- Witnesses;
- Persons ordered or sought to summoned to appear before the judicial authorities for acts for which they are prosecuted;
- Persons to be served with the sentence or other procedural document of the process in which they are prosecuted or summons to carry out the penalty.

Article 98 of the CISA foresaw that such an alert can be issued on the request of the judicial authority, but Article 34 of the Decision 2007/533/JHA broadens the concept of the requesting authorities from judicial to competent ones. A new regulation also foresee that the alert could be issued not only to serve a summons in relation to the penalty applied, but also criminal judgment or other procedural documents related to the prosecution of the person in question. From first sight, this widening of the reasons to issue an alert could seem unnecessary and widening the list of people "under alert", but from another perspective, it allows a prosecuted person to be informed about the process against him / her and to ensure his / her procedural warranties (especially those foreseen in the Art. 6 of the ECHR, Art. 2-4 of the Protocol No. 7 to the ECHR, Chapter VI of the Charter) to inform the person about the judgment that will be, or has been taken, *in absencia* and to give him / her the opportunity to seek better defence .

The fourth category of alerts is for discreet checks (surveillance), or specific checks on persons and objects and has experienced the biggest modification in the new legislation.

First of all, it is related to the terms used. The CISA had foreseen "discreet surveillance" and "specific check" and the Decision 2007/533/JHA modified "surveillance" into "check", establishing in this way alerts for "discreet checks" and "specific checks". But legal provisions on the performance of "discreet surveillance" / "discreet checks" did not undergo any changes: it still remains a collection of information when border, other police and customs controls are carried out.[378] That means that this discreet action is performed only at the moment of the border, police or customs check and is not continued afterwards, i.e. After this check the person or object is allowed to continue the journey and is no longer observed. Therefore, the modification of "discreet surveillance" into "discreet check" is reasonable, as "surveillance" is an action more coherent with the process of movement after the followed subject and lasting in time. The change into "discreet check" also helps to avoid mixing up the category of alert in SIS II with the police cooperation instrument "Cross-border surveillance", foreseen in Article 40 of the CISA. In later cases "surveillance is a continuous process with the involvement of the competent authority of different Member State and can last hours, days or months, depending on the need."[379]

[378] See Article 99(4) of the CISA and Article 37(1) of the Decision 2007/533/JHA.

[379] Misuse of the term "surveillance" is also pointed out by the Association of Chief Police Officers of England, Wales & Northern Ireland who states that, "There is no intrusive, directed surveillance in this alert". See ASSOCIATION OF CHIEF POLICE OFFICER OF ENGLAND, WALES & NORTHERN IRELAND, "Guidelines for the use of the Schengen Information System II to locate people for judicial purposes", version 7, 2010, p. 5, accessed January 16, 2013, http://www.acpo.police.uk/documents/criminaljustice/2008/200810CJUSIS01.pdf.

The following modification is more significant as Decision 2007/533/JHA extends the categories of the object that could be under discreet or specific checks and besides vehicles, includes boats, aircraft and containers.

The general purposes of checks remain the same: prosecuting criminal offences, the prevention of threats to public security or internal or external national security. The table below presents in detail the differences between previous and current regulation.

CISA - Art. 99	**Decision 2007/533/JHA - Art. 36**
Such an alert may be issued for the purposes of prosecuting criminal offences and for the prevention of threats to public security:	Such an alert may be issued for the purposes of prosecuting criminal offences and for the prevention of threats to public security:
(a) where there is clear evidence that the person concerned intends to commit or is committing numerous and extremely serious criminal offences; or	(a) where there is clear indication that a person intends to commit or is committing a serious criminal offence, such as the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA; or
(b) where an overall assessment of the person concerned, in particular on the basis of past criminal offences, gives reason to suppose that that person will also commit extremely serious criminal offences in the future.	(b) where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to suppose that that person will also commit serious criminal offences in the future, such as the offences referred to in Article 2(2) of Framework Decision 2002/584/JHA.
3. In addition, the alert may be issued in accordance with national law, at the request of the authorities responsible for national security, where re is clear evidence that the information referred to in paragraph 4 is necessary in order to prevent a serious threat by the person concerned or serious threats to internal or external national security. [...]	3. In addition, an alert may be issued in accordance with national law, at the request of the authorities responsible for national security, where re is concrete indication that the information referred to in Article 37(1) is necessary in order to prevent a serious threat by the person concerned or serious threats to internal or external national security. [...]

Table 3: Difference between regulation of alerts on wanted persons in SIS and SIS II.

The first modification (from "clear evidence" to "concrete indication") can raise contradictory discussions. From the perspective of fundamental rights, "clear evidence" is a more accurate background for the restriction of the right to private and family life than is made by the discreet or specific check and the term "concrete indication" is much broader and could lead to the violation of the above mentioned right.

From the procedural perspective, evidence is a term more related to the judicial trial than to the phase when discreet or specific checks are ordered, i.e. The phase of investigation or operational activity. There could be concrete intelligence information or indication about the preparation to commit a crime, or about the

object being related to a serious crime, but is no evidence as yet. For example, one of the countries is gathering intelligence on the group of people that, according to police sources (agents, undercover officers, etc.) Are related to the trafficking of drugs, but competent authorities are missing information about the modus operandi used and the organisers. As trafficking is usually cross-border crime, it is logical that the competent authorities have the need to issue an alert for discreet checks, in order to find out missing information, e.g. the movement of suspects, their contacts and people who they mix with. This can help to reveal drug trafficking schemes and also possible relationships with organized crime groups from other Schengen area countries.

The second modification (from "extremely serious criminal offence" to "serious criminal offence such as offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA") brings legal certainty, because there is no definition of "extremely serious criminal offence", but Art. 2(2) of the Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States[380] foresees the exhaustive list of criminal acts that represent the background for the surrender procedure and are classified as serious crimes.[381]

[380] OJ L 190, 18.7.2002, p. 3.

[381] According to Article 2(2) of the Framework Decision 2002/584/JHA, there are two conditions for treating a crime as serious.
1. It has to be one of the following crimes: "participation in a criminal organisation, terrorism, trafficking in human beings, sexual exploitation of children and child pornography, illicit trafficking in narcotic drugs and psychotropic substances, illicit trafficking in weapons, munitions and explosives, corruption, fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests, laundering of the proceeds of crime, counterfeiting currency, including of the euro, computer-related crime, environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties, facilitation of unauthorised entry and residence, murder, grievous bodily injury, illicit trade in human organs and tissue, kidnapping, illegal restraint and hostage-taking, racism and xenophobia, organised or armed robbery, illicit trafficking in cultural goods, including antiques and works of art, swindling, racketeering and extortion, counterfeiting and piracy of products, forgery of administrative documents and trafficking rein, forgery of means of payment, illicit trafficking in hormonal substances and other growth, promoters, illicit trafficking in nuclear or radioactive materials, trafficking in stolen vehicles, rape, arson, crimes within the jurisdiction of the International Criminal Court, unlawful seizure of aircraft/ships, sabotage."
2. It shall be punishable in the alert issuing Member State by a custodial sentence or a detention order for a maximum period of at least three years (without verification of the double criminality of the act).
As correctly noticed by Oubiña Barbolla, in theory it sounds perfect, but in practice, one or other crime will face inexistence in some Member State, or the application of a lesser punishment than the maximum of three years; the regulation of the requesting (issuing) authority also has to be taken into account. See OUBIÑA BARBOLLA, Sabela "The European Arrest Warrant in Law and Practice" in RUGGERI, Stefano, *Liberty and Security in Europe. A comparative analysis of pre-trial precautionary measures in criminal proceedings* (Göttingen: V&R Unipress GmbH, 2012), p. 53-54.

Before this modification, the Schengen Joint Supervisory Authority pointed out that the method for selecting criminal offences leading to an Article 99 alert, varied between the States. Most of them declared that the decision depends on the type of measure and the type of crime. For instance, Belgium, Greece, Iceland, Italy, and Norway notified that Article 99 would be applied to serious crimes. In Sweden and Hungary, offences punishable with, respectively, more than four and five years of imprisonment are regarded as serious criminal offences. Austria applies both methods. In Denmark, Germany, Netherlands, Spain and Portugal, no specification exists on the category of criminal offences that may lead to an Article 99 alert given that any type of crime can be used. As a consequence of this diversity, the Schengen Joint Supervisory Authority recommended that "the list of serious crimes for which Europol is competent or the Council Framework Decision on the European Arrest Warrant can be used for this purpose".[382]

The last category of alerts in SIS II is related to objects for seizure or use as evidence in criminal proceedings. Article 38(2) of the Decision 2007/533/JHA has widened some of the existing types of objects and added new ones. For the sake of clarity, changes are shown in the table below.

CISA - Art. 100(3)	**Decision 2007/533/JHA - Art. 38(2)**
Stolen, misappropriated or lost motor vehicles (capacity over 50 cc)	Motor vehicles (capacity over 50 cc)
Stolen, misappropriated or lost trailers and caravans over 750 kg	Trailers over 750 kg, caravans
	Stolen, misappropriated, lost or invalidated vehicle registration certificates and license plates
	Boats and aircraft
	Industrial equipment, outboard engines and containers
Stolen, misappropriated or lost firearms	Firearms
Stolen, misappropriated or lost blank official documents	Stolen, misappropriated or lost blank official documents
Stolen, misappropriated or lost identity documents	Stolen, misappropriated, lost or invalidated identity and travel documents
Banknotes	Banknotes
	Securities and means of payment

Table 4: Differences between regulation of alerts on object for seizure or use as evidence in SIS and SIS II.

[382] JOINT SUPERVISORY AUTHORITY OF SCHENGEN, "Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 99 alerts in the Schengen Information System", 2007, p. 8, 12, accessed January 14, 2013, http://schengen.consilium.europa.eu/media/135672/07-02%20draft%20report%20article%2099.en08.pdf.

Changes brought by the Decision 2007/533/JHA have not only broadened the list of the objects that can be subject to the alert, but has also relinquished conditions on issuing alerts for vehicles, trailers, caravans and firearms.

According to Art. 100 of the CISA alerts on vehicles, trailers, caravans and firearms for seizure or use as evidence, could only be issued if those objects that were "stolen, misappropriated or lost". Disclaiming these conditions should be regarded as a positive change, because in the criminal process a need to seize, or to use as evidence, an object used for the commission of a crime appears (e.g. A car or a gun used for the robbery, container or caravan used for trafficking), but not necessarily stolen, misappropriated or lost.

The category of identity documents is broadened by the inclusion of invalidated documents (in addition to previous categories of those stolen, misappropriated or lost) and the addition of new travel documents. This extension makes sense as a document could be invalid or out of legal use, not only due to it having been lost, misappropriated or stolen, but also due to the decision of the competent authority. Inclusion of travel documents is justified by the wide circulation of visas that are not identity documents but very relevant in order to enter Schengen area.

The inclusion of new objects (boats, aircrafts, travel documents, vehicle registration certificates, vehicle license plates and payment methods) was influenced by changes in crime trends (which objects are used to commit a crime or to be the object of a crime) and developments in society (different modalities of payment methods). In the first half of the year of using the SIS II, the "champion" among the new types of object was payment methods , 99.8 % of which were entered by Italy.[383]

As alerts on refusing the entry of aliens have little relevance to criminal process, the following analysis of functioning and use of SIS II will include only: alerts on persons wanted for arrest for surrender or extradition purposes; alerts on persons sought to assist with a judicial procedure; alerts on persons and objects for discreet checks or specific checks; alerts on objects for seizure or use as evidence in criminal proceedings.

From the analysis above, the differences in authorities that are allowed to request the issuing of the alert can be noticed, as summarised in the following table.

[383] Information provided by KLEIN Dominique, representative of the Unit C3 (Transeuropean Networks for Freedom and Security and Relations with eu-LISA) of the Directorate General HOME of the European Commission on the Heads of SIRENE Offices Conference in Vilnius on 30 October, 2013.

Category of the alert	**Background**
Alert with respect to a person wanted for extradition or surrender	Request of judicial authority
Alert on a missing person	Competent authority of the Member State
Alert on persons sought to assist with a judicial procedure	Competent authority of the Member State
Alerts on persons and objects for discreet checks or specific checks	Authorities foreseen in national law and authorities responsible for national security
Alerts on objects for seizure or use as evidence in criminal procedure	Not specified

Table 5: Authorities authorised to request different types of alerts.

The diversity of authorities is justified by the actions that have to be taken in relation to an alert. The most precise requirement (or limitation) is established for the alert with respect to a person wanted for extradition or surrender. Only judicial authority is permitted to make this request as the consequence of an alert is a deprivation of liberty. In other cases, the term "competent authorities of the Member State" is used and can include both judicial and law enforcement authorities, depending on the national legislation. As an example, a table of competent authorities from some countries that have a right to authorise alert requests on persons and objects for discreet or specific checks is presented.[384]

Member State	**Competent authority (-ies) to request an alert for discreet or specific check**
Austria	Law enforcement authorities (Directorate-General for Public Security, Land Security Directorates, Federal Police Departments, Federal Police Services)
Belgium	All police and judicial authorities working 24 hours a day
Cyprus	Police and customs authorities
Czech Republic	Police and intelligence services
Denmark	Police
Estonia	Security Police Board, Tax and Customs Board, the Border Guard authorities, police and Prosecutor´s Office
Finland	Police, customs and border guard services
France	Police, judicial authorities, authorities of prefectures, special division of the Ministry of the Interior of the Republic of France
Germany	Police, customs and intelligence service
Greece	Public Security Division and the State Security Division of the Ministry of Public Order
Hungary	Police and customs authorities
Iceland	National Commissioner of the Police
Ireland	National Police
Italy	Main law enforcement authorities (Polizia di Stato – Arma dei Carabinieri and Guardia di Finanza)

[384] See JOINT SUPERVISORY AUTHORITY OF SCHENGEN, "Report of the Schengen Joint…", loc. cit., p. 16-17; Council document 12301/08, p. 2-6.

Member State	Competent authority (-ies) to request an alert for discreet or specific check
Latvia	Law enforcement authorities, Military Police, Prison Administration, Constitution protections Bureau
Luxembourg	Public Prosecution Office on the request of the police
Malta	Police service and security service
Netherlands	Public prosecutors
Norway	Prosecuting police attorney on request of National Bureau of Crime Investigation or district police
Portugal	Public prosecutor and the police.
Slovenia	Public prosecutor on the request of the police
Spain	Law enforcement and judicial authorities; also, those authorities responsible for the security of the state
Sweden	Public Prosecutor's Office, the police, customs and border guard services
Switzerland	Law enforcement authorities
United Kingdom	All law enforcement institutions

Table 6: Authorities of different Member State authorised to request alert for discreet or specific check.

The Schengen Joint Supervisory Authority criticised some countries (such as France and Italy) for disproportionate authorization to issue alerts by comparison with others where only one authority (in the case of Greece, Luxembourg and the Netherlands) is permitted to do that.[385] As already mentioned, Italy issued 32. 2% of all alerts.

In some cases, even the national law of one country foresees the different competencies of the national authorities in relation to the same category of alert. For example, according to the legislation of the United Kingdom, in the case of an alert for witnesses to seek to assist with a judicial procedure, the alert will be issued by the police and in the case of persons that are to be prosecuted – the Prosecutor or the Court.[386]

For alerts on objects for seizure, or use as evidence in criminal procedure, no authority is specified, but it could also be interpreted as a "competent authority", because national rules on SIS II have to indicate the authorities allowed to come out with an alert request.

Every alert contains a certain amount of data on subjects or objects, including personal ones. For the sake of personal data protection, Article 94 of the CISA, Article 20 of the Council Decision 2007/533/JHA and Article 20 of the Regulation

[385] See HAYES, Ben, "EU-SIS Schengen Information System Article 99 report: 33,541 people registered in SIS for surveillance and checks" (Statewatch Analysis, February 2008), p. 2-3, accessed October 13, 2013, http://www.statewatch.org/analyses/no-67-sis-art99.pdf.

[386] See ASSOCIATION OF CHIEF POLICE OFFICER OF ENGLAND, WALES & NORTHERN IRELAND, "Guidelines for the use of the Schengen…", loc. cit., p. 5-7.

1987/2006 establish limitations on data contained in the system. All three legal acts foresee the following categories of data on a person subject to an alert that can be stored:

- Surname and forenames, any aliases possibly entered separately;
- Any specific objective physical characteristics, not subject to change;
- First letter of second forename;
- Date and place of birth;
- Sex;
- Nationality;
- Whether the persons concerned are armed;
- Whether the persons concerned are violent;
- Reason for the alert;
- Action to be taken.

Article 20 of Decision 2007/533/JHA and Article 20 of the Regulation 1987/2006 increase the scope of the data included in SISI II by introducing new categories:

- Photographs;
- Fingerprints;
- Authority issuing the alert;
- A reference to the decision giving rise to the alert;
- Links to other alerts in SIS II;
- The type of offence.

New categories directly related to the person (subject to alert) are photographs and fingerprints. Article 22(1b) of Decision 2007/533, and Article 22(1b) of Regulation 1987/2006 state that these new categories of data can be used only to confirm the identity of a person that has been detected on the basis of the alphanumeric data in SIS II. Introducing photos and fingerprints into SIS II allows verification with greater accuracy, whether the person subject to an alert and the one that is checked are the same. There are numerous cases when the offender commits a crime using stolen documents and his/her real identity is not known to the law enforcement and judicial authorities, and therefore, an alert is issued in the name of the misused identity. In this case, a photo and the fingerprints of the offender are the only criteria to verify whether a person checked is a wanted person, or the legal owner of stolen documents. Previously, an officer having a hit of alphanumeric data had to detain a person and wait to receive the photo or fingerprints as supplementary[387] information.

[387] For supplementary information see subsection 2.4 of this Chapter.

Storage of the photos and fingerprints in the SIS II, allows immediate verification of the person is checked and to avoid deprivation of the liberty of the innocent person.

In 2015, the countries of the Schengen area agreed that introducing information about whether a person is a foreign fighter or a terrorist suspect could be mentioned in the alert.[388] It is especially applicable to alerts on specific and discreet checks. In the case of an alert hit that includes such information (irrespective of the category of the alert), the authority that carries out searches has an obligation to immediately inform the SIRENE bureau of the State which issued an alert.

According to the general rule, established in Article 40 of the Decision 2007/533/JHA and Article 27 of the Regulation 1987/2006/EC, access to SIS II data and the right to search is granted to the authorities responsible for border controls, other police and customs checks. Nevertheless, according to Art. 40(2), giving access to the national judicial authorities is allowed, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge within the limits that are needed for their duties.

With respect to the purpose, information from alerts can be used for purposes other than for which they were issued, only in order to prevent serious threats to public policy or security, to national security or to prevent serious crimes. In such cases, consent from the Member State that has issued the alert has to be obtained.

Decision 2007/533/JHA does not provide a definition of serious crime. But as in Article 36, a reference to a list of Article 2(2) of the Framework Decision 2002/584/JHA is made; serious crime should be understood as one of offences mentioned, or national competent authorities can interpret this provision according to their national provisions which can differ a lot. In order to avoid such uncertainty, it would be better to include in Article 3(1) a definition of serious crime, even if it is not a comprehensive one, than a reference to the Framework Decision 2002/584/JHA.

According to Articles 41 and 42 of the Decision 2007/533/JHA, Europol and Eurojust are also allowed to access some categories of alerts as it is presented in the table below.

[388] COM(2015) 185 final, p. 5.

Europol	**Eurojust**
- On wanted persons - On persons and objects for discreet or specific checks - On objects for seizure or use as an evidence	- On wanted persons - On missing persons - On persons sought to assist with a judicial procedure - On objects for seizure or use as an evidence

Table 7: Categories of alerts that can be issued by Europol and Eurojust.

Europol's access to the aforementioned categories of alerts was raised in 1999 as a recommendation in the EU "Action Plan on Organised Crime"[389], and officially foreseen in Article 1(9) of Council Decision 2005/211/JHA of 24th February 2005 concerning the introduction of some new functions for the Schengen Information System, included in the fight against terrorism (hereinafter, Decision 2005/211/JHA).[390]

Apart from the limitation in relation to the content of the SIS II, Europol's and Eurojust's right to access is different from the one granted to the States (and their national authorities), from a technical point of view as well. Europol and Eurojust are not able to access either N.SIS or C.SIS, but only special SIS II database copies with the relevant category articles for which they have an authorisation. These copies are updated by the C.SIS.

The European Data Protection Supervisor in its Opinion on the legislative proposals concerning the Second Generation Schengen Information System (SIS II) has highlighted that Europol and Eurojust, unlike competent institutions of States, are not authorised to take specific actions on alerts (arrest a person, perform specific or discreet check, etc.) And therefore these agencies will not use the SIS II as a compensatory measure for the abolition of the borders. They will use SIS II for their own institutional purposes and moreover, the legislation does not provide any specification of the purposes to access and allows "fishing expeditions"[391].

According to Article 41(3) of the Decision 2007/533/JHA, Europol can use the information obtained from a search in the SIS II with the consent of the Member State that has issued the alert, but it is clear that this use does not derive directly from the purpose of the SIS II.

In the case of Eurojust, Article 42(6) permits access to the SIS II only to the national members of Eurojust and their assistants and excludes Eurojust staff. According to the Article 2(1) of the Council Decision 2002/187/JHA of 28th

[389] See HAYES, Ben, "From the Schengen Information System to SIS and the Visa Information (VIS): proposals explained" (Statewatch analysis, February 2004), p. 10, accessed October 13, 2013, http://www.statewatch.org/news/2005/may/analysis-sisII.pdf.
[390] OJ L 68, 15.3.2005, p. 46-47.
[391] Council document 14091/05, p. 12.

February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime,[392] national members are prosecutors, judges or police officers of equivalent competence. And it does not contradict the general right of access to the SIS II established in the aforementioned Article 40(2) of Decision 533/2007/JHA.

Hayes questions Europol's and Eurojust's access needs, "With 125,000 access points to the SIS, it is surely beyond any credibility to suggest that an EU-level information broker is needed. Europol clearly wants the information in the SIS to use in conjunction with its own extensive *investigative* database. Eurojust and national prosecuting authorities' will also use SIS II for investigative purposes; it is worth stating again that the use of the SIS is currently limited to police and immigration checks. SIS II will be an altogether different proposition with a host of law enforcement and 'security' functions."[393]

Regulation (EC) 1986/2006 of the European Parliament and of the Council, regarding access to the Second Generation Schengen Information System (SIS II), by the services of the Member States responsible for issuing vehicle registration certificates[394], foresees access of the aforementioned services to alerts for seizure or use as evidence in criminal proceedings of the following objects: motor vehicles, trailers, data concerning vehicle registration certificates and vehicle number plates, in order to check whether the vehicles presented to them are stolen, misappropriated or lost, or are sought as evidence in criminal procedure.

In order to have general understanding in relation to the dimension of the SIS and the SIS II, the quantitative information on records is presented below. For this purpose, the years 1995 (the beginning of the functioning of the system with the first 7 countries), 2007 (functioning with 15 countries), 2008 (the access of new 9 countries) and latest available information are reflected.

Year	Number of countries	Number of records
1995	7	3,868,529[395]
2007	15	17,615,945[396]
2008	24	22,933,370[397]
2014	26	50, 279, 389[398]

Table 8: Figures on alerts issued in 1995, 2007, 2008 and 2014.

[392] OJ L 63, 6.3.2002, p. 2.
[393] HAYES, Ben, "SIS II: fait accompli?...", loc. cit., p. 6.
[394] OJ L 381, 28.12.2006, p. 1-3.
[395] HAYES, Ben, "From Schengen Information System…", loc. cit., p. 6.
[396] SCHENGEN JOINT SUPERVISORY AUTHORITY, "Eight Activity Report – December 2005 – December 2008", p. 9, accessed January 16, 2013, http://schengen.consilium.europa.eu/media/135384/8th%20schengen%20act.report%202005-08.en.pdf.
[397] Ibid.
[398] EUROPEAN AGENCY FOR THE OPERATIONAL MANAGEMENT OF LARGE-SCALE IT SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE, Report "SIS II – 2013 Statistics", loc. cit., p. 9.

2.3.2. Relationships between multiple alerts: compatibility, links and priorities

By entering an alert into SIS, a Member State can face a situation of the existence of another alert on the same person or subject. It could be an alert of the same or another category entered by the other institution of the same or other Member State. For example:

- SIS contains an alert on a person sought to assist with a judicial procedure and then, in relation to another (or the same case) judicial authority of the same or another Member State, issues European Arrest Order and orders the issue of an alert for arrest for surrender procedure.
- A car is subject to a specific check in the investigation of drug trafficking, but in another case, run by another authority, this car figures as a means to commit a robbery and an alert for seizure has to be issued.

For such cases, SIRENE Manual and other implementing measures for SIS II[399] approved by the Commission Implementing Decision (EU) 2015/219 (hereinafter –SIRENE Manual), foresees the protocol to be followed and establishes compatibility of alerts and priorities in cases of multiple alerts.

Every country is allowed to enter only one alert per person or object, i.e. If one institution is looking for a person as a witness to a crime, and another institution of the same country has issued a European Arrest Warrant, only one of these issues can be announced as an alert in the SIS II. The remaining one is kept at national level and can be introduced only when the prevailing alert is deleted from SIS II. The Member State has to decide the priority in which its alerts would be entered into the SIS II by itself, but the reference rules of the SIRENE manual on priority between alerts of different Member States can be applied.

On persons	On objects
- Arrest with a view to surrender or extradition	- Use as evidence
- Refusing entry or stay in the Schengen territory	- Seizure of document invalidated for travel purposes
- Placing under protection	- Seizure
- Specific checks with immediate action	- Specific checks with immediate action
- Specific checks	- Specific checks
- Discreet checks with immediate action	- Discreet checks with immediate action
- Discreet checks	- Discreet checks
- Communicating whereabouts	

Table 9: Priority in case of multiple alerts. [400]

[399] OJ L 44, 18.2.2015, p. 75-116.
[400] Ibid, p. 92.

Different Member States can have alerts on the same person if they are compatible among themselves according to the rules established by the SIRENE Manual as it presented below.

	Arrest	Refusal of entry	Missing person (protection)	Specific check (immediate action)	Specific check	Discreet check (immediate action)	Discreet check	Missing person (whereabouts)	Judicial procedure
Arrest	+	+	+	-	-	-	-	+	+
Refusal of entry	+	+	-	-	-	-	-	-	-
Missing person (protection)	+	-	+	-	-	-	-	+	+
Specific check (immediate action)	-	-	-	+	+	-	-	-	-
Specific check	-	-	-	+	+	-	-	-	-
Discreet check (immediate action)	-	-	-	-	-	+	+	-	-
Discreet check	-	-	-	-	-	+	+	-	-
Missing person (whereabouts)	+	-	+	-	-	-	-	+	+
Judicial procedure	+	-	+	-	-	-	-	+	+

Table 10: Compatibility of alerts on persons.[401]

Thus alert for arrest is compatible with all categories of alerts except alerts for specific or discreet checks. Alerts for specific or discreet checks are neither compatible with any other category of checks or among themselves.

In the case of multiple alerts for arrest, decision about the order of execution has to be taken by the executing judicial authority in the country where the arrest has occurred.

If alerts are incompatible, SIRENE bureaux of the countries involved have to consult each other and decide, which alert remains in the SIS II. If an agreement cannot be reached on the basis of the above mentioned list of priorities, the oldest alert is kept in the system.

In the case of the example with the car, the Member State has to issue an alert for seizure and the existing alert to check has to be deleted. If the Member States involved cannot reach an agreement, the older alert will be kept in the SIS II, i.e. Alert for check.

In the case of alerts on objects, the rules of compatibility are as presented in the table below.

401 Ibid, p. 91.

	For use as evidence	Invalidated doc. for travel	For seizure	Specific check (immediate action)	Specific check	Discreet check (immediate action)	Discreet check
For use as evidence	+	+	+	-	-	-	-
Invalidated doc. for travel	+	+	+	-	-	-	-
For seizure	+	+	+	-	-	-	-
Spec. Check (immediate action)	-	-	-	+	+	-	-
Specific check	-	-	-	+	+	-	-
Discr. check (immediate action)	-	-	-	-	-	+	+
Discreet check	-	-	-	-	-	+	+

Table 11: Compatibility of alerts on objects.[402]

Article 52 of the Decision 2007/533/JHA and Article 37 of the Regulation 1987/2006 bring a novelty that has not been possible in the SIS – links between alerts. In cases of operational need, it allows a relationship between two or more alerts on different persons or objects to be established. The link can be made only if the same Member State enters those alerts. For example, if one Member State investigates an organized group that steals cars, it can make a link between alerts on stolen cars, persons (members of the organized group) to be subject to discreet checks, other persons involved and already wanted for arrest.[403] Boehm echoes the

[402] Ibid, p. 92.

[403] SIS and SIRENE experts that working on the elaboration of the SIS II foresaw not exhaustive list of possible links:
- gang members + family members wanted for surrender or extradition;
- EU national offender wanted for surrender or extradition + convicted companion to be refuse entry;
- kidnapper + missing person;
- (sexual) offender + his child-victim or child-witness to crime;
- husband wanted terrorist or convicted to be refused entry + specific or discreet check of wife suspected accomplice;
- wanted person + specific or discreet check of his yacht or car;
- wanted person + stolen object;
- parent to be refused entry + missing child (third country national);
- person to be refused entry + stolen identity document;
- two or more missing siblings;
- missing person + person wanted for questioning on that missing person;
- missing child + car used for abduction, etc.

See Council document 12573/3/04, p. 3.

aforementioned opinion of the European Data Protection Supervisor[404] and interprets this development as transforming the SIS II into an investigative tool, "The status of an individual in the SIS II no longer depends solely on his or her personal actions, but, when connected to the actions of other people, the person concerned might be treated with more suspicion than before. This can easily lead to a situation in which a previously innocent individual is linked to an alert of a criminal, having as a consequence that the status of the relevant person will be negatively influenced."[405]

This reasoning could be criticised from different perspectives:

- As the SIS II remains, the task of the SIS to be one of the compensatory measures to the abolishment of the control of internal borders, the linking of the alerts enhances this function by making such an expensive tool as SIS II more effective. For example, if a competent authority performs specific or discreet checks on a person according to the alert that shows links to other persons that form organized crime groups, the officer would pay more attention to the persons travelling in the same car or on the same flight, etc. If linked persons use new aliases or forged identity documents with a different name from the one entered into SIS II, it would be impossible to detect them directly in SIS on the basis of alphanumeric data. But with the detection of at least one of the linked persons, the officer can access not only the alphanumeric data of linked alerts, but also attached photos and on this basis identify other persons under alert.
- A Person's status does not change by the linking alerts and still depends on the category of alert that is issued in relation to him. For example, if a person sought as a witness is linked to wanted persons, it is done because they figure in the same investigation, but it does not mean that the witness becomes more suspicious than before, at least they were detected together. In the last situation, first of all it can be considered that witness is travelling with the wanted person against his will and relevant measures can be taken. If he or she is travelling willingly, then SIRENE office of issuing country should be informed, but it does not change the status of a witness neither measure that can be applied to him or her.

[404] See Council document 14091/05, p. 13.

[405] BOEHM, Franziska, *Information Sharing and Data Protection in the Area of Freedom, security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU Level* (Verlag Berlin Heidelberg: Springer, 2012), p. 266.

2.4. SIRENE Bureaux

As already mentioned, SIRENE stands for "Supplementary Information request at the National Entries".

Article 7 of the Decision 2007/533/JHA and Article 7 of the Regulation 1987/2006 oblige every Member State to designate the authority to verify the quality of the information entered into the Schengen Information System, and to exchange all supplementary information – the SIRENE Bureau.

The need of the SIRENE bureaux was pointed out in the feasibility study on the CISA, in order to ensure the proper and quick exchange of supplementary information on the alerts and on other information. Nevertheless, SIRENE bureaux were officially mentioned only in 2005 by the modification of the Article 92 of the CISA by the Article 1 of the Council Decision 2005/211/JHA and Article 1 of the Council Regulation 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, included in the fight against terrorism.[406]

Until then, 2 different opinions existed:

- The basis for the SIRENE bureaux is Article 108 of the CISA that states that, "Each Contracting Party shall designate an authority which shall have central responsibility for its national section of the Schengen Information System…The said authority shall be responsible for the smooth operation of the national section of the Schengen Information System and shall take the necessary measures to ensure compliance with the provisions of this Convention."

  This point of view was supported by the experts that have drafted the SIRENE manual for the functioning of the first generation of the SIS.[407]

- There is no legal basis for the SIRENE bureaux in the CISA. This opinion was supported by the Schengen Joint Supervisory Authority and reflected in its activity reports.

The statement that Article 108 of the CISA is the basis for the SIRENE bureaux can be denied by the systematic analysis of the legal acts regulating Schengen Information System:

[406] OJ L 162, 30.4.2004, p. 30.

[407] See point 1 of the Council Decision 2003/19/EC on declassifying certain parts of the SIRENE Manual adopted by the Executive Committee established by the Convention implementing the Schengen Agreement of 14 June 1985 (OJ L 8, 14.1.2003, p. 38).

- If the legislator has considered that Article 108 is a basis for the establishment of SIRENE bureaux it would not adopt changes of Article 92 in 2004 and 2005, directly introducing SIRENE bureaux and defining their purpose and without making any reference to Article 108.
- Article 7 of the Decision 2007/533/JHA and the Regulation 1987/2006 stipulate that an authority which shall have central responsibility for its national section of the SIS II (equivalent to the wording of the Art. 108 of the CISA) is N.SIS II office and is different from the SIRENE Bureau whose task is to ensure the exchange of all supplementary information.

Meanwhile, as stated by Kabera Karanja, "Since the CISA was silent on the issue of the SIRENE and at the same time it allowed the application of the national law in such circumstances, then the national law was the legal basis of the SIRENE."[408]

The SIRENE bureau is the unique contact point working on a 24/7 basis, in order to provide supplementary information not stored in the C.SIS, but related to alerts, and is the "human interface" of SIS[409]. As highlighted by Hayes, "There is no effective limit on the data that can be exchanged through the SIRENE bureaux"[410], but there is a restriction on its use, as, according to Art. 8 of Decision 2007/533/JHA and of Regulation 1987/2006, it can be used only for the purpose for which it was transmitted.

The importance of the SIRENE Bureau within the functioning of the SIS is highlighted by the European Court of Justice in the case Commission v Spain (case C-503/03) where is stated that the SIRENE bureau has to be consulted before taking any further decision on action with a person that is subject to the alert.[411]

According to SIRENE Manual, the supplementary information shall be exchanged:

- For consultation with other countries whilst entering an alert;
- To inform about hit;
- To inform that actions required cannot be performed;
- For ensuring the quality of the SIS II data;
- To deal with the exercise of the right to access;

[408] KABERA KARANJA, Stephen, *Transparency and Proportionality in the Schengen Information System and Border Control Cooperation* (Leiden: Martinus Nijhoff Publishers, 2008), p. 204.

[409] See GARCÍA VÁZQUEZ, Sonia, "La cooperación policial y judicial como ejes de consolidación del espacio de Libertad, Seguridad y Justicia e instrumentos de protección de los derechos fundamentales en la Unión Europea" in GOIZUETA VÉRTIZ, Juana and CIENFUEGOS MATEO, Juan, *La eficacia de los Derechos Fundamentales de la UE* (Navarra: Aranzadi, 2014), p. 436.

[410] HAYES, Ben, "From Schengen Information System…", loc. cit., p. 14.

[411] See Judgment of the Court of Justice in *Commission of the European Communities v Kingdom of Spain,* C 503/03, ECLI:EU:C:2006:74.

- To deal with the compatibility and priority of the alerts that will be the object of further analysis.

Thus the SIRENE bureaux can be defined as a dynamic part of the SIS II as it helps to solve any question and problem related to the static alert of the C.SIS: to clarify uncertainties of alert, to find out whether it is still in force, to assure that the person or object detected is the one searched for under the alert, to agree on further actions, and so on.

3. Information exchange under Articles 39 and 46 of the CISA

Article 39 of the CISA establishes the legal basis for the assistance between national police authorities. Its content is not explained, but according to Moreno Catena and Castillejo Manzanares it can be understand in a broad sense and includes any measures, procedures or actions that constitute the competence of the requested authority.[412] Nevertheless, using a systematic analysis of the CISA, from which such assistance has to be excluded, for example, hot pursuit, cross-border surveillance and controlled delivery, as they have separate specific regulation.

Even if in the first paragraph of Article 39, the broad term "assistance" is used, the following paragraphs mainly focus on information exchange for the purpose of preventing and detecting criminal offences and establishing the following rules:

- Police authorities request and reply within their competence regulated by the national law;
- A request or its execution does not imply coercive measures from requested party;
- Only information that is not within the competence of judicial authorities can be exchanged;
- Received information cannot be used as evidence without authorisation of judicial authorities;
- Requests and replies are sent through the central national units responsible for the international police cooperation,
- In case of urgency direct assistance between competent authorities can take place, but anyway such information exchange later has to be notified to the central authority responsible for the international police cooperation of the requested party:

[412] See MORENO CATENA, Víctor and CASTILLEJO MANZANARES, Raquel *La persecución de los delitos en el Convenio…,* op. cit., p. 65.

Article 39(4) allows stipulating other rules of cooperation by bilateral or multilateral agreements for the border areas.

Article 46 of the CISA foresees almost the same rules for spontaneous information exchange, i.e. Providing information without previous request, if it is considered useful to combat future crime and prevent offences and threats to public security.

In the nineties, these provisions were of the utmost importance as they provided an opportunity for any kind multinational police assistance, except one demanding coercive measures. But the millennium came along with a wide range of specific instruments, channels and agencies for police cooperation and the above mentioned articles of the CISA lost their significance.

Moreover, their application has been limited by Decision 2006/960/JHA, which develops the provisions of the Schengen Acquis.[413]

Article 12 of the Framework Decision 2006/960/JHA establishes that the provisions of Article 39(1), (2) and (3) and Article 46 of the CISA are replaced as far as information and intelligence exchange for the purpose of conducting criminal investigations or criminal intelligence operations are concerned.

This formulation means that Articles 39 and 46 of the CISA are not replaced totally, and to some extent still stay in force. To find out the scope of current Article 39 of the CISA, the following table presents a comparison of its content with the relevant provisions of the Framework Decision 2006/960/JHA.

	Art. 39 of the CISA	**Framework Decision 2006/960/JHA**
Action	Assistance	Exchange
Object	Not specified	Information and intelligence
Purpose for the exchange	Preventing and detecting criminal offences	- Art. 1: Conducting criminal investigations[414] or criminal intelligence operations[415] - Art. 5: detection, prevention or investigation of an offence
Competent authorities	Police authorities	National police, customs or other authorities that are authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take

[413] SEC(2011) 593 final, p. 3.

[414] A definition is provided in Article 2(b) of the Decision 2006/960/JHA "A procedural stage within which measures are taken by competent law enforcement or judicial authorities, including public prosecutors, with a view to establishing and identifying facts, suspects and circumstances regarding one or several identified concrete criminal acts".

[415] A definition is provided in the Article 2(c) of the Decision 2006/960/JHA "A procedural stage, not yet having reached the stage of a criminal investigation, within which a competent law enforcement authority is entitled by national law to collect, process and analyse information about crime or criminal activities with a view to establishing where concrete criminal acts have been committed or may be committed in the future."

	Art. 39 of the CISA	Framework Decision 2006/960/JHA
		coercive measures in the context of such activities.
Limitations	- Not applied in the case of a need for judicial cooperation - Not applied in the case of a request whose execution demands a measure of constraint - Provided information cannot be used as evidence without the consent of the competent judicial authority of the requested Contracting Party.	- Request does not impose any obligation to obtain information or intelligence by means of coercive measures. - Provided information cannot be used as evidence before a judicial authority without the consent or providing Member State. Such consent can be given at the time of transmittal of the information or intelligence.

Table 12: Interrelationship between Article 39 of the CISA and Framework Decision 2006/960/JHA.

Thus the purpose of the information exchange under the Framework Decision 2006/960/JHA is established in two articles using different wording which, from the perspective of legal technique, should not be acceptable. Moreover, it seems problematic to put an "equal" sign between "conducting criminal investigations or criminal intelligence operations" and "detection, prevention or investigation of an offence", especially when talking about crime prevention. From one perspective, the definition of "criminal intelligence operations" (see Section 5 of the Chapter I) includes criminal acts that "may be committed in the future", and could be treated as prevention, but the same definition determines that criminal intelligence operations have "a procedural stage" and this aspect goes beyond the content of what is traditionally understood as prevention. A criminal intelligence operation is not yet an investigation, but already has its own procedural form and rules to be followed and mostly sticks to the gathering of intelligence that leads to investigation and prosecution. Prevention by nature is much broader and seeks to preclude factors that provoke crime.

Articles 4.1 and 4.3 of the Framework Decision 2006/960/JHA mention exchange of information and intelligence in relation to the offences listed in Art. 2(2) of the Framework Decision 2002/584/JHA (see footnote 382) and it could lead to understanding that this is an area of information exchange regulated by this legal act. Notwithstanding, systematic analysis of articles 1 (Objective and scope), 3 (Provision of information and intelligence), 4 (Time limits for provision of information and intelligence), 5 (Request for information and intelligence) and 7 (Spontaneous exchange of information and intelligence) leads to the conclusion that the Member State is free to make any request for information and intelligence when its purpose is conducting criminal investigations or criminal intelligence

operations, but deadlines for urgent response [416] are applied only when the request is related with the offence mentioned in Art. 2(2) of Framework Decision 2002/584/JHA. It makes sense in the view of the flow of requests and the limited possibilities to reply within the established deadlines and reference to the Framework Decision 2002/584/JHA which allows prioritisation in the workflow.[417]

Taking all that into account, the conclusion can be made that the Framework Decision 2006/960/JHA creates a "grey area" in which information exchange for crime prevention hangs without certainty, whether it falls within its scope or remains under Article 39 of the CISA.

On the basis of the analysis presented above, a very cautious conclusion can be made about the actual scope of Article 39 of the CISA. It has to be applied to:

a) Police co-operation assistance, other than providing information and intelligence in the prevention and detection of criminal offences;

b) Information exchange on crime prevention when it does not take place under the procedure of the criminal intelligence operation.

The Catalogue of Recommendations for the correct application of the Schengen Acquis and Best practices on Police cooperation[418] (hereinafter – Catalogue of Recommendations), updated in 2011 (more than 2 years after the deadline to implement the Framework Decision 2006/960/JHA[419]) does not help too much in establishing the line between the application of the Article 39 and the Framework Decision 2006/960/JHA because:

– Recommendation 6 says that "In the field of public order and public security, the central authorities should hold a list of requests for which direct assistance can be given in urgent situations"[420] and as the best practice, the reference to Art. 3 and 4 of the Framework Decision 2006/960/JHA is given. It means that the "equal" sign between "assistance" and "exchange" (of information) is made.

[416] At the most, 8 hours in case of urgent requests and one week in non-urgent cases when the information requested is directly accessible by the requested authority. In other cases – 14 days.

[417] Annex A and Annex B of the Framework Decision 2006/960/JHA make clear that urgency in reply is applied only in case of the offence that falls under the Art. 2(2) of the Framework Decision 2002/584/JHA. The same line is followed in Guidelines on the implementation of Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (Council document 9512/1/10).

[418] Council document 15785/2/10.

[419] According to the Art. 11 of the Framework Decision 2006/960/JHA (See Corrigendum OJ L 75, 15.3.2007, p. 26) it had to be implemented before 19 December 2008.

[420] Council document 15785/2/10.

- Recommendation 28 establishes that all police personnel should have basic knowledge of Article 39 of the CISA and Article 12 of the Framework Decision 2006/960/JHA. This introduces even more confusion, because it focuses on the article from the CISA dedicated to assistance (including information exchange) and on the article from the Framework Decision dedicated only to the spontaneous information exchange (without previous request), leaving articles on the information exchange on request on the margin.
- Recommendation 36, 37 and 39 on the information exchange on request totally refers to the Framework Decision 2006/960/JHA.

Even more inconsistency shows recommendations 40-46 on the spontaneous information exchange, as they do not make any reference to the Framework Decision 2006/960/JHA and its Article 12, which was mentioned in recommendation 28. It seems that Member States are urged to provide knowledge on Article 12, but are not urged to use it.

The latest recommendations lead to the analysis of spontaneous information exchange under Article 46 of the CISA, and relevant provisions of the Framework Decision 2006/960/JHA. For the sake of coherence with the analysis carried out on Article 39 of the CISA, the table below provides a comparison of the content of both mechanisms on spontaneous information exchange.

	Art. 46 of the CISA	**Council Framework Decision 2006/960/JHA**
Action	Exchange	Exchange
Object	Information	Information and intelligence
Purpose for the exchange	Not identified precisely, but the Contracting Party has to consider it useful to combat future crime and prevention of offences against, or threats to public policy and public security.	- Article 1: Conducting criminal investigations or criminal intelligence operations. - Article 7: There have to be factual reasons to believe that information and/or intelligence could assist in the detention, prevention or investigation of offences referred to in Art. 2(2) of the Framework Decision 2002/584/JHA.
Competent authorities	Not specified	National police, customs or other authorities that are authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities.

	Art. 46 of the CISA	Council Framework Decision 2006/960/JHA
Limitations	Not specified	Information and intelligence shall be limited to what is deemed relevant and necessary for the successful detection, prevention or investigation of the crime or criminal activity in question.

Table 13: Interrelationship between Article 46 of the CISA and Framework Decision 2006/960/JHA.

In this case, the object covered by the regulation of the Framework Decision 2006/960/JHA is even broader (information and intelligence) than the one from Article 46 of the CISA (information), but from another perspective, it is not clear, whether the provision of the information or intelligence without previous request can take place for the sake of any criminal investigations or criminal intelligence operation, or is limited only to the detention, prevention or investigation of offences referred to in Art. 2(2) of the Framework Decision 2002/584/JHA?

In the first case, the application of Article 46 of the CISA would be redundant; in the second case, it could be applied to combat future crime and prevention of offences against or threats to public policy and public security when they do not fall under Art. 2(2) of the Framework Decision 2002/584/JHA.

Within this topic, it is worth drawing attention to the changes that occurred in the SIRENE Manuals. Point 3.2.1b of the SIRENE Manual from 1985[421] established that the SIRENE Bureaux of the Contracting Parties can exchange any useful information whilst respecting national measures taken to implement Articles 39 and 46, and that it is an area of supplementary intervention of the SIRENE Bureaux. On the contrary, the SIRENE Manual from 2008[422] did not make any reference to the above mentioned articles, but established that "exchange of information under the SIS II legal instruments shall not prejudice the tasks entrusted to the SIRENE Bureaux by national law implementing other legal instruments of the European Union, in particular in application of the national law implementing Council Framework Decision 2006/960/JHA [...]."

Even more surprising is that the Commission, in its Communication of 2010, "Overview of information management in the area of Freedom, security and Justice"[423] did not make any reference at all to Articles 39 and 46 of the CISA; it only mentions the SIS.

[421] OJ L 8, 14.1.2003, p. 1-24.
[422] OJ L 123, 8.5.2008, p. 1-38.
[423] COM(2010) 385 final.

On the contrary, the International Centre for Migration Policy Development, in its Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments, has stated that "The SIS might be used as legal basis more often than it gets credit, as reference might still be made to Arts 39 and 46 of the Schengen Convention while Art 12 of the Swedish Framework Decision largely supersedes these two Articles."[424]

The current SIRENE Manual makes a step backwards and foresees that, "Additional tasks may be entrusted to the Sirene Bureaux, in particular, by the national law implementing Framework Decision 2006/960/JHA, Articles 39 and 46 of the Schengen Convention, in as far as they are not replaced by Framework Decision 2006/960/JHA".

Such obscurity and overlapping of the legal provisions is not a novelty, either at a national or international level. Nevertheless, in the case of Articles 39 and 46 of the CISA, it is very important as their application makes a part of the evaluations on the implementation of the CISA that take place every five years in each member of the Schengen area. This raises a question: How can countries be evaluated on something that is not clearly regulated by EU law, and is totally confusing in the Catalogue of Recommendations and other explanatory acts?

Without legal clarity at European level, Member States make different use of these Articles. For example, Italy presumes that Article 39 can be applied to provide the information following the match (hit) in the SIS. Hungary applies them in co-operation between law enforcement authorities of border regions, Poland uses it only in cases of offences that fall under Art. 2(2) of the Framework Decision 2002/584/JHA.

4. Police and Customs Cooperation Centres

Although neither the establishment, nor the functioning of bilateral or trilateral Police and Customs Cooperation Centres (PCCC) at common borders is directly foreseen in the CISA, they are one of the compensatory mechanisms for the abolition of control of internal borders.[425]

Nevertheless, its Articles 39(4) and 39(5) allow cooperation measures by bilateral (or trilateral) arrangements and agreements that give a possibility to make other

[424] INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT AND EUROPEAN PUBLIC LAW ORGANIZATION, "Study on the status of information…", loc. cit., p. 40.

[425] Since the very beginning, it should be pointed out that the topic of PCCCs has been almost abandoned and with little academic research.

co-operation arrangements as compensatory measures to be established, among which special attention deserves PCCC.

PCCC is a centre operative in border areas, usually in the premises of the former border checkpoint of one of the contracting parties (or in common premises if contracting parties have had common checkpoints), or in the immediate vicinity. Located in positions of strategic importance for observing cross-border crime, PCCCs play a key intelligence role for the operational services. As stated by del Moral Torres, it is a mechanism that has contributed to security improvements in border areas where the border control had been abolished but law enforcement services maintained exclusively by national competence.426

According to its nature, PCCC consists of representatives responsible for police, border and customs tasks in the border area. Representatives of the relevant services must be granted with the access to their national police and customs data bases that are used for prevention and detection of crimes. Working in common premises, they can rapidly exchange information on suspicious persons or vehicles in the border area (both by request and spontaneously), provide assistance to their national forces in the case of continuation of hot pursuit or urgent surveillance[427]

[426] DEL MORAL TORRES, Anselmo, *Cooperación policial en la Unión Europea: la necesidad de un modelo de inteligencia criminal eficiente* (Madrid: Dykinson, S.L., 2011), p. 184.

[427] Cross-border hot pursuit and cross-border surveillance are compensatory measures for the abolishment of border control, foreseen in Articles 40 and 41 of the CISA.
Article 40 previses a possibility to continue the surveillance started in one country of the Schengen area on the territory of its neighbouring country of the Schengen area, and Article 41 establish the same possibility for hot pursuit. Their main feature is the performance of law enforcement functions on the territory of the other country, with the general possibility (if it is not agreed to the contrary) to use official cars weapons and uniforms.
In the case of surveillance, two modalities are possible:
- Pre-planned surveillance – in which a permission of its continuation and / or take over is agreed in advance.
- Urgent surveillance – that happens unexpectedly (person or object of a surveillance were not expected to move towards the border) and the permission is asked "on the spot" of the operation. In this case, according to Article 40(2), surveillance shall be ceased when neighbouring country which territory was entered requests so or, where authorization has not been obtained in 5 hours after crossing the border.

In the case of hot pursuit, it is always unexpected and the permission to continue the pursuit is requested before the crossing of the border, or at the same moment. Hot pursuit is possible only over land borders and shall cease when the neighbouring country, whose territory was entered so requests.
Surveillance and hot pursuit are allowed in prosecution of any extraditable offence, evasion after an accident that has resulted in death or serious injury, escape from provisional custody or while serving a sentence involving deprivation of liberty.
In both cases, it is forbidden to enter into private homes and places not accessible to the public, and to use weapons in situations other that legitimate self-defence.
Surveillance and hot pursuit rules established in the CISA can be extended by bilateral agreement and in any case, it is up to bilateral agreements to establish the area (distance) or time for the surveillance and hot pursuit on the territory of the neighbouring country.

on the territory of neighbouring countries, and provide any other assistance that can be needed. As a rule, PCCCs should be open 24/7, but for the sake of the rational use of human resources, it is common to have only one duty officer 24/7.

It should be noted that PCCC is an effective cooperation tool in the border areas with a high density of towns and population, or even towns divided between countries and these PCCCs are mainly open 24/7. In less populated border regions there are part-time PCCCs (called by Hufnagel[428] "multijurisdictional police facilities"), or other compensatory measures, like in the case of the Lithuanian and Latvian border, where, in 2009, a bilateral decision to substitute PCCCs with Border Region Cooperation Model was taken (the same applies to the Lithuanian – Polish border).[429]

As noticed by Esain López, PCCC existed before the CISA, as in 1965, Spain and France signed the first agreement on National Offices of Juxtaposed Controls.[430] In 1969, Belgium, Germany and the Netherlands established Euroregional Police

Thus the allowed distance of pursuit between France and Spain is 10 km, between Portugal and Spain – 50 km or 2 hours, between Lithuania and Poland – 1 hour or 100 km, between Latvia and Lithuania – 1 hour.

[428] HUFNAGEL, Saskia, *Policing cooperation across borders: comparative perspectives on law enforcement within the EU and Australia* (Hampshire: Ashgate Publishing Limited, 2013), p. 189.

[429] After a joint Lithuanian-Latvian study visited the French-German PCCC in Kehl, it was bilaterally decided for the time being to not establish a PCCC, but to apply the Border Region Cooperation Model. A decision was taken in 2009 and was reasoned by lack of essential problems in cross-border cooperation, increasing the number of cross-border crimes or of insufficiency of existing cooperation means, as well as difficulties with financial and human resources caused by the global economic crisis. The Border Region Cooperation Model foresees that the main PCCC functions are performed by border area police forces. As a compensation for PCCC, the following are applied:

- Creation of bilingual forms for information exchange that in urgent cases, can be sent directly between competent authorities in border areas (informing about that the central authorities);
- Enhanced use of joint patrolling;
- Establishment of protocols that have to be followed in the case of cross border surveillance and hot pursuit;
- Exchange of radio communication means and frequencies, and facilitation of other communication means;
- Periodical meetings of different police units' representative in order to share information about crime situation in the border area and to prepare annual analysis;
- Annual organisation of joint training.

See Policijos Departamento prie Lietuvos Respublikos vidaus reikalų ministerijos ir Latvijos Respublikos valstybinės policijos išvados. "Dėl bendradarbiavimo pasienio regione modelio įgyvendinimo bei bendrų centrų steigimo", Biržai, 2009 m. vasario 19 d., accessed, February 3, 2013, http://www.policija.lt/index.php?id=2603.

A similar Border Region Cooperation Model is established for Lithuanian-Polish cooperation in the border area. See Policijos Departamento prie Lietuvos Respublikos vidaus reikalų ministerijos ir Lenkijos policijos vyriuasiojo komendanto ketinimo protokolas dėl kai kurių Lietuvos ir Lenkijos policijos bendradarbiavimo pasienio regione klausimų, 2012 m. spalis, accessed, February 3, 2013, http://www.policija.lt/index.php?id=2603.

[430] See ESAIN LÓPEZ, Roberto, *Cooperación policial transfronteriza (iniciativas, obstáculos y futuro)*, (Trabajo de investigación fin de CCACES, Aranjuez, 2010), p. 60.

Information and Coordination Centres. Within the CISA, the first model of PCCC and its agreement was concluded on French-German PCCC (Stasbourg-Kehl).

For the time being, there are 45 PCCCs, most of them full-time and some (like the one on the border between Lithuania and Poland (Budzisko) or Latvia and Lithuania (Kalviu)) part-time PCCCs or similar mechanisms.

Depending on geographical situation, there are bilateral and multilateral centres. The biggest centre in terms of the number of countries and institutions involved is the Belgian – French – German – Luxembourgish Centre, established in Luxembourg. Trilateral centres also see Austria, Hungary and Slovenia (Dolga Vas), Austria, Italy and Slovenia (Thörl-Maglern), Austria, Italy and Romania (Oradea), Belgium, the Netherlands and Germany (Heerlen).

PCCCs are also created with the countries of the Schengen area that are not EU Member States, e.g. The PCCCs of France, Germany and Switzerland (Basel), Italy and Switzerland (Chiasso), France and Switzerland (Geneva), Austria, Lichtenstein and Switzerland (Schaanwald).

Due to its nature in combatting cross-border crime, PCCCs can be also be established with the third neighbouring countries that are not members of the Schengen area. Such centres exist between Bulgaria and Serbia, Bulgaria and Macedonia, Moldova and Romania, Romania and Ukraine. The Bulgarian agreements with third countries deserve a closer look, as they are quite recent ones. Both agreements make specific emphasis on illegal migration, forgery of travel documents and ids, illegal trafficking and smuggling, crimes and violations related to motor vehicles. The functions of the PCCC consist of information exchange (including surveillance and control along the border) and elaboration of common risk analysis.[431]

They also foresee comprehensive data protection rules and exchange of classified data.

As pointed out by the Council of Europe "One of the main reasons for the creation of se centres was the finding that most international law enforcement structures, like Europol and Interpol, give priority to serious and organised crime. However,

[431] See Agreement between the Government of the Republic of Bulgaria and the Government of the Republic of Macedonia on Establishment and Functioning of a Common Contact Centre for Police and Customs Cooperation, accessed October 10, 2013, http://www.mvr.bg/NR/rdonlyres /41C16B10-5ECE-4969-9846-15EB33272EAE/0/Mac_4_EN.pdf.
Agreement between the Government of the Republic of Bulgaria and the Government of the Republic of Serbia on Establishment and Functioning of a Common Contact Centre for Police and Customs Cooperation, accessed October 10, 2013, http://www.mvr.bg/NR/rdonlyres /7BDDF080-4F74-43B0-BCFC-302805781A6C/0/finaltext_en.pdf.

trans-national criminality not only concerns organised crime but also thefts, burglaries and the like, which are often perpetrated by criminals who live less than twenty kilometres away from the scene of the crime."[432]

Although every bilateral or trilateral agreement can foresee different PCCC tasks[433], European Best Practice Guidelines for Police and Customs Cooperation Centres foresee 3 main functions:

- Information collection and exchange;[434]
- Assisting operations in border area;[435]
- Perform analysis of cross-border crime.[436]

According to the European Best Practice Guidelines for Police and Customs Cooperation Centres, "A PCCC's responsibilities must not encroach on those of the

[432] COUNCIL OF EUROPE. "Cross Border Cooperation in the Combating of Organised Crime" (Organised crime – Best Practice Survey nº 5, Strasbourg, January 2003), p. 14, accessed, October 16, 2013 http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/BestPractice5E.pdf.

[433] Thus the Council of Europe reveals more functions of PCCCs:
- Exchange and analysis of information;
- Enhancement of trans-national cooperation;
- Support to criminal investigations;
- Collaboration with requests for mutual judicial assistance;
- Cooperation in the coordination of operations;
- Conduction of common crime pattern analyses;
- Collaboration in educational matters regarding trans-national cooperation.

See COUNCIL OF EUROPE, "Cross Border Cooperation…", loc. cit., p 14.

[434] According to the "European Best Practice Guidelines for Police and Customs Cooperation Centres", (Council document 9105/11), information exchanged via PCCCs relates in particular to petty and moderately serious crime, illegal migration flows and public order problems. Nevertheless, bilateral and trilateral agreements can expand this scope. For example, Article 5 of the Convention between The Kingdom of Spain and The Republic of France on Cross Border Cooperation in police and customs matters, establishes that PCCCs serve cross-border co-operation, in particularly for the fight against illegal immigration, cross-border crime, prevention of threats to public order and illegal trafficking.

[435] It includes operations foreseen in the CISA (such as surveillance and hot pursuit mention in the footnote 432) and agreed among the neighbouring states (such as common patrolling, common operational measures or investigations, controlled deliveries, use of undercover officers, etc.).

[436] Analysis is mainly carried out for the law enforcement agencies of the border region, as well as for the authorities that develop security strategies and priorities for these territories and consists of:
- Follow-up of criminal events and offences taking place in the border region, falling within their competence, e.g. comparison of crime on both side of the border, identification of new risks;
- Identification of connections between events or present/past facts;
- Support to the coordination and to the follow-up of cross-border inquiries;
- On request, follow-up of specific groups of perpetrators and/or specific studies within the framework of specific phenomena;
- The relay between international, national, regional cross-border analyses.

national central units (in particular with regard to organised crime and terrorism) so as not to compromise the latter's competences and objectives."[437]

According to the Article 6(2) of the Framework, Decision 2006/960/JHA PCCC are obliged to provide exchanged information to Europol and Eurojust if its content falls within the competence of the agencies.

Nevertheless, "local" cases can be much more effectively and rapidly resolved by direct co-operation through PCCC, especially when bilateral or multilateral agreement allows the use of all legal measures and all communication forms allowed by national law in order to achieve PCCC's goals[438]; and as foreseen in Article 7 of the Agreement of 19th November 2005, between The Kingdom of Spain and The Portuguese Republic on cross-border co-operation in police and customs matters.

Due to the prompt process of information exchange, the most discussed question related to information exchange through PCCCs are the so-called "chain requests" between different PCCCs that take place in practice, but are not formally regulated. Let's imagine that Spain needs urgent information from Poland, and instead of sending a request to its central authority, a request is sent through the chain of PCCCs: Spain to Spanish-French PCCC, then to French-German PCCC and the latter to German-Polish PCCC.

For this reason, during the fourth PCCC conference in October 2013, it was proposed to foresee the possibility of "chain requests" in urgent cases, but only if allowed by bilateral / multilateral agreements and the national central authorities of the involved countries.[439]

From first sight, the process does not seem difficult, but if we take the already mentioned example of Spain – Poland information exchange, the possibility of a chain request shall be established in bilateral agreements between Spain and France, France and Germany, and Germany and Poland. Also, it is not clear which National central authorities should be informed: Only those of Spain and Poland or also those of France and Germany? The last option does not have too much sense, because it means the overloading of information (including personal data) for states that are used only as a chain (channel) for the information, but do not have any interest in its content.

[437] Council document 9105/11, p. 10.
[438] See MARTÍN DIZ, Fernando, "Aspectos recientes de la cooperación judicial y policial hispano-portuguesa; especial consideración del Acuerdo de Évora" in *Revista de Estudios Europeos*, 2010, no. 56, p. 103.
[439] See Council document 16249/13, p. 2.

France and Germany expressed their concern about this initiative, as an opening of a new channel for information exchange that has never been foreseen. Though France by itself is used by Guile as an example to illustrate such information exchange, "If the Spanish authorities need some information from their Italian counterparts, they will often go through the French authorities in the French-Spanish CPCC. Those in turn will contact their French colleagues in the French-Italian CPCC, who will then ask their Italian counterparts. Other countries which do not have CPCCs also use this network to get relevant information (for example, Andorra and the UK)."[440]

As Guille points out in his research, "Although central authorities were not pleased with this increasingly important networking system of information exchange through CPCCs[441], the high volume of exchanges demonstrated that this network of CPCCs responded to real needs, and therefore the central level informally allowed this information exchange to take place to a certain extent".[442]

It could be concluded that due to their typical functions, PCCCs contribute to common and agreed responses to crime in countries that share borders. All this is possible due to the face-to-face work of police, border and customs authorities which allows, on a daily basis, familiarisation with the legal system of neighbouring countries and so to find out the best possible solution to common security challenges.

5. Liaison officers: within the Schengen Agreement and beyond

Collins Dictionary defines "liaison officer" as a person who liaises between groups or units. [443] In the case of international co-operation, a law enforcement authority liaison officer is an officer delegated to another country or region, to keep close contact with its law enforcement and judicial authorities, to facilitate contact and cooperation between sending and hosting countries, or sending country and region. Liaison officer can also be sent to international or regional organisations; the most important examples of such organisations are INTERPOL and Europol, which funding legislation establish that, in the case of INTTERPOL, its members can, and in case of Europol, its members shall, delegate liaison officers.

[440] GUILLE, Laure, "Policing in Europe: An Ethnographic…", loc. cit., p. 267.
[441] It has to be noted that in some research, "Police and Customs Cooperation Centres" are called "Centres for Police and Custom Cooperation", although the official name used by the European Union is "PCCC".
[442] GUILLE, Laure, "Policing in Europe: An Ethnographic…", loc. cit., p. 267.
[443] Collins, English Dictionary, accessed October 16, http://www.collinsdictionary.com/dictionary/english/liaison-officer.

Liaison officers were used for the first time at the turn of the XIX and XX centuries, during the Anarchist era, in order to share information and to counter cross-border political concerns; later, they started to be used to combat drug trafficking.[444]

Within the Schengen Acquis, Article 47 of the CISA foresees a possibility to conclude agreements for the secondment of liaison officers to another state of the Schengen area, as well as to the third countries. Although this article mentions secondment "to the police authorities of another Contracting Party", it has to be interpreted more broadly than just the police, and to be understood as law enforcement authorities that have the function of combatting crime and ensuring internal security within the Schengen area.

In parallel with the CISA, the interior ministers of the Member States of the European Community had started discussions on liaison officers within the TREVI group and:

- In 1987, Agreement on the development of a network of drugs liaison officers was adopted, to the benefit of European Community Member States.
- In 1996, the Council adopted Joint action 96/602/JHA of 14th October 1996, on the basis of Article K.3 of the Treaty on the European Union providing for a common framework for the initiatives of the Member States concerning liaison officers (hereinafter – Joint action 96/602/JHA).[445]

While Joint action 96/602/JHA talks about both intra-community liaison officers and those seconded to third states, the Council Decision 2003/170/JHA of 27th February 2003 on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States[446] (hereinafter – Decision 2003/170/JHA) that repeal it, envisages only posting and common use of liaison officers in third countries and international organisations[447]. Thus it seems that the political signal is to use this cooperation tool with the third countries, leaving the cooperation within the EU under the auspices of other cooperation instruments.

---

[444] See YON, Hasan, "Police liaisons as builders of transnational security cooperation" in AYDINLI Ersel, *Emerging Transnational (In)Security Governance: A Statist-transnationalist approach* (Routledge. New York. 2010), p. 137.

[445] OJ L 268, 19.10.1996, p. 2-4.

[446] OJ L 67, 12.3.2003, p. 27-30.

[447] Decision 2003/170/JHA provides us with the following definition of the liaison officer "A representative of one of the Member States, posted abroad by a law enforcement agency to one or more third countries or to international organisations to establish and maintain contacts with the authorities in those countries or organisations with a view to contributing to preventing or investigating criminal offences."

Nevertheless, Decision 2003/170/JHA does not repeal the provisions of the CISA on the secondment of liaison officers among Schengen countries.

The figures on liaison officers posted abroad also show that despite modifications brought about by the Decision 2003/170/JHA, Member States still delegate a lot of them within the EU and Schengen area. The table below presents figures on EU Member States liaison officers posted abroad during the last six years.[448]

	2009	2010	2011	2012	2013	2014	2015
EU, Andorra, Iceland, Norway and Switzerland	210	233	229	229	227	222	212
Central and Eastern Europe	116	120	126	125	116	105	106
Africa	74	87	78	80	84	83	85
Asia Pacific	44	45	43	42	44	41	41
South Asia	18	22	20	20	20	21	20
Middle East	29	28	28	28	30	30	30
Americas	81	88	89	89	93	94	95

Table 14: Figures on liaison officers posted abroad by the EU Member States.[449]

As can be deduced from the table, the figures do not vary a lot and the biggest "jump" in the number of liaison officers posted within the EU was from 210 to 233 between 2009 and 2010; but there is no country or region with a more significant rise in number. The increases in each country resulted in the posting of between one and three more liaison officers. The biggest increase is related to the number of liaison officers in the Netherlands, but it has to be taken into account, that the Netherlands hosts Europol's Office, and liaison officers seconded to Europol are also accredited to the Netherlands, even if they perform their main functions within the framework of Europol.

In 2013 the decrease in the number of liaison officers seconded to Central and Eastern Europe can be explained by the accession of Croatia to the EU and a decrease in the number of countries which remain outside the EU in this region. In the case of the year 2014, the decreasing tendency was noticed in this region as well, but not in any country in particular. The biggest reduction (3 liaison officers) took place in Russia.

[448] 2009 as the beginning is taken not by chance, as it starts a relevantly stable period without bigger changes that could have a significant impact on the secondment of liaison officers, for instance 2004 with the accession of 10 new Member States to the EU, 2007 with the accession of Bulgaria and Romania and the extension of the Schengen area by 9 new members. The only significant factor during the elected period 2009-2015 had been the global economic crisis and this could determine opting for "cheaper" cooperation tools.

[449] Compiled by author from Council documents 10504/2/09, 16389/10, 16560/1/11, 16686/12, 13129/13, 11996/14, 10597/15.

In 2015, a decrease in the number of liaison officers posted to EU Member States can be observed; however, closer analysis reveals that per country, the number normally varies by one or two liaison officers.

Decision 2003/170/JHA concentrates on the most efficient, common use of the liaison officers seconded to the third countries, and in Article 5 foresees the possibility for law enforcement institutions of the Member State that does not have them in the third country, to request liaison officers from another Member State, with a view to the exchange of relevant information. It also establishes meetings between all Member States' liaison officers posted in third countries or international organisations; and with the amendment of the Decision 2003/170/JHA made by the Council Decision 2006/560/JHA on 24th July 2006, amending Decision 2003/170/JHA on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States[450] (hereinafter – Decision 2006/560/JHA), previses that such meetings are organised by the Member State holding the Presidency of the Council or the European Union or on the initiative of Member States with liaison officers posted there or, as a novelty, by the Member State to which responsibility for coordination (leading) of the EU cooperation in a particular country or region has been given. The outcomes of meetings are discussed in the preparatory bodies of the Council of the European Union, and serve as indispensable input for the policy in judicial and home affairs cooperation with third countries.

Not all third countries or regions have leading Member States, because a Member State by itself has to offer to perform such a role. For the time being, Italy has accepted (and was granted) the responsibility to coordinate EU Member States' liaison officers in China, the Central Asia Region and Kosovo. Austria has a leading role in the Republic of Moldova and France - in West African countries.[451]

Decision 2006/560/JHA also foresees information exchange between Member States' liaison officers in the third countries and Europol, as well as between Member States' law enforcement institutions and Europol's liaison officers posted in third countries.[452]

Going back to the CISA, its Article 47 does not entail any special scope of action by liaison officers, establishing that the purpose is to combat crime by means of both prevention and law enforcement. In the case of Decision 2003/170/JHA, its recital 15 establishes the aim to regulate questions relating to the fight against serious cross-border crime.

[450] OJ L 219, 10.8.2006, p. 31-32.
[451] Council document 11996/14, p. 5.
[452] Europol has its liaison officers at INTERPOL's headquarters in Lyons (France) and Washington (United States of America).

García Vázquez states that liaison officers do not perform operational activities in hosting country, but increase the effectiveness of police co-operation by collection and exchanging information.[453]

But even without operational activities, their role is much more significant and comprehensive than just information exchange.[454] As pointed out by Block, "Requests for information, usually referred to as 'cases', are likely to be routed through liaison officers instead of through the other available channels whenever a case requires more active support than a simple information-exchange because of its complexity, sensitivity or urgency."[455]

The biggest advantage of the liaison officer in information exchange is his / her familiarity with the system and personal contacts with the law enforcement authorities of the hosting country. Also, knowledge of the language and cultural particularities play an important role in "breaking the ice" and smoothing contacts with representatives of the hosting country, region or organisation. Depending on the situation and needs, liaison officers have the possibility to manoeuvre between using personal informal contacts, or more official ones within the authorities of the hosting country.

Despite increasing transnational cooperation, a lot of law enforcement authorities are quite "possessive" and "jealous" about the information they have, or the operations they perform, and do not tend to share it with the rest. But a physical presence and the possibility of establishing "face to face" contacts very often facilitates exchange of information, as it enhances mutual trust between officers. Face to face contact especially helps in sensitive cases and operations, as it allows the discussion of some aspects or questions "out of records", "making deals" and finding the best solution for everybody.

H. Yon defines liaison officers as "masters of informal cooperation practices" and says, "Informal cooperation eases up the process of communication about particular cases and developments within them. During informal communication with counterparts, police liaison officers share their experiences. During those information exchanged both parties give each other information about what is going on in cases, what kind of developments they are seeing in criminal strategies and are able to share ideas about specific problems."[456]

---

[453] See GARCÍA VÁZQUEZ, Sonia, "La cooperación policial y judicial…," loc. cit., p. 433.

[454] See INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT AND EUROPEAN PUBLIC LAW ORGANIZATION, "Study on the status of information…", loc. cit., p. 60.

[455] BLOCK, Ludo, "Bilateral Police Liaison Officers: Practices and European Policy" in *Journal of Contemporary European Research*, 2010. vol. 6, issue 2, p. 196, accessed October 16, 2013, http://www.jcer.net/ojs/index.php/jcer/article/view/266/205.

[456] YON, Hasan, "Police liaisons as builders…", loc. cit., p. 132-133.

According to Article 47 of the CISA, it is prohibited for liaison officers to take independent police action on the territory of a hosting state, or, in other words, they do not have the power to investigation in the jurisdiction where they are posted.[457] Although there is no other legal act referring to that prohibition, it is understood *per se*, that the mission of the liaison officer is to establish and maintain contacts for the exchange of information, and to facilitate cooperation.

6. Data protection

As already mentioned in subsection 4.3.3.1 of the Chapter II, the general data protection framework established in Decision 2008/977/JHA is not applied to the Schengen Information System, neither to SIS and or to SIS II. With respect to other information exchange under Schengen Acquis, such as through PCCCs, liaison officers, the aforementioned Decision is applied as *lex generalis* and *lex especialis* can be included in bilateral or multilateral agreements that regulate PCCC and or liaison officer as well as the national law of the Member States involved.

Thus the data protection system applicable to SIS is complicated, fragmented and includes both *lex generalis* and *lex specialis.* [458]

Lex specialis for SIS data protection previously was included in Chapter III of Title IV of CISA, and is actually regulated by Decision 2007/533/JHA and Regulation 1987/2006. *Lex generalis* applied for alerts regulated by the aforementioned Regulation are Directive 95/46/EC and Regulation 45/2001 of the European Parliament, and of the Council of 18th December 2000 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[459] ; for the rest of alerts – European Convention on Data Protection.[460]

[457] BLOCK, Ludo, "Bilateral Police Liaison…", loc. cit., p. 196.

[458] See Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)230 final); the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)236 final), and the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005)237 final), OJ C 91. 19.4.2006, p. 41.

[459] OJ L 8, 12.1.2001, p. 1-22.

[460] See GARCÍA SÁNCHEZ, Manuel, "El Sistema de Información Schengen: estructura, funcionamiento y evolución del sistema de supervisión conjunta en protección de datos" in GOIZUETA VÉRTIZ, Juana; GONZÁLEZ MURUA, Ana Rosa and PARIENTE DE PRADA, Iñaki, *El Espacio de Libertad, Seguridad…*, op. cit., p. 229.

Despite such complexity, a system could be acceptable if it did not lead "either to discrepancies between national regimes on fundamental aspects, or to a watering down of the present level of data protection."[461]

Thus this Section sets out to establish the level of data protection provided to such a wide centralised data base. Due to the scope of this research, in the following subsections only data protection related to alerts for crime prevention and investigation will be analysed.

However, before starting, few general remarks should be made.

First of all, according to Article 56 of Council Decision 2007/533/JHA and Article 40 of the Regulation 1987/2006, the processing of sensitive data in SIS is prohibited; this is understood in different ways.

In the case of Council Decisions, sensitive data is understood within the meaning established by the first sentence of Article 6 of the European Convention on Data Protection, i.e. Racial origin, political opinions or religious or other beliefs, health or sex life. Nevertheless, unlike the above mentioned Convention, SIS II can include processed data on criminal convictions.

In case of Regulation – as is foreseen in Article 8(1) of Directive 95/46/EC and in addition to the categories of sensitive data mentioned previously it also includes trade-union membership, but on the other hand, it talks only about religious or philosophical beliefs and not about beliefs in general.

Secondly, Schengen acquis does not foresee any processing of classified information. It raises some questions given that since 2005, SIS II can include counter-terrorism information.[462]

6.1. Persons included

Each category of alerts held in SIS directly indicates persons or objects to which it is applied. Thus SIS consists of the following alerts on persons:

- Wanted for surrender, i.e. Prosecuted or convicted;
- Missing or in need of special protection due their physical or mental condition;
- Sought for assistance in judicial procedure;
- Needed to be checked;

[461] Ibid, p. 39.
[462] O'NEILL, Maria, "The Issue of Data Protection…", loc. cit., p. 226.

- Not allowed to enter one of the members of the Schengen zone;

Less specified is the last category of persons, as each State may apply different criteria to decide on whether he or she is not allowed to enter its territory. But as commented previously, this type of alert is not an object of this research due to its dissociation from investigation into crime. In addition to predetermined types of alerts, Article 51 of the Decision 2007/533/JHA and Article 36 of Regulation 1987/2006 allow the inclusion of data on persons whose identity was misused. But unlike other categories of persons, for such data inclusion the consent of the data subject is needed, and there is a complete list of data that can be entered to the SIS II. Therefore, only the following data on a person whose identity was misused can be processed: names and surnames, data and place of birth, sex, nationality, photographs, fingerprints, any specific and permanent characteristics and number of identity documents.

According to Articles 44.1 and 45.1 of Decision 2007/533/JHA, alerts are stored for the period that is necessary to achieve their purpose. But in any case, the State that has issued an alert shall make a revision on such a need and inform C.SIS if it is necessary to store it longer. If the State does not communicate such a need, an alert is automatically deleted after:

- 1 year if it concerns discreet or specific check of person;
- 3 years – other alerts on persons;
- 5 years – discreet or specific check of object;
- 10 years – other alerts on objects.

The SIRENE office shall delete data exchanged in relation to an alert as soon as the purpose of its transfer has been achieved, and in any case, not later than one year after the deletion of the alert. This provision can be criticised because of the meaninglessness and purposelessness of keeping data when an alert to which it is related has been deleted. Besides, from a practical point of view, it is much easier to delete data related to an alert once it is withdrawn from the system, than to remember it within one year.

6.2. Access

As mentioned before, according to Article 40 of Decision 2007/533/JHA, access to SIS II is given to law enforcement authorities, i.e. Police, border guards and customs, vehicle registration certificates as well as Europol and Eurojust (within the scope that is necessary to perform their mandate). When it is allowed by the national legislation, judicial authorities participating in investigations and their coordinators can also be granted an access.

Regarding Europol and Eurojust and their "fishing expeditions" in SIS II, it was proposed to restrict their access only to data about individuals and objects that have already been included in their own files. From one perspective, this proposal seems reasonable, but from another it lacks mechanisms of effective control, given that the search in SIS II has really been made on a person or an object that is already included in the files of these agencies.

Talking about persons having access to the SIS II data, each of them shall fulfil national rules of confidentiality. At SIRENE level, usually this would be equivalent to having security clearance and at other levels – the duty to maintain professional secrecy. Breach of secrecy, depending on its severity, can result in disciplinary or criminal responsibility.

According to Articles 12, 18, and 41.4 of Decision 2007/533/JHA, all access to and exchanges of personal data shall be recorded and shall include "the history of the alerts, the date and time of the data transmission, the data used to perform a search, a reference to the data transmitted and the name of both the competent authority and the person responsible for processing the data."

Its Article 16 establishes Management Authority (since May 2013 is eu-LISA) controls access (including facilities and persons) and processing (including input, communication and storage).

6.3. Third parties

As a general rule established in Article 54 of the Decision 2007/533/JHA, data from SIS II cannot be transferred to third parties, meaning neither countries nor organisations. The only permitted exception is data submission to the Interpol database on stolen or missing travel documents (Article 55). Such transfers include only data on the type of stolen, lost, invalid or misappropriated document, its number and issuing country, and can be performed only with the following conditions:

a) Interpol and the European Union sign relevant agreement;

b) Issuing Member States gives a consent for such transfer;

c) Data shall be accessible only to those Interpol members (third countries) that provide with the relevant data protection level.

Such provision is useful for those countries that do not have a system that allows submitting the same information to a different database. Those who have such a system do not need an application of the Article 55 as introducing information into

its own system, a competent authority from the same interface chooses in which data bases it wants to announce an alert: national, SIS, Interpol, and so on.

For the time being, this provision is not applicable as the relevant agreement between Interpol and the European Union has not been singed. And due to the technological developments and constant updates of national data processing systems, it probably it will be not needed.

6.4. Data subject's rights

Article 49 of Decision 2007/977/JHA establishes Member State's responsibility for the accuracy of entered data and its correction.

Its Article 58 entails data subject's right of access, deletion and correction, but more specific regulation on implementation of this right is left to the national legislation of each Member State. The European legislator foresees only two restrictions:

- Access shall be denied if it necessary to the performance of tasks related to an alert, or in order to protect the rights of third parties.
- If a request is related to data submitted to SIS II by another Member State, it has to be consulted before an answer being given to the data subject.

Replies shall be provided within the deadlines foreseen by the national law of the requested Member State, but not later than within sixty days in cases of implementation of the right to access, and within three months in cases of implementation of the right to deletion or correction. This is a novelty of the SIS II legal basis in comparison with the previous one that did not envisage any deadlines for replies.[463]

As all N.SIS are identical reflections of C.SIS, the data subject can file a request in any Member State.[464]

The majority of Member States (e.g. Austria, Bulgaria, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Malta, the Netherlands, Norway, Poland, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom) provide direct access, meaning that the data subject can address his or her request directly to the competent authority that

[463] See BROUWER, Evelien, "The Other Side of Moon: The Schengen Information System and Human Rights: A Task for National Courts" (Working Document No. 288, Centre for European Policy Studies, April 2008), p. 4, accessed October 20, 2013, http://www.ceps.eu/publications/other-side-moons-schengen-information-system-and-human-rights-task-national-courts.

[464] RECUERO, Paz, "La protección de datos y Schengen: Una visión…", loc. cit., p. 213.

handles the data. Very few Member States (e.g. Belgium, Luxembourg and Portugal) apply indirect access, meaning that the data subject has to address the request to the national supervisory authority (independent data protection institution).[465]

France and Hungary apply a mixed access system and based of different principles.

In the case of France, access depends on the category of alert, i.e. Direct access is granted in relation to alerts on persons being searched for in relation to family reasons, minors and those that are referred to in alerts on stolen vehicles. In the case of the remaining alerts, indirect access is used. In Hungary, a request can be addressed both to competent and supervisory authorities, but finally the national SIRENE office deals with all of them.[466]

The system applied by France seems confusing as it can be applied only when a person knows what kind of alert is issued in relation to him or herself. And without such knowledge, the person will need to use both mechanisms.

6.5. Supervising authorities

To ensure the application of data protection, as with any fundamental right, there is a need for a control mechanism.

As SIS II consists of central and national systems, its supervision is divided between national and European authorities.

The European Data Protection Supervisor performs supervision at EU level. Controls can be performed in respect to some category of alert, data or specific basis or complaint, but in any case, at least once every four years, a comprehensive audit of eu-LISA's data processing activities is performed. Its first audit took place at the end of 2014, but the report is still not publicly available.

To control data processing within N.SIS and SIRENE, each Member State has to nominate a national, independent, supervising authority. As with the European Data Protection Supervisor, in performing their functions, national supervisory authorities shall perform comprehensive national auditing at least every four years, and also on an ad hoc basis when necessary.

---

[465] See SIS SUPERVISION COORDINATION GROUP, "A Guide for Exercising the Right of Access", October 2014 (updated October 2015), p. 11-29, 33-38, 41-89, accessed November 3, 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Large_IT_systems/SIS/15-10-12_SIS_II_GUIDE_OF_ACCESS_UPDATED_2015_EN.pdf

[466] See SIS SUPERVISION COORDINATION GROUP, "A Guide for Exercising the Right…", loc. cit., p. 30, 39.

To ensure smooth and equal data protection, the European Data Protection Supervisor and national authorities have to co-operate and meet at least twice a year.

7. Brief summary and evaluation

Although the direct objective of the multilateral Schengen agreement, the CISA and its incorporation into the EU legal system as Schengen acquis, is the free movement of persons and goods within the Schengen area, it is the pioneer tool of the police and judicial co-operation; it is the first, and for the moment the last, so the comprehensive legal framework that regulates the centralised data base, its supporting offices and data protection, information exchange and other non-data base assistance; the setting up a network of co-operation officers and units, as well as cross-border actions, do not have equivalents.

Despite widely the prevalent consideration of the EU and Schengen area as an equal geographical territory, it should be realised that some EU countries are not members of the Schengen zone (Bulgaria, Croatia, Cyprus and Romania), some EU countries are only participating partially (Ireland and the United Kingdom), some countries belonging to the Schengen zone are not Member States of the EU (Iceland, Lichtenstein, Norway and Switzerland).

Despite criticisms of being a "Big Brother" tool, regulation of the SIS followed by SIS II is one of the most comprehensive regulations which has ever existed at international level, with precise foreseeing of data categories that can be exchanged, and the prohibition of exchange sensitive data.

With respect to rights to privacy and data protection, the Schengen agreement, the CISA, incorporation of the Schengen acquis through the primary law of the EU (Treaty of Amsterdam), later joining the Schengen area by third countries, required ratification by the national parliament of each country, and therefore can be treated more as a fulfilment of the legality criteria for restriction of the above mentioned fundamental rights.

Its purpose also seems to be justified as the abolition of control on internal borders has meant increased danger to public safety, and compensatory measures used on external borders and within the area of free movement were, and still are, needed.

With respect to proportionality criteria, SIS II includes alerts on limited categories of persons and objects. The inclusion of persons wanted for extradition or surrender is totally justifiable and proportional to public safety and combatting crime. Missing persons, or those needing special protection due their physical or

mental conditions, generally do not present a direct threat to public safety. But public authorities are responsible for their safety (especially in the case of minors) and abolition of the control of internal borders makes this responsibility difficult to exercise and therefore requires some additional measures. The introduction of persons sought for assistance in judicial procedure can also be justified as their detection allows the performance of justice and in some cases, the prevention of malicious avoidance of it and in further cases, making a person aware of his or her inclusion in it.

More problematic are alerts on persons that have to be checked, as it is not established to what extent information should be gathered and processed, and it could, therefore, mean interference into personal and family life. This situation could be avoided by indicating in the alert, which precise information is needed, for example only the itinerary of his or her journey, means of transport used, and so on. Creating the linking of alerts allows the checking officer to pay attention to those persons who are also alerted, but who do not interfere with information of the rest.

Although SIS II is equipped with its *lex especialis,* in relation to data protection that is quite comprehensive, taking into account the existence of other centralised data bases and the creation of *lex generalis* for all data exchange within the area of police and judicial co-operation, it would be more coherent to apply it to SIS II as well, and to ensure the application of the same standards to all data bases. *Lex especialis* could be used for those aspects not regulated by *lex generalis*, for example control measures that have to be taken at national level in relation to N.SIS.

In terms of clarity and difficulty of application, the Schengen acquis and its further development can be defined as a quite clear mechanism, although complicated in terms of establishment (e.g. Creation of SIS II, establishment of PCCCs).

The greatest problem causes a perfunctory approach in the creation of new mechanisms, overlapping with already existing regulations, and demonstrates the need for a philosophy foreseen in the IMS and the Stockholm Programme to revise existing cooperation and other instruments before the creation of new ones.

CHAPTER 4:
EUROPOL

The second object of this research is the European Police Office (hereinafter – Europol), nowadays an EU agency that aims "to support and strengthen action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy."[467]

The establishment of Europol's predecessor dates back to the beginning of the nineties, but due to the changes introduced by different modifications of TFUE throughout the decades, both to the Europol's status and the area of security, liberty and justice, the legal regulation of Europol is still under development. The last modifications introduced by the Lisbon Treaty (Article 88(2) of the TFEU) foresee an obligation to adopt the regulation that determines the Agency's structure, operation, field of action and tasks.

The Proposal of the 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[468] (hereinafter – Draft Europol Regulation) was presented by the Commission on 27th April 2013, but is still under the legislative procedure. The Council of the European Union and the European Parliament have finished the first reading and now, due to numerous modifications proposed to the original draft by both institutions, are in the stage of trilogues (the analysis of the Draft Europol Regulation is presented in the part "Projects in the pipeline").

Before entering into an analysis of Europol's role in information exchange, there is a need for a clear definition of its competence.

[467] Article 88.2 of the TFEU.
[468] COM(2013) 173 final.

Although one can encounter comparisons between Europol and the European FBI, federal police, or ascribing to it executive powers, its main objectives are information exchange, threat analysis, technical assistance to national law enforcement institutions and training.

As pointed out by Bures, Europol, "Is not an executive police force with autonomous supranational authority to conduct its own investigations, undertake searches, or arrest suspects."[469]

From the very beginning, Germany was in favour of endowing Europol with the same coercive and executive competence as the *Bundeskriminalamt*[470], but there was little support for this idea from other Member States, and the focus was on the improvement of the information flow. Thus, "Without Member State-level follow-up, Europol's work cannot be translated into action and results."[471]

As stated by Fijnaut, "While the integration of the 1990 Schengen Convention can be described as bottom up cross-border operationalization of police co-operation in the EU, the intention to include Europol more closely - in particular through joint teams – in criminal investigations of Member States in the field of organized crime can be called a top down attempt at cross-border operationalization of the actions [...]."[472]

The following sections will present development of Europol, its role in information exchange and its future. The emphasis will be on very important, specific and arguable issue, i.e. Europol's right to exchange information with third parties (third states and international organisations).

1. From ministerial agreement to regulation by the TFEU

The idea to create a police entity at European level dates back to the beginning of the informal, intergovernmental co-operation within the TREVI, where from time

[469] BURES, Oldrich, "Europol's Fledging Counterterrorism Role" in *Terrorism and Political Violence*, 2008, vol. 20 (4), p. 501.

[470] This idea was strongly supported by the Germans. For example, German Chancellor Schröder proposed to transform Europol into a European police force with the same coercive and executive competence as the *Bundeskriminalamt*. See STORBECK, Jürgen, "La cooperación policial europea", loc. cit., p. 167; BENYON, John, "Policing the European Union…", loc. cit., p. 500.

[471] DISLEY, Emma; IRVING, Barrie; HUGHES, William et al., "Technical report on Evaluation of the implementation of the Europol Council Decision and of Europol's activities makes a majority of information exchange", Cambrige: RAND Corporation, 2012, p. 51, accessed December 4, 2014, https://www.europol.europa.eu/content/publication/evaluation-implementation-europol-council-decision-and-europol's-activities-1655.

[472] FIJNAUT, Cyrille, "Police Co-operation and the Area…", loc. cit., p. 249-250.

to time, informally different visions of possible common law enforcement co-operation body were raised.

Some modest ideas were suggested with competence limited to some categories of crime. The most political and ambitious one sought to become more independent from information and intelligence gathered by the Unites States.[473]

Nevertheless, it took 15 years for the proposal to create a European police entity to be approved by German Chancellor Helmut Kohl at the highest political levels of the European Council of 28th-29th June 1991, where the TREVI ministers were asked to submit a report on the possible development of a central European criminal intelligence office. After prompt reception of the report, the Summit of 9th-10th December 1991 agreed on the establishment of the European Police Office, beginning with its drug intelligence unit.

A few months later, Article K1(9) of the Treaty of Maastricht on European Union foresaw that one of the areas of common interest would be, "Police co-operation for the purposes of preventing and combating terrorism, unlawful drug trafficking and other serious forms of international crime, including if necessary certain aspects of customs co-operation, in connection with the organization of a Union-wide system for exchanging information within a European Police Office (Europol)."[474]

Although the Treaty was signed on 7th February 1992, it was obvious that its ratification would take some time and that it would take longer to agree on a Convention that would regulate Europol's mandate and activities.

1.1. Ministerial agreement

Taking into account the seriousness of the drug threat to the European Communities, and realizing the time needed for the preparation and ratification of the Convention on Europol, TREVI ministers decided to start with the Ministerial Agreement on the Establishment of the Europol Drug Unit that was signed on 2nd June 1993 in Copenhagen.

Consequently, a non-operational team of the liaison officers of all the participating countries were sent to the EDU headquarters for the establishment of intelligence exchange and analysis was. The EDU's mandate was limited to actions where the crime or organized group affected two or more Member States. Each liaison officer

[473] See BIGO, Didier, "EU Police Cooperation: National Sovereignty Framed by European Security?" in GUILD, Elspeht and GEYER, Florian (eds.), *Security versus Justice?...*, op. cit., p. 94.
[474] OJ C 191, 29.7.1992, p. 61.

had to perform his or her duties according to the national regulation, including that on data protection. The agreement entailed only the following data exchange and protection rules:

- All information exchange takes place on a bilateral basis between requesting and requested states.
- If information related to the request has other than the requested state, this information can be transmitted to the requesting state only by that other state, and not by the requested one.
- It is not allowed to transmit personal data to the non-Member State, or to any international organisation.
- No personal information can be stored centrally in the EDU.
- National data protection authorities supervise the activities of their liaison officers.

Despite giving the first initiative towards a European police co-operation institution, the ministerial agreement had been far from sufficient to establish a full time functioning international office (defining its structure, competences, responsibility, accountability, maintenance, etc.) And therefore, two weeks later,[475] the Summit of Brussels determined that the Ministerial Agreement should be replaced by a Convention on Europol before October 1994.[476]

1.2. Europol Convention

Despite the established deadline, Europol had been in "embryonic existence"[477] for over five years, as ratification of the Convention signed in 1995 lasted until mid-1998, and Europol only replaced the EDU from 1st July 1999.

Meanwhile, as indicated by the Report on the Organised Crime Situation of the Council of Europe, Albania, Czech Republic, Denmark, Greece, Hungary, Finland, Island, Latvia, Lithuania, Slovenia, Sweden and Turkey had between 25 and 100 organised groups; Macedonia, former Yugoslav Republic of Macedonia, Moldavia, the Netherlands and Slovakia between 100 and 200; Poland, Spain, Switzerland and Ukraine between 200 and 500; Germany, Italy, Romania, the Russian Federations and United Kingdom – more than 500.[478] A large number of them took advantage of free movement to get around with their activities and international

[475] On 10-11 December 1993.
[476] See BRUGGEMAN, Willy, "Europol and the Europol Drugs Unit: Their Problems and Potential for Development" in BIEBER, Roland and MONAR, Joerg *Justice and Home Affairs in the European Union. The Development of the Third Pillar,* (Brussels: European Interuniversity Press, 1995), p. 220-221.
[477] PEERS, Steve, *EU Justice and Home Affairs…,* op. cit., p. 931.
[478] COUNCIL OF EUROPE, "Report on the Organised Crime…", loc. cit., p. 25.

police co-operation, and relevant measures were indispensable in order to combat this spreading phenomenon.

As had been supposed, the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office[479] (hereinafter - Europol Convention) expanded the scope of action foreseen for the EDU, establishing as Europol's objective the prevention and combatting of terrorism, unlawful drug trafficking and other serious forms of international crime when they affect two or more Member States. It had foreseen some kind of transitional period until full functioning: Europol had to start with the prevention and combatting of crimes of trafficking in drugs, human beings, nuclear and radioactive substances and motor vehicles as well as illegal immigrant smuggling, and after two years of functioning to also cover terrorism and other crimes, if decided by the Council. In all cases, Europol's competence included money laundering and other criminal offences related to the above mentioned forms of crime.

1.2.1. New Information Processing and Exchange Scheme

Compared with the EDU, Europol had the right to maintain a computerized system of collected information, and to notify Member States about information possessed which was related to them.

The information exchange scheme became the following:

- Every Member State has only one liaison body between its competent authorities and Europol – national unit (hereinafter – ENU);
- Every Member State sends at least one liaison officer to Europol's headquarters in order to maintain contacts and forward information between Europol and its ENU. They represent the Member State and their mission is "to watch over the defence of Europol National Unit's interests respecting provisions of national law and those related to Europol's functioning."[480]

From another perspective, it should not be forgotten that representing its ENU and Member State liaison officer is a first contact point and aid for other Member States, and can directly provide other liaison officers of other Member States with information from databases to which he or she has access, to consult the national rules and possibilities of co-operation, and so on.

[479] OJ C 316, 27.11.1995, p. 1-32.
[480] ARROYO ROMERO, Francisco Javier, *La influencia de EUROPOL en la comunitarización de la policía europea* (Madrid: Akal, 2006), p. 40.

The Europol Convention, equal to other instruments, did not endow Europol with the application of coercive measures. As explained, the first Europol director STORBECK, Europol "is not authorised to perform either telephone tapping, or searches or detentions or other types of police measures that seldom violate citizens' fundamental rights and therefore in addition to the requirement to be performed in conformity with relevant legal provisions, they have to be subject to the supervision of a prosecutor or other democratically competent institution."[481]

The third Round of Mutual Evaluations[482] has shown that Member States are not in favour of granting it operation activities, but to strengthening analytical ones,[483] which by some authors such as Arroyo Romero, is seen as a lack of real efficiency of Europol.[484]

In 2005, Europol information system (hereinafter – EIS) was created containing information contributed by Member States in compliance with their national procedures, and received by Europol from third parties.

With respect to the content of the EIS, it was allowed to process data on:

- Persons suspected of already committed crime that is subject to Europol's competence or accomplices;
- Persons suspected in future commission of such crime;
- Committed crimes, *modus operandi;*
- Convicted persons.

Direct access to the EIS was provided to ENUs, liaison officers and authorised Europol staff.

A possibility was also established by the agreement of two thirds of the members of the Management Board to create thematic[485] data (work) files, also called Analysis Work Files (hereinafter - AWF). The rules of authorisation to open AWFs were modified by the Protocol drawn up on the basis of Article 43(1) of the Convention on the Establishment of a European Police Office (Europol Convention). Instead of a mandate of the authorization to open AWFs, the Management Board was endowed with the right to close it. Thus Europol (the Director) became free to open AWFs, sending relevant information to the

[481] STORBECK, Jürgen, "La cooperación policial europea", loc. cit., p. 167.
[482] Member States had agreed to organize evaluations to assess applications of different police and judicial co-operation mechanisms, and the third round was dedicated to information exchange with Europol.
[483] See Council document 13321/07, p. 35.
[484] See GÓMEZ-JARA DÍEZ, Carlos, "¿Federalsmo jurídico-penal en la Constitución Europea? Un diálogo con el profesor Silva Sánchez" in ARROYO ZAPATERO, Luis and NIETO MARTÍN, Adán, *El Derecho Penal de la Unión*…, op. cit., p. 89.
[485] Focused on phenomenon, organised group or region.

supervisory body and the Management Board, and to continue its development and use until objection was received from the latter.

The purpose of AWFs was (and still remains) analysis defined by the assembly, processing or utilization of data with the aim of helping a(n) (ongoing) criminal investigation of all interested Member States and is "one of the main ways in which Europol delivers operational support to Member States."[486]

Thus they would provide information and intelligence related to the topic and Europol staff, using analytical tools, would compare it with information received from other Member States, in order to establish possible links between crimes, persons, *modus operandi*, groups, etc. For example, such an AWF was created to combat trafficking in cocaine (to investigate, dismantle laboratories, etc.) And sought "to collect intelligence associated with the activities of suspected criminal organisations and networks involved in the production, processing or trafficking of cocaine, including intelligence relating to precursor chemicals and cutting agents."[487]

Unlike the EIS, AWFs can contain not only data on convicted persons and persons suspected of commissioning crime, but also data on victims, witnesses, contacts and associates, providers of information related to offences under consideration. And as mentioned in subsection 5.3 of Chapter II, in indispensable cases for the file, it is allowed to process in AWFs, special personal data, such as racial or ethnic origin, religion, state of health or sex life.

AWFs can also contain data on criminal offences, modus operandi, entities responsible for the investigation, case reference, even if no references to persons exist.

In addition to information processing, Europol was also endowed with the additional tasks of developing specialist knowledge, providing strategic intelligence and preparing general situation reports.

The Management Board – as already mentioned – is Europol's decisive body. As Europol was the result of intergovernmental co-operation, there was the need for a body that would ensure the participation of all Member States in approval of essential decisions on Europol's functioning (those not regulated or endowed to the Council), and so the Management Board was created as such a unit. It became responsible for the definition of rules for liaison officers (their rights and

[486] DISLEY, Emma; IRVING, Barrie; HUGHES, William et al. "Technical report on Evaluation…", loc. cit., p. 78.

[487] EUROPEAN MONITORING CENTER FOR DRUGS AND DRUG ADDICTION, EUROPOL, "Cocaine: A European Union Perspective in the global context", 2010, p. 33, accessed, June 7, 2015, https://www.google.es/#q=analytical+work+file+Cola.

obligations), regulation of security clearance, participation with the Council in the extension of Europol's mandate, appointment of the Director, his or her Deputies and financial controller, drawing up the budget (consisting of Member States' contributions[488] and other incidental incomes).

1.2.2. Way Forward

The Europol Convention was subject to modification by three protocols signed in 2000, 2002 and 2003:

- Council Act of 30th November 2000 drawing up, on the basis of Article 43(1) of the Convention on the establishment of a European Police Office (Europol Convention), of a Protocol amending Article 2 and the Annex to that Convention[489] that included money laundering into Europol's competence, as well as any other crime which predicates the crime that represents its core competence;
- Council Act of 28th November 2002 drawing up a Protocol amending the Convention on the establishment of a European Police Office (Europol Convention), and the Protocol on the privileges and immunities of Europol, the members of its organs, the deputy directors and the employees of Europol[490], that spelled out Europol's possibility to participate in joint investigation teams and to request Member States to conduct or coordinate investigations.
- Council Act of 27th November 2003 drawing up, on the basis of Article 43(1) of the Convention on the Establishment of a European Police Office (Europol Convention), a Protocol amending that Convention[491] that established the regulation of Europol's operational agreements with third states for information exchange and their participation in AWFs.

Due to a long ratification procedure, all three protocols only came into force in 2007. It was a clear sign that with the application of conventional procedure, Europol would not be able to adapt rapidly to changing crime tendencies with relevant modifications of its competences, tasks or functions. Under these circumstances, it was decided to change the Convention by the Council Decision

[488] According to Article 35 of the Europol Convention, "Each Member State's financial contribution shall be determined according to the proportion of its gross national product to the sum total of the gross national products of the Member States for the year preceding the year in which the budget is drawn up." In the Ministerial Agreement the cost was borne, "within the limits of their budgetary rules and annual procedures, each Ministry's voluntary annual contribution [...] will be determined on the basis of the country's gross national product."

[489] OJ C 358, 13.12.2000, p. 1–7.

[490] OJ C 312, 16.12.2002, p. 1.

[491] OJ C 2, 6.1.2004, p. 1-11.

that would be allowed, in case of necessity, to make rapid changes without the need to wait for the ratification process of all Member States, especially taking into account that since the first decisions on Europol, their number had increased from 12 to 27. This initiative was presented by the Austrian Presidency of the Council of the European Union in 2006, and resulted in the Commission's proposal on draft Council Decision.[492]

After more than 2 years of discussions, on 6th April 2009 the Council Decision 2009/371/JHA of establishing the European Police Office (Europol)[493] (hereinafter – Europol Decision) was adopted. It has been in force until now, but in the near future it will be changed by the Regulation as explained at the beginning of this chapter.

2. Europol – EU agency

With entrance into force of the Europol Decision, Europol became a European agency financed from the EU Budget, and subject to the same staff and other administrative requirements as other EU institutions and entities as well as being accountable to the European Parliament. Although the title of the Europol Decision includes the term "establishment", it only refers to the change of Europol's legal form, and Article 1(2) states that it "shall be regarded as the legal successor of Europol, as established by the Europol Convention."[494]

With respect to its objective, the Europol Decision entails support and strengthening action of cooperation and refers to the prevention and combatting of organised crime, terrorism and other forms of serious crime affecting two or more Member States. According to the Europol Convention, the relation with organised crime had been a compulsory condition in assigning crimes of terrorism, drug trafficking and other serious crime to Europol's competence. That meant that before the Europol Decision, drug trafficking, terrorism and other serious crimes would be Europol's competence only when these crimes were related to organised crime and would affected two or more Member States. With the Europol Decision, terrorism and other serious crimes would be within its competence when they affected two or more Member States, but are not necessarily related to organised crime.

The Europol Decision retains the same policy in relation to related crimes, given that the Europol Convention, i.e. Article 4(3) of the Decision, foresees Europol's

[492] See more explicitly AMICI, Victoria, "Europol et la nouvelle décision du Conseil: entre opportunités et contraintes" in *Revue du Droit de L'union Européenne*, 2010(1), p. 80-81.
[493] OJ L 121, 15.5.2009, p. 37-66.
[494] OJ L 121, 15.5.2009, p. 39.

involvement in prevention and combatting other criminal offences committed to facilitate those ones that are under its direct competence.

Regarding the processing of information, changes were not great, as Member states remain responsible for making decisions relating to the scope of information that can be provided to Europol. The Europol Decision only established the legal basis allowing wider access to its data bases in order to ensure better use of Europol's capacities and to enhance trust in it as a partner.[495] This novelty will be discussed more broadly in the following subsection.

Although since its establishment, Europol had been carrying out analytical functions, only the Europol Decision established the task to elaborate threat assessments and strategic analysis.

Europol's staff maintains the possibility of participating, in a supporting capacity, in joint investigation teams on the basis of arrangements with Europol's Director and the competent authorities of the participating Member States in it. Supporting capacity can be carried out within the limits established by the law of the Member State where joint investigation team is operating.

The structure and cooperation mechanism has remained the same, with the obligation of Member States to maintain single ENU and to send at least one liaison officer to Europol's Headquarters.

According to the last available data (September 2015), there were 134 liaison officers seconded to Europol by the Member States, and 37 by non-EU partners on the basis of cooperation agreements with Europol.[496]

Comparing the workflow from 2005 and 2013, the number of cases increased by 120 % and resulted in more than 18,000 cases.[497]

In order to maintain contacts and information exchange with the Member States and other partners, Europol has 24/7 operational coordination centre that: has a workflow of more than 300 operation messages a day, assesses whether incoming data can be included in the Europol databases, is responsible for a centralised

[495] See SANTOS VARA, Juan, "Las consecuencias de la integración de Europol en el Derecho de la Unión Europea (comentario a la Decision del Consejo 2009/371/JAI, de 6 de abril de 2009)" in *Revista General de Derecho Europeo,* 2010(20), p. 10.
[496] Council document 10597/15, p. 76.
[497] Council document 10426/14, p. 4.

cross-checking service, [498] and, if necessary, produces analytical reports that are immediately sent to the Member States in question.[499]

2.1. Information exchange tools

Since becoming an Agency, a description of Europol as an information exchange hub, a centre of expertise, can be encountered.

The Europol Decision, like the Europol Convention, directly establishes and regulates the Europol Information System and AWFs. It also foresees that the Management Board shall approve the creation of a new personal data processing system. Consequently, the Management Board agreed on the establishment of the Secure Information Exchange Network Application (hereinafter - SIENA).

Additionally, Europol is granted access to other centralised information systems in the EU: SIS II, Customs Information System, Visa Information System and Eurodac.

The subject of analysis of the following subsections will be the actual regulation of these tools.

2.1.1. Europol Information System

The functioning of the EIS is based on Articles 11-13 of the Europol Decision. EIS continues to be a database that stores information about offences and individuals involved, as well as other related criminal data.

According to Article 12, it contains only that data necessary for the performance of Europol's tasks and, talking about the categories of persons – only those that were already subject to inclusion under the Europol Convention.[500]

In addition to the data categories foreseen by the previous regulation (surname, maiden name, given names, alias, assumed name, date and place of birth, nationality, sex and where necessary other characteristics likely to assist in identification[501]), Article 12 of the Europol Decision allows the inclusion of the place of residence and whereabouts, profession, social security numbers, driving licences and identification documents. In the case of other characteristics,

[498] Quick cross-check of all data against criminal intelligence gathered in Europol's databases.
[499] Thus in 2013, Europol provided 1656 cross-match reports, 220 operational analysis reports and 385 other operational reports. See Council document 10426/14, p. 25.
[500] As mentioned: persons suspected of already having committed a crime, being accomplices or of its future commission, and subject to Europol's competence as well as information on committed crimes and convicted persons.
[501] Article 8 of the Europol Convention.

previously not specified, dactyloscopic data and DNA profiles are now distinguished.

Access to the EIS (both for input and retrieval) is granted to duly empowered Europol staff (including the Director and his or her Deputies), liaison officers and ENUs. A novelty established by Article 13(6) of the Europol Decision is that Member States can decide to give EIS access to other competent authorities, but it will be limited to the possibility of verifying whether or not requested information exists (hit / no hit bases). In the case of a hit, a request for relevant information has to be sent through the ENU of that country.

As in the case of SIS, only the party that submits information has the right to modify or delete it.[502]

According to data from 2013, EIS contained 245,142 objects, 70,917 suspects or convicted persons with 321,429 executed searches.[503]

2.1.2. Analysis Work Files

As already mentioned, in performing its tasks, when necessary, Europol when can create AWFs to process and analyse information on some types of crime, organised groups or modus operandi.

The Europol Decision has the same categories of persons that can be included in AWFs, i.e. Categories of persons whose data can be processed in the EIS, and data of witnesses who can be called to testify, victims, contacts and associates of suspects as well as of informers. In order to specify their regulation and establish clearer rules about the processing of different categories of personal data, Decision 2009/936/JHA was adopted.

Data categories that can be stored in AWFs depend on each category of person and vary considerably as shown in the following table.

[502] Article 20 of the Europol Decision foresees that data has to be deleted after 3 years (or if the data is not necessary – earlier) with a review within 3 months before the deadline of deletion. Within the period of review, a decision to leave the data for a longer period during which it remains necessary can be taken, but no longer than until the next review. If the review is not carried, data is deleted automatically after 3 years of storage.

[503] Council document 10426/14, p. 17. Report on Europol's activities in 2014 presents only data on objects contained in the EIS, but not persons and searches therefore presentation of older, but more complete data was elected.

Categories of person	Categories of data collected
All categories of persons	1. Present and former surnames (i.e. Real and alias, nickname, residence, nationality, parents (if it necessary, etc.) 2. Physical description 3. Identification means (i.e. Documents, ID and other official numbers, images, fingerprints and DNA profiles, etc.)
Suspect of a crime (already committed or future), accomplice, convicted persons, contacts and associates[504]	1. Education, skills, employment (including associated legal persons) 2. Economic and financial information 3. Information on behaviour data 4. Contacts and associates 5. Communication means 6. Transport means 7. Criminal activities under the competence of Europol (including associated legal persons) 8. References to other databases
Victims	1. Identification 2. Motives for victimisation 2. Damage suffered 3. Need to guarantee anonymity 4. Possibility to participate in a court hearing 5. Their provided information about crime Data categories mentioned in relation to suspect also can be collected if it is necessary for analysis
Witnesses	1. Need to guarantee anonymity 2. Need to guarantee protection 3. New identity 4. Possibility of participating in a court hearing 5. Their provided information about crime
Informers	1. Type of information provided 2. Encrypted personal data 3. Negative experiences 4. Rewards 5. Data categories applied to witnesses

Table 15: Categories of data stored in AWFs depending on category of person.

Among the information that can be included on victims, witnesses and informers, anonymity, use of new identity, need or application of protection measures deserve special attention. These categories can make any AWF a very powerful tool

[504] In the case of contacts and associates, previous evaluation on whether such data in necessary to analyse their role in relation to suspects, accomplices or convicted persons shall be carried out.

in the wrong hands and therefore, very high standards of secure communication, confidentiality and data protection shall be applied.

The right of direct input to an AWF remains the responsibility of Europol's analysts designated for that file. Thus the role of Member States[505] is limited to the submission of information to Europol, where it is evaluated before being stored. Nevertheless, it is up to Member States to establish a degree of data sensitivity and the processing conditions.

Third parties directly related to AWFs can participate in them and, in the case of the existence of a relevant agreement between the third party and Europol, all participants agree.

Every piece of data included in an AWF is categorised according to its source and information evaluation codes as is shown below.

Source evaluation code	Information evaluation code
(A): trustworthy and authentic information (B): information from a reliable source (C): information from a source which has, in most instances, proved to be unreliable (X): reliability assessment is not possible	(1): no doubts about accuracy of information (2): the source knows the information personally, but not the official passing it on (3): the source does not know the information personally, but it coincides with already recorded information (4): the source does not know the information and it cannot be corroborated

Table 16: Evaluation codes of sources and information processed in AWFs.

Europol can create AWFs of both a general and strategic nature[506], and in this case information will be available to all Member States.

In the case of operational AWFs[507], information will be available and retrieval can be carried out, only by participants and only after Europol's accreditation and special training. Every access to data and its transmission, will be recorded in order to identify the entity of the action. According to Article 15, the Director, his or her Deputies, Europol's staff, liaison officers and ENUs who do not participate in AWFs are authorised to access the index of the AWF only; this allows them to find

[505] ENU or in urgent cases, competent authorities directly. See Article 3 of the Council Decision 2009/936/JHA.

[506] Article 11 of Decision 2009/936/JHA defines its aim as the processing of relevant information concerning a particular problem, or to develop or improve initiatives by the competent authorities.

[507] The same article defines its aim as obtaining information on criminal activities in order to commence, assist or conclude bilateral or multilateral investigations when two or more Member States are involved.

out whether or not searched information exists, but does not give them direct access to it.

According to Article 17(1) of the Decision 2009/936/JHA, "All personal data and analysis results transmitted from an analysis work file may only be used in accordance with the purpose of the file or for the purposes of preventing and combating other serious forms of crime."

The Europol Decision continues to maintain the same policy on creation and closure of AWFs, where the main decisive power belongs to the Director, but the Management Board at any moment can order the closure of an AWF or to oppose the opening order.

Data storage terms and conditions depend on the way of closing AWFs:

- If the AWF was closed as a result of a finished operation, or analysis or term for which it was established, the data would be stored for up to eighteen months in separate file, for the purpose of internal or external control. The result of the analysis of an AWF can be stored in electronic form for up to 3 years and afterwards, only as a paper document.
- If the AWF was closed on the request of the Management Board, all data has to be deleted immediately.

In 2012 Europol, run 23 AFWs and from the years of experience, it came to the conclusion that a vertical approach (on one region, group or phenomenon) is not always sufficient, and more a generative thinking approach is needed. In these circumstances, and basing its decision on Article 18(1)a of Decision 2009/936/JHA, Europol proposed to participants of all AWFs, that they merge into two large AWFs: an AFW for serious and organised crime (AWF SOC), and an AWF for counter terrorism (AWF CT). Thus in May – July of 2012, 18 AWFs related to serious and organised crime migrated to AWF SOC, and 5 AWFs related to counter terrorism – to AFW CT. A characteristic of the new AWFs is that within them, different analyses and actions could be carried out. A distinction was made between a Focal Point and a Target Group. The first one focuses on a certain phenomenon from the perspective of topic, regional angle or commodity, and Europol provides it mainly with analysis and support information and intelligence exchange. The second one is more operational than a Focal Point, as in addition to analysis, Europol designates its team to support an investigation or intelligence operation against a specific target.

2.1.3. Secure Information Exchange Network Application

In 2009, Europol's Secure Information Exchange System (SIENA) was created.

The system allows the exchange of strategic and operational information within the mandate of Europol, assuring a high level of communication, security and interoperability with other Europol systems and enabling the secure exchange of restricted and confidential information.

SIENA provides two possibilities:

- To exchange information using a web browser.
- Since 2012, to exchange information "system to system" that allows two types of connection: simple (to receive SIENA messages) and advanced (to receive and send them). The latter means the connection of a national system in such a way that it could be used both for national and international information exchange.

SIENA has multilingual user interface in all languages of the EU. Nevertheless, the text of a message is not translated and must normally be written in English, except in those cases when the parties in question agree to use another language.

SIENA can be used both for information exchange purely under Europol's mandate, and for bilateral or multilateral communication among Member States that remain outside its scope (that according to the technical report on Evaluation of the implementation of the Europol Council Decision and of Europol's activities carries out a majority of information exchange).[508] But on addressing one of Europol's cooperation partners (third party), Member States will be notified via SIENA that this exchange should only take place as far as crimes within Europol's mandate are concerned.

Depending on national arrangements, SIENA can be used not only by the ENU and liaison officers, but other competent authorities as well. Nevertheless, all the authorities of one Member State have to be connected through one national system.

Before connecting to SIENA, it has to be ensured that the national system fulfils all security and data protection requirements (authentication, access control, input and output validation, logging and error handling, infrastructure controls).[509]

[508] See DISLEY, Emma; IRVING, Barrie; HUGHES, William et al., "Technical report on Evaluation…", loc. cit., p. 49.
[509] Council document 10303/14, p. 20-21.

At the end of 2014, SIENA included 573 competent authorities with 4,663 users from the Member States; Europol's operational and strategic partners had an average of 50,000 messages exchanged every month.[510]

2.1.4. Information handled under Article 10.4 of the Europol Decision

Article 10.4 of the Europol Decision foresees the processing of submitted data for no longer than 6 months, in order to determine whether it can be included in EIS, AWFs or another system. This provision, in all cases, is applied to AWFs, as only Europol specialized staff can enter information regarding ES or other systems when it is not directly included by a Member State, EU entity or authorized third party. After six months, information shall be either in EIS, AWF, another system or deleted.

Submitted information is automatically cross-checked with the index system of the EIS and then evaluated. Nevertheless, evaluation criteria are not clear. One of them should be conformity of information with Europol's mandate. But application of only these criteria would be unjustifiably disproportionate.

Nevertheless, this area stays in the shadow, as there is no publicly available document that regulates these Europol activities.

2.2. Information exchange with EU institutions and other entities, third states and international organisations

Exchange of information between Member States through Europol, or its submission to Europol's databases directly derives from the Agency's objective to support and strengthen the actions of competent authorities, and their cooperation. Nevertheless, in achieving this objective and acting against threats to the EU internal security information and intelligence from entities other than Member States (inside the EU as well as from third states and organisations), can be of upmost importance. For example:

- Information exchange with the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX). Can help to identify links between organised crime, trafficking in human beings and illegal migration;

[510] See Council document 8082/15, p. 42.

information from Eurojust – to make link with ongoing investigations, and so on.

- Such crimes as drug trafficking, illegal migration and trafficking in human beings usually have their origin outside the EU, envisaging its Member States as the point of final destination. Therefore, to guarantee EU internal security, effective international cooperation with competent authorities in countries of origin and transit is indispensable. For example, as big drug flows come from West Africa, and South and Central America, a closed co-operation and effective information exchange with the competent authorities in these countries has to take place. In the case of criminal organisations of Albanian[511] or Russian[512] origin which act within the EU, information and intelligence from these countries is vital as well. Such co-operation could be based on reciprocity, that does not guarantee either rapidness or effectiveness, or on co-operation agreements. In reference to bilateral agreements, it is difficult to imagine that each Member State would have the necessary agreements with all important partners outside of the EU, because they are usually concluded in line with national priorities of co-operation with neighbouring states or specific regions, depending on their geographical position, historical links with other countries and threats to their security. In these circumstances, the optimum would be EU wide possibility of information exchange, which would serve to combat threats at EU level.[513]

Therefore, the Council has envisaged for Europol, the possibility to exchange information with other EU bodies and third parties.

When it comes to exchange of strategic information and analysis, operational analysis, non-personal, personal and confidential data, different regulations are applied. In the case of personal data, a general rule of its transmission is an objective of" preventing or combating criminal offences in respect of which Europol is competent."[514]

Receiving information, Europol shall ask submitting party to assess it and its source, applying the same evaluation codes as Member States providing information for AWF.

[511] See STORBECK, Jürgen, "La cooperación policial europea", loc. cit., p. 157.
[512] See ESPIGARES MIRA, Jesús, "Instrumentos internacionales de cooperación" in MONTERO, Julián, ROMERO and Francisco, VALIENTE, Elena. *¿Hacía una Policía Europea?*, op. cit., p. 119.
[513] See more in RENARD, Thomas, "Partners in crime? The EU, its strategic partners and international organised crime" (Working Paper, European Strategic Partnership Observatory, May 2014), p. 15-20, accessed June 2, 2015, http://fride.org/publication/1191/partners-in-crime?-the-eu,-its-strategic-partners-and-international-organised-crime.
[514] Article 8 the Council Decision 2009/934/JHA.

The following subsections of this work are rendered to the regulations and problems that faced by Europol in information exchange with the EU entities and third parties, leaving the personal data protection questions to section 3.[515]

2.2.1. Information exchange with EU institutions and other entities

Article 22 of the Europol Decision permits cooperative relations with all institutions, bodies, offices and agencies of the EU, and in particular with those directly or indirectly related to the Europol's activities. It envisages an obligation to conclude agreements or working arrangements on operational, strategic, technical and classified information exchange with Eurojust, the European Anti-Fraud Office (OLAF), Frontex, the European Police College (CEPOL), the European Central Bank and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA).[516] With other bodies, agreements can be concluded if the Management Board gives an authorisation for negotiations. Once negotiations on agreement or working arrangements are finished, before a definitive conclusion is reached, Europol has to obtain the approval of the Management Board.

Europol's agreements with EU institutions, agencies and other entities can be:

- Strategic – permitting only the exchange of general information and strategic analysis without providing any personal data or confidential information.
- Operative – regulating in depth data protection and allowing the exchange of personal data.

It has to be mentioned that Article 55 of the Europol Decision envisages that with this new regulation, previously concluded agreements[517] are not affected.

As for the date, Europol has concluded:

- Strategic agreements with the European Commission, European Central bank, Frontex, CEPOL, EMCDDA, OLAF, as well as the Office for

[515] In this context, it has to be mentioned that according to Article 25 of the Europol Decision, it is also allowed to receive information from private parties (legal entities, NGOs, etc.) and private persons from the EU Member States and third parties with already concluded agreements. This can only be done through ENU of Member States or the contact point of third parties. When an entity or a person is from a third party with no co-operation agreement, a memorandum of understanding between Europol and that party must be concluded. Europol is not allowed to contact private parties and persons in the third states with whom it does not have agreement; the initiative shall come from the third country or private party/person.

[516] Strengthening of co-operation between the EU agencies is also foreseen in the European Internal Security Strategy.

[517] Australia, Canada, Iceland, Norway, Switzerland and United States of America.

Harmonisation in the Internal Market and the European Union Agency for Network and Information Security.

- Operational agreement with Eurojust.

That means that it is only allowed to exchange personal data with Eurojust, and with the rest of the European partners, co-operation is of a strategic nature.

On the other hand, Article 22(3) allows information exchange (without specific rules concerning personal data) prior to any the agreement, if it is necessary to perform the recipient's tasks (Europol's or of other EU institution). This raises a question of expedience to start more difficult negotiation processes of operational agreement, if in any case there is the possibility of transmitting personal data without an agreement, foreseeing such a wide margin of purpose as tasks of entities involved in exchange.

2.2.2. Information exchange with third states and international organisations

Article 23 of the Europol Decision foresees the possibility of establishing and maintaining cooperative relations with third countries and organisations. Normally such co-operation, the same as in cases of the EU institutions and other entities, would be based on strategic or operational agreements.

The list of countries and organisations with which Europol can conclude agreements is established (and can be complemented) by qualified majority of the Council of the European Union. Such a list was approved by the Council Decision 2009/935/JHA of 30th November 2009 determining the list of third States and organisations with which Europol shall conclude agreements[518] (hereinafter – Decision 2009/935/JHA) and includes: Albania, Australia, Bolivia, Bosnia and Herzegovina, Canada, China, Colombia, Croatia[519], former Yugoslav Republic of Macedonia, Iceland, India, Israel, Liechtenstein, Moldova, Monaco, Montenegro, Morocco, Norway, Peru, Russia, Serbia, Switzerland, Turkey, Ukraine, United States of America, ICPO-Interpol, United Nations Office on Drugs and Crime and World Customs Organisation. It should be mentioned that it does not envisage whether strategic or operational agreement with one or another country or organisation has to be concluded. According to Articles 5 and 6 of Decision 2009/934/JHA, it depends on the data protection level of the third country or organisation that is subject to evaluation prior to negotiations (see more subsection 3.3.1 of this Chapter). On this basis, the Management Board allows Europol to enter into

[518] OJ L 325, 11.12.2009, p. 12-13.
[519] The agreement is not necessary since 1 June 2013 as Croatia became EU Member State.

negotiations of one or another type of agreement. Once negotiations are finalised, the draft is submitted for the endorsement of the Management Board and approval of the Council of the European Union (in the case of operational agreement, opinion of the Joint Supervisory Body is also submitted). This is a different from the approval of agreements with the EU bodies, where the top decisive institution is the Management Board.

Without agreement in force, Europol can receive any data necessary for performing its tasks, but is limited to transmitting only non-personal and non-confidential data to the states and organisations mentioned in Decision 2009/935/JHA, and if transmitted information has been provided by a Member State – only with its consent. The only exceptions are established in Article 23(6) and 23(8) and discussed in subsection 3.3.1 of this Chapter.

In the case of countries and organisations not listed in Decision 2009/935/JHA, Europol is allowed to transmit only non-personal and non-confidential data in "absolutely necessary individual cases". In this case, the same question about the content of "individual cases" arises, but at least it is not related to the transmission of personal data.

For the time being, Europol has concluded:

- Strategic agreements with Bosnia and Herzegovina, Moldova, Russian Federation, Turkey and Ukraine.
- Operational agreements with Albania, Australia, Canada, Colombia, Former Yugoslav Republic of Macedonia, Iceland, Montenegro, Norway, Republic of Serbia, Switzerland, the Principality of Liechtenstein, the Principality of Monaco, United States of America.

It has to be stressed that the scope of purpose of co-operation in agreements differs. Thus in agreements with Albania, Australia, Colombia, former Yugoslav Republic of Macedonia and Liechtenstein, the scope of co-operation is all or almost all crimes that fell under Europol's mandate at the date of entry into force of agreement. In the case of Iceland, Monaco, Norway, Switzerland and United States of America, the scope is limited to a few types of crime, such as unlawful drug trafficking, trafficking in nuclear and radioactive substances, illegal immigrant smuggling, trade in human beings, motor vehicle crime, crimes committed or likely to be committed in the course of terrorist activities against life, limb, personal freedom or property, and the forgery of money and means of payment.[520]

[520] See, for example, Article 3 of the Agreement between the Kingdom of Norway and the European Police Office; Agreement between the United States of America and the European Police Office; Agreement between the Republic of Iceland and the European Police Office.

According to the already mentioned Council Decision 2006/560/JHA, Europol can also delegate its employees to one or more third countries, or to international organisations. Any Member State can send a request to Europol to use its liaison officer for information exchange with the third party. For the time being, Europol has liaison officers in Interpol and the United States.[521]

2.3. European Cybercrime Centre

In addition to different information exchange tools, Europol also has units specialising in different topics. One of the latest and most significant is the European Cybercrime Centre, also called EC3. It developed from the European platform on cybercrime established and hosted by Europol on the basis of Council Conclusions of the 2,899th Justice and Home Affairs Meeting of 24th October 2008.

In the Communication from the Commission to the European Parliament and the Council, "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe"[522] (hereinafter – Communication on Implementation of ISS) within the objective of raising security in cyberspace, it was foreseen that by 2013, a cybercrime centre will be established "to build operational and analytical capacity for investigations and cooperation with international partners" [523] and it will be established within existing structures.

For this purpose, in 2012, RAND Europe performed a feasibility study and after comprehensive analysis of the option to allocate the Cybercrime Centre in Eurojust, Europol or ENISA, or create it as a virtual centre, a new agency or an organisation to be run by one Member State or by a Public-Private Partnership, it was proposed to create it within Europol.[524] It was recommended, especially taking into account that only Europol is a criminal intelligence agency with a clear mandate and that "the legal basis of the agency is tailored to its operational role – it has an extensive data- protection regime and a complex set of rules governing participation in the AWFs."[525]

[521] Council document 11996/14, p. 73.
[522] COM(2010) 673, final.
[523] COM(2010) 673, final, p. 9.
[524] ROBINSON, Neil; DISLEY, Emma; POTOGLOU, Dimitris et al., "Feasibility Study for a European Cybercrime Centre" (Final report, RAND Europe, February 2012), accessed 1 June, 2015, http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre_en.pdf.
[525] Ibid, p. 110.

Functions foreseen in the Communication from the Commission to the Council and the European Parliament "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre":[526]

- To be a focal point between national competent services, the private sector and CERT;
- To support capacity building of Member States;
- To support investigations;
- To act as a point of reference in relation to cybercrime investigations and "common voice" in this area.[527]

In June 2012, the Council supported the creation of EC3 in Europol, and it became operational on 11th January 2013.

As with Europol, EC3 also has a co-ordination function in relation to transnational operations on cybercrime, which involve organised crime; in particular child abuse, online fraud and threats to the EU information systems and the critical infrastructures of Member States. It is also a "central hub" for information and intelligence, produces its own strategic analysis product – Internet Organised Crime Threat Assessment (IOCTA) - which has already been mentioned in the first Chapter; it also ensures forensic support.[528]

As there are no specific legal acts regulating EC3 activities, and no restrictions in comparison with Europol in general, it can be concluded that general Europol regulations are applied to its work, and on the same basis as Europol, it can be part of AWFs, access to EIS and communicate through SIENA. Member States can address their request exactly in the same way as they do in relation to other crimes that fall within Europol's competence.

2.4. Efficiency

According to what has been already presented, since mid-1999, Member States have had an opportunity to use a new co-operation tool in combatting cross-border crime.[529] Moreover, the success of this tool depended on the good faith of

[526] COM(2012) 140 final.
[527] Ibid. p. 4-5.
[528] See "Combating Cybercrime in a Digital Age", Europol, accessed June 9, 2015, https://www.europol.europa.eu/ec3
[529] See AMICI, V., "Europol et la nouvelle décision…", loc. cit., p. 96.

co-operation of national law enforcement agencies, as Europol Convention had not established obligations either to submit information or to reply to requests. [530]

In parallel with the entrance into force of the Convention on Europol and the last preparatory works, political emphasis on the promotion of the co-operation with this entity came with the Amsterdam Treaty, as well as with the statement of the Tampere Conclusions, declaring that within five years Europol's role "should be strengthened by means of receiving operational data from Member States and authorising it to ask Member States to initiate, conduct or coordinate investigations or to create joint investigative teams in certain areas of crime, while respecting systems of judicial control in Member States."[531]

But the process of obtaining trust in politically originated law enforcement entity was long and complicated, as not all Member States were ready to reveal their national investigations and provide Europol with the relevant information. It was aptly defined by Castillejo Manzanares that Europol had faced "scepticism of police" that did not provide it with sufficient and systematic support.[532] After two years of functioning, in 2001, Europol's director, Storbeck, recognised this problem and tried to justify it saying that, "Even now when European interests coincide like never before, intercultural conflicts and fears of population about the establishment of federal super-state very seldom are obstacles for closer co-operation in a big variety of matters within the European Union. For some of them any small progress is a big step forwards."[533]

Six years later, in 2007, only Denmark, France, Germany and Spain had issued internal instructions to prioritise the Europol channel for information exchange. In other Member States, Interpol remained the preferred channel for day-to-day cooperation.[534] At the same time, Bruggeman noticed that, "With reference to the co-ordinating role [of Europol], it can be said that this is very important from a European Perspective, but that the real impact right now is still very limited, since many police officers in the field still work bilaterally (the so-called 'old boys' network)."[535]

---

[530] See ARROYO ROMERO, Francisco Javier, *La influencia de EUROPOL en la comunitarización…*, op. cit., p. 39.

[531] Presidency Conclusions, Tampere European Council, 15-16 October 1999, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/00200-r1.en9.htm.

[532] See CASTILLEJO MANZANARES, Raquel, "Europol y las investigaciones transfronterizas" in *Dereito*, 2008, vol. 17-2, p. 95.

[533] STORBECK, Jürgen, "La cooperación policial europea", loc. cit., p. 158.

[534] See Council document 13321/07, p. 24, 31.

[535] BRUGGEMAN, Willy, "A Vision of Future Police…", loc. cit., p. 209. The same observation in much broader context (any changes brought by the EU law into national system) made MITSILEGAS, MONAR, REES saying that it provokes "almost instinctive reaction against such European "interference" with well-established national approaches, basic concepts and traditions". See

And even a technical report from 2012 on the Evaluation of the implementation of the Europol Council Decision, and of Europol's activities, reveals that there is a fear that submitted information is automatically available to all Member States. Therefore, bilateral agreements are used more as they allow better control of the provision of information and "national law enforcement officials already have a large number of domestic databases in which to enter data. Law enforcement officials under time pressure tend to use familiar, national-level systems, and might see entering data into Europol systems as too burdensome or time-consuming."[536] It also reveals both Europol's and the Commission's worries about data quality and their disappointment in Member States' actions, taken as a consequence of Europol providing information.[537]

Nevertheless, during recent years, t more and more information has been published about Europol's assistance and participation in operations, beginning with on the spot support to one Member State (as in the case of operation Walker[538]) or multinational operations such as Archimedes or Blackshades. In operation Archimedes all Member States participated, along with Australia, Colombia, Norway, the United States, Serbia and Switzerland with more than 1,000 persons were arrested, 339 seizures of 2.1 tonnes of drugs and more than one million euros in cash.[539] In operation Blackshades (coordinated by Eurojust and supported by EC3 at Europol), sixteen Member States took part; it resulted in more than eighty arrests and 359 house searches in combatting Blackshades malware.[540]

Notwithstanding, it is quite difficult to identify whether co-operation is improving or more publicity is being given to the same state of co-operation, in order to make it "attractive" to other law enforcement institutions.

MITSILEGAS, Valsamis; MONAR, Jörg and REES, Wyn, *The European Union and Internal...,* op. cit., p. 10.

536 DISLEY, Emma; IRVING, Barrie; HUGHES, William et al. "Technical report on Evaluation…", loc. cit., p. 50-51.

537 Ibid, p. 51, 79.

538 Europol assisted Spanish police to target an organised group responsible for telecommunication fraud in total of at least 2 million euros and its laundering. Although the group acted from Spain, victims of their crimes were from all over the EU. See "Europol supports Spanish Police to dismantle serious cybercriminal group" (Europol Press Release, 10 July 2015), accessed July 13, 2015, https://www.europol.europa.eu/content/europol-supports-spanish-police-dismantle-serious-cybercriminal-group.

539 See EUROPOL. "Operation Archimedes infographics", September 2014, accessed July 6 2015, https://www.europol.europa.eu/content/operation-archimedes-infographics.

540 See EUROPOL. "Worldwide Operation against Cybercrime", May 2014, accessed July 6, 2015, https://www.europol.europa.eu/content/worldwide-operation-against-cybercriminals.

3. Data protection

Protection of data processed in Europol is regulated by an individual set of provisions established by the Europol Decision, and other, already mentioned, Council Decisions; on some occasions, it is considered as comprehensive and exemplary to guarantee the right to data protection.[541]

On the other hand there are opinions that, "The adequacy of the current legislative framework governing Europol in terms of privacy protection, judicial control, transparency and accountability leaves much to be desired."[542]

It should also be pointed out that the national law of the country providing information also has to be accomplished, for example,

- Article 4.2 of the Council Decision 2009/936/JHA envisages that a Member State decides on the basis of its national law about what data and to which extent can be supplied to AWF;
- Article 15.1 of the same Decision foresees that information on the use of data from AWF shall be transmitted to the Member State of its origin when so allows national legislation of the receiving Member State;
- Article 13.5 of the Europol Decision establishes that transmission of information included in the EIS between ENU and competent authorities of the same Member States is regulated by its national law;
- Its Article 17 foresees that other use of information than by the competent authorities or for other purpose is allowed only according to the national law of transmitting Member State;
- Its Article 25.3.a and 25.5 envisages fulfilment of national law in transmitting information from private parties.

General data protection rules applicable to Europol are established in Chapter V of Europol Decision. Article 27 also makes a reference to the principles established in the European Convention on Data Protection, its modifications and Recommendation (87) 15 that shall be taken into account in personal data processing. Nevertheless, neither an obligation to follow them is established nor are they integrated into obligatory provisions.

[541] See DISLEY, Emma; IRVING, Barrie; HUGHES, William et al. "Technical report on Evaluation…", loc. cit., p. 91-92; DE HERT, Paul; PAPAKONSTANTINOU, Vagelis and RIEHLE, Cornelia, "Data protection in the third pillar: cautious pessimism", in MAIK, Martin, *Crime, rights and the EU: the future of police and judicial cooperation* (London: Justice, 2008), p. 141.

[542] MITSILEGAS, Valsamis, "The third wave of third pillar law: which direction for EU criminal justice?" in *European Law Review,* 2009, vol. 34, no. 4, p. 552.

According to the Article 29, Europol is responsible for data its own processed data. Notwithstanding, responsibility for data accuracy, legality and other aspects of its collection and transmission to Europol lies within the Member State that has submitted it, and within Europol when it was submitted by the third party.

Europol's responsibility for the information provided by the third parties raises a question: how can Europol be sure about the accuracy, legality and other legal aspects of data provided by the third parties? It would be more probable to evaluate those third parties with whom Europol has operation agreements, but not in other cases. On the other hand, in those cases there is no possibility to establish an obligation to the third party to evaluate and be responsible for data provided, and the establishment of Europol's responsibility is the only possible option to establish; although it is not perfect. In these circumstances, Europol, receiving information from a third party with whom no agreement is concluded, should evaluate carefully the received information and classify it according to the codes applied to sources and information.

As there are different opinions about Europol's data protection regime, the following subsections are dedicated to the analysis of its coherence and comprehensiveness.

3.1. Persons included

As mentioned in previous sections, in Europol's different information processing tools, the data of different categories of persons is processed. Its summary is presented in the following table.

Europol's information system or other information exchange through Europol	**Categories of persons whose data can be included**
EIS	- Suspects of already committed crime - Suspects of possible future commission of the crime - Convicted persons
AWF	- Suspects of already committed crime - Suspects of possible future commission of the crime - Convicted persons - Witnesses - Victims - Contacts, associates

	- Informers
SIENA	Not specified by the legislation. Interpreted as "crime-related information"[543]. SIENA can be used both for information exchange purely under Europol's mandate and for bilateral or multilateral communication among Member States out of its mandate.

Table 17: Categories of persons that can be included in EIS, AWFs and SIENA.

According to Article 12.1 of the Europol Decision, the notion of suspect and backgrounds for suspicion of future commitment of a crime are left to the definition of the national law of each Member State. Thus they depend on national procedural law and vary among themselves. For example:

- Spanish Criminal Procedure Code does not provide a definition of a suspect, and with the modifications of the Criminal Procedure Code that enters into force on 6th December 2015, the terms *investigated person* and *accused person* will be used. The only Article that mentions "suspect" is 363 which regulates taking samples for DNA analysis.[544]
- According to Article 21 of the Lithuanian Code on Criminal Procedure, a suspect is a person detained or questioned under suspicion of committing a crime, or to whom a notification of suspicion is addressed, or if his or her place of residence is not known he or she is recognized as a suspect on the basis of the prosecutor's or pre-trial judicial authority's resolution.
- According to Article 71 of the Polish Code on Criminal Procedure, a suspect is a person towards whom a resolution on allegation of committing a crime is issued, or who is questioned as a suspect without the above previously mentioned resolution.
- According to Article 27 of the Dutch Code on Criminal Procedure, a suspect is a person reasonably suspected in commission of offence.

European legislation on minimum standards in criminal procedure is applied to suspects and accused persons, but it does not include their definition, and that results in no point of reference on this issue.

Article 5 of the Europol Decision foresees that in every case, the Director taking the decision to open an AWF, also specifies the categories of personal data that can be processed, meaning that not all data categories automatically allowed by this Council decision will be processed in every AWF, but applying a principle of "need

[543] See DISLEY, Emma; IRVING, Barrie; HUGHES, William et al., "Technical report on Evaluation…", loc. cit., p. 78.

[544] See more. SOLETO MUÑOZ, Helena and ALCOCEBA GIL, Juan, "Protección de datos y transferencia de perfiles de ADN" in CABEZUDO BAJO, María José, *Las bases de datos policiales…*, op. cit., p. 338-339; SOLETO MUÑOZ, Helena and FIODOROVA, Anna, "DNA and Law Enforcement...", loc. cit., p. 156.

to know". In cases of special categories of data[545] about the victims, witnesses, contacts, associates and informers, according to Article 5(2) they can be included only upon request by two or more Member States participating in the AWF.

3.2. Access

Access rights to Europol's information systems differ, depending on their nature; and they are not equal.

Thus access to all EIS data is granted to empower Europol staff, liaison officers and ENUs. Access on a hit / no hit basis can be granted to national competent institutions according to national provisions. This allows broader use of Europol's stored information, making EIS a more useful tool for law enforcement institutions, and increasing its efficiency, but at the same time relevant requirements on secure connection and data protection must be applied. Third parties do not have access to the EIS. If they need information, Europol makes the search on their behalf and on the basis of existing operational co-operation agreement.

Access to strategic AWFs is granted to all Member States, but access to operational AWFs is much more restricted and given on a "need to know" basis", [546] i.e. Only to authorised analysts from the Europol, authorised staff of participating competent authorities, authorised liaison officers and ENU staff from participating Member States. Access to AWF Index System that allow its consultation on a hit / no hit basis is given to all liaison officers of Member States, ENUs and competent Europol staff.

Such access restriction in respect to AWF is indispensable due to the possibility of processing data of victims, witnesses and informers, as well special categories of information.

Regarding SIENA, it can be used as an information communication tool by Europol's staff, liaison officers, ENUs, competent authorities designated on the basis of national law, as well as third parties that have co-operation agreements with Europol. In the last case, third parties with concluded operational agreements can send request messages directly to the destination (Europol or the Member State), but in the case of strategic agreement, messages pass through the Europol Operational Centre, where a decision on its acceptance and further transmission or rejection is taken.

---

[545] Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and data concerning health or sex life.

[546] See DISLEY, Emma; IRVING, Barrie; HUGHES, William et al., "Technical report on Evaluation…", loc. cit., p. 83.

3.3. Third parties and onward transmission

3.3.1. Personal data transmission to third parties

According to Article 10 of the Decision 2009/934/JHA, "Europol shall be responsible for the legality of the transmission of data. Europol shall keep a record of all transmissions of data under these rules and of the grounds for such transmissions. Data shall be transmitted only if the recipient gives an undertaking that the data will be used only for the purposes for which they were transmitted."

As mentioned before, as a general rule personal data exchange with third countries and organisations is possible on the basis of operational agreements with prior evaluation of the data protection level. Agreements cannot be finalised without the inclusion of relevant data protection requirements and, therefore, it is considered that Europol has become the key protagonist in exporting the European model of data protection and in achieving that, a lot of the third state modify their legislation in order to get access to Europol's data.[547]

Already mentioned Articles 23(6) and 23(8) of Decision 2009/935/JHA establish two exceptions when transmission of personal and confidential data from Europol prior to agreement is allowed:

- When it is necessary in individual cases to prevent or combat crimes that are within Europol's competence;
- When the Director considers that it is necessary to safeguard essential interests of the Member State, or prevent imminent danger of terrorist attack and assesses the level of data protection in that country or organisation.

In the first exception, there is a lack of strict criteria of how individual cases have to be understood: individual investigations or operations, exclusively important investigations or operations; is that individual Europol case interest or third party? Due to such uncertainty, it would be appropriate to specify or to eliminate this provision. Of course, one can argue that unpredictable situations can always happen, but between establishing an unpredictable situation and soft wording, there is a possibility to regulate it in such a manner that prevents misuse. Even envisaging subsequent reporting of transmitted information to the Management Board and Joint Supervisory Body is not a sufficient measure, as personal or

[547] See BLASI CASAGRAN, Cristina, "El papel de Europol como actor normativo de la UE en el intercambio de datos con terceros estados" in PI LLORENS, Montserrat and ZAPATER DUQUE, Esther, *La dimensión exterior de las agencias…*, op. cit., p. 111.

confidential data is already in the possession of the third party and out of Europol's control.

3.3.2. Onwards transmission of personal data

Articles 17 and 18 of Decision 2009/934/JHA establish the possibility of onward transmission of personal data by other EU bodies or the competent authorities of a third State. This is allowed only when Europol and the onwards transmitting party has concluded the operational agreement. Nevertheless, different agreements establish different regulation of this issue. Thus agreements with:

- Canada, Iceland, Norway and Switzerland do not allow data transmission to third states;
- Albania, Liechtenstein and Serbia permit it in both directions (onward by this third country or Europol) with the previous consent of the information provider;
- Australia, former Yugoslav Republic of Macedonia and Monaco permit it only from this third state to another third party and with the previous consent of Europol,
- United States of America does not regulate this question.

In any case few different situations of onward transmission are possible and have to be analysed:

- Further transmission within the same third party. In this case it is not quite clear whether it is applied to third states, third parties or also EU bodies as the first two parts of Article 17 mention only third states where onwards transmission is possible, and only to those competent authorities listed in the agreement with Europol. Nevertheless, in part 3 we find reference to EU bodies and third parties (both states and organisations) and their obligation to ensure that onward transmission "Will take place under the same conditions as those applying to the original transmission."[548]
- Further transmission by the EU body or third party to another EU entity or third party.

As Article 17 establishes requirement to intra-state onward transmission, it is logical and coherent not to skip application of the same requirements for onward transmission to another EU body or third party. Then it also depends on the relationship between Europol and the final recipient of data:

[548] OJ L 325, 11.12.2009, p. 10.

- If they have operational agreement, Europol has to give prior consent to such transmission;
- If they do not have operational agreement, it can only take place in exceptional cases after authorisation by the Director of Europol, when it is, according to Article 18(2)b, "Absolutely necessary (i) to safeguard the essential interests of the Member States concerned which are within the scope of Europol's objectives; or (ii) in the interests of preventing imminent danger associated with crime or terrorist offences."

The chain of information transmission: Member State – Europol – Third party with operational agreement – other third party seems to be quite long in order to assure proper data protection on all levels. Finally, there is no effective mechanism to control data at the final destination and to guarantee that its further onward transmission will not occur.

3.4. Classified information

Among different types of exchanged information (both within and outside the EU) classified information deserves special attention; defined by the Council Decision 2009/968/JHA of 30th November 2009, adopting the rules on the confidentiality of Europol information[549] (hereinafter –Decision 2009/968/JHA), as "any information and material in any form, an unauthorised disclosure of which could cause varying degrees of prejudice to the essential interests of Europol or of one or more Member States, and that requires the application of appropriate security measures."

In order to ensure exchange of such information, a highly secure mechanism has to be applied that includes a secure communication system, limited and controlled access, equally high physical protection measures both in Europol and Member States, as well as other partners with whom exchange of such information is allowed, and only in the case of the conclusion of relevant agreements. Some agreements just foresee such a possibility, others (such as with Colombia or former Yugoslav Republic of Macedonia) dedicate 15 article long Annexes to regulate this process.

Transmission of classified information to other third parties (without relevant agreement) is allowed only when, according to the consideration of the Director of Europol, it is indispensable to guarantee the essential interests of the Member States or to prevent imminent danger from crime of terrorism. About such

[549] OJ L 332, 17.12.2009, p. 17-22.

transmission the Management Board and the Security Committee[550] has to be informed as soon as possible.

Comparing these rules with ones on personal data transmission to the third country discussed in previous subsection, regulation of classified information is more precise and narrow.

3.5. Data subject's right to access

Article 30 of the Europol Decision establishes the data subject's right to "obtain information on whether personal data relating to him or her are processed by Europol and to have such data communicated to him or her in an intelligible form, or checked."

The data subject can address his or her request to the designated authority of any Member State who shall forward it to Europol. Such a system facilitates the implementation of the data subject's rights, giving possibility to apply in Member States that are more convenient to a person due to his or her interests, language, place of residence or other motives.

According to Article 30.4, Europol, analysing the request, has to consult the "Member State concerned" before giving an answer without specifying which Member State it is: one that has forwarded the request or one that has submitted information (that in many cases will not be the same one that received the request). As such the Member State should be understood as one that has provided Europol with data as, despite of transmission, it remains responsible for personal data and besides, would probably have, or had, an investigation open. It can also be any other Member State that carries out investigation with a person who asks for the processing of his or her data.

Article 30.5 of the Europol Decision foresees that in some cases information cannot be given to the data subject. Such an obligation falls to Europol when it would jeopardise: the proper fulfilment of Europol's tasks, crime prevention, security, public order, national investigation and rights and freedoms of third parties. From this provision a conclusion can also be made that, "Member States concerned" which Europol has to consult are the ones that have submitted data and one that keeps investigation on that person. If the provision of information is forbidden, Europol notifies the data subject that checks have been carried out in such a

[550] The Security Committee is an advisory body to the Management Board and the Director in questions of information security. It consists of representatives of all Member States and Europol and meets at least twice a year.

manner that it would be impossible to verify whether the person's information is processed or not.

According to Article 30(7), requests for the processing of personal data can also be addressed to the Joint Supervisory Body, but its competence is limited only to the provision of the answer that relevant checks have been made. It would make sense if the reply to the request would jeopardise the performance of Europol's tasks or other interests mentioned above. But using systematic analysis of Article 30, a conclusion can be made that the Joint Supervisory Body can be requested in the same way as any authority of any Member State, and for any data processing; but it is authorized to limit answer as each request jeopardises Europol's tasks or national investigation.

A different situation arises when the Joint Supervisory Body is consulted as an appeal institution when the data subject:

- Is not satisfied with Europol's answer;
- Has not received any answer within four months[551].

In this case, before giving a response to the data subject, the Joint Supervisory Body has to consult:

- As a general rule, national supervisory bodies or competent judicial authority from Member State from which data was received or other Member State concerned;
- Europol, if information was introduced to the EIS by Europol or is in AWF. If Europol opposes to provide with data subject with information, the Joint Supervisory body only by qualified majority of its members can overrule such decision.

In relation to data correction or deletion, the responsibility rule is the same as for data accuracy, i.e. Europol corrects or deletes data received from third parties and Member States – submitted by them. In any case, Europol shall inform data subject in writing about the correction or deletion that has been carried out upon his or her request.

Despite the establishment of the data subject's access right, and the system of its implementation, for many years it could not be considered comprehensive due to the lack of clear judicial protection rules, as there was no judicial authority to whom Europol's decisions or those of its Joint Supervisory Body could be appealed.

[551] The designated authority has to forward a request without undue delay and in any case, not later than within one month. Europol shall answer without undue delay as well, and but not later than within three months.

It was of utmost importance, especially when taking into account that Europol tends not to reveal information to the data subject, motivated by the reason that it could be requested by organised crime members and therefore jeopardise investigation. Besides, the Joint Supervisory Body overruled such a decision / reply only in a very few cases. [552] The situation has changed, but only with the entrance into force of the Treaty of Lisbon; Article 263(1) of the TFUE allows individual claims to the Court of Justice of the EU against acts of all EU institutions and entities, including those of the former Third Pillar.[553] Nevertheless, no case has been filed yet.

3.6. Supervising authorities

In relation to the data processed by Europol, a three step mechanism supervising data protection is established:

- An independent national supervisory body in each Member State that monitors data input, retrieval and communication to Europol, and supervises the activities of its ENU and liaison officers when they are related to data protection.
- A Data Protection Officer established at the level of Europol[554] that acts independently and supervises compliance of the data protection provisions at Europol's level, by advising its staff and unit on data protection and by starting procedure relating to breach of data protection rules.[555] In the case of incompliance of rules, he or she informs the Europol Director about the need to resolve it. In case of non-resolution, the Data Protection Officer has the right to address this issue to the Management Board, and if the problem is not resolved– to the Joint Supervisory Body.
- A Joint Supervisory Body established at the level of the Europol and consisting of up to two representatives of each National supervisory body, supervising data subjects' rights in relation to the data held in Europol and monitoring its transmission. But when the data is exchanged between liaison officers for bilateral exchange, although on Europol's premises, the Joint Supervisory Body does not intervene, as such national and not Europol's data protection rules regulate the exchange.[556] When the Joint Supervisor Body detects any breach of data processing rules in Europol, it

[552] See MARICA, Andrea, *Manual de Europol,* op. cit., p. 218, 229-231.
[553] See ESQUINAS VALVERDE, Patricia, *Protección de datos personales en la Policía Europea* (Valencia: Tirant lo Blanch, 2010), p. 98-101.
[554] Appointed by the Management Board.
[555] See DREWER, Daniel and GUTIÉRREZ ZARZA, Ángeles, "Intercambio de información y protección de datos personales en el ámbito de Eurojust, Europol y OLAF" in GUTIÉRREZ ZARZA, Ángeles, *Nuevas tecnologías, protección…, o*p. *cit.*, p. 178.
[556] See BOEHM, Franziska, *Information Sharing and data…*, op. cit., p. 200.

informs the Director. According to Article 34(2)c, decisions related to breach are obligatory to implement. If the Director does not provide the problem's resolution, an issue is addressed to the Management Board.

All supervisory authorities shall be provided with access to the information stored by the authorities that are subject to their control:

- National supervisory bodies: to the data input to Europol's databases and premises of its ENU and liaison officers.
- Data Protection Officer and Joint Supervisory Body: to data held by Europol and on its premises (but not by liaison officers).

Despite multilevel data protection supervision, some kind of closed circle system than impugns its effectiveness can be observed. As already mentioned, the Data Protection Officer addresses data protection incompliance issues to the following authorities and in the following order: the Director, the Management Board and the Joint Supervisory Body. Thus it can be concluded that the Joint Supervisory Body is the highest authority in this chain to which issues, not resolved by the Director and the Management Board, are communicated. Nevertheless, as already mentioned, the Joint Supervisory Authority refers to the Director and to the Management Board, i.e. The same authorities that were consulted before.

On the other hand, problems arise when the responsibility of data stored in EIS belongs to Member States and not to Europol, because nowhere obligatory by the Joint Supervisory Body's decisions to Member States has been established.[557] In this case, the Joint Supervisory Body should have an opportunity to forward an issue to the national supervisory body of the Member State concerned, if it is related to sporadic infringement of data protection. In the case of repetitive infringement of data protection, or non-application of European legislation, there should be a possibility to address the issue to the European Data Protection Supervisor or to the European Court of Justice.

In the Draft Europol Regulation, the substituting Joint Supervisory Authority by the European Data Protection Supervisor changes this circuit. Thus a three level institutional system remains, but is headed by the authority with more power in the data protection area.[558]

[557] Ibid, p. 201.
[558] See Council document 10033/14, p. 97, 99.

4. Brief summary and evaluation

During the twenty years of its existence (counting from the establishment of the EDU), Europol has gone through development from a politically inspired organisation[559] established by a top-down decision[560], with a not very clear future in terms of its effectiveness and possibilities, to being granted with executive powers by the EU Agency, with precisely defined competence and reference in the primary EU legislation with the primordial task of "Information management together with the capacity to generate intelligence."[561]

Although EDU was created at the same time, when implementation of the CISA took place; further developments of Europol and Schengen Acquis have taken different paths. In the case of Schengen Acquis, it was more related to improvement of its functioning and embracing more new Members, and in the case of Europol – dynamic widening of its competence both in meaning of scope and co-operation methods and entities. A summary of what has been said in this Chapter about the scope of Europol's activities is presented in the following table.

Legal basis (signed/into force)	**Type of crimes**	**Conditions**
Treaty of Maastricht (1992/1993)	- Terrorism - Unlawful drug trafficking - Other serious forms of international crime	
Ministerial Agreement (1993)	- Illicit drug trafficking - Criminal organisations involved - Associated money laundering	Affecting two or more Member States
Amsterdam Treaty (1997/1999)	No changes of scope	
Europol Convention (1995/1998)	- Terrorism, - Unlawful drug trafficking - Other serious forms of international crime + - Money laundering and other crimes related the above mentioned	Possibly affecting 2 or more Member States and Organised crime involved.

559 ANDERSON, Malcolm, "Trust and Police Co-operation", loc. cit., p. 41.
560 BURES, Oldrich, "Europol's Fledging Counterterrorism Role" in *Terrorism and Political Violence,* 2008, vol. 20 (4), p. 501.
561 MARICA, Andreea. *Manual de Europol,* loc. cit., p. 119.

Legal basis (signed/into force)	Type of crimes	Conditions
Council Decision 2009/371/JAI	- Organised crime, - Terrorism, - Other forms of serious crime + - Related offences	Affecting 2 or more Member States.
Lisbon Treaty (2007/2009)	- Serious crime	Affecting 2 or more Member States or Terrorism and forms of crime which affect a common interest covered by a Union policy.
Commission's Proposal of Regulation	- Equally as Lisbon Treaty - Related offences	Equally as Lisbon Treaty
Parliament's Proposal	- Organised crime - Terrorism - Other forms of serious crime	Affecting 2 or more Member States in such a way to require a common approach by the Member States taking in account the scale, significance and consequences of the offence

Table 18: Development of Europol's competences.

With respect to the information exchange scheme, if at the beginning it took place only directly between Member States, later the scheme was changed, establishing co-operation in a chain: Europol – liaison officer – ENU and finally giving hit/no hit access to all interested law enforcement institutions. Forthcoming regulation foresees the possibility of direct co-operation between Europol and national law enforcement agencies as well. Thus Europol evolved from facilitating direct contacts between competent national authorities to the entity in possession of information and intelligence, and has become a much more active partner in combatting crime.[562]

With respect to the right to privacy and data protection in Europol's activities, the question is quite controversial.

First of all, referring to the establishment of restrictions by law, this requirement can be treated as fulfilled when democratically elected institutions have participated in its adoption. Thus provisions established by means of Convention or Treaties, fulfil this requirement due to their ratification by national parliaments. Future approval of Draft Europol Regulations will also be considered sufficient legal basis as the European Parliament is directly participating in the decision-making process. Europol Decision deserves a special mention. Even if it was approved according to existing legislative procedure, neither the European

[562] PEERS, Steve, *EU Justice and Home Affairs...*, op. cit., p. 873.

Parliament nor national parliaments directly participated[563] and ratification procedure was not applied.

Secondly, data processing for the purpose of combatting transnational terrorism, organised and serious crime can be treated as protection of general interest and be justifiable reasons to restrict fundamental rights.

Thirdly, proportionality of the processing of information to the purpose is a more complicated and versatile issue.

In the case of EIS, it contains information on very few categories of persons: suspects and convicted and besides includes limited categories of data. Such information is indispensable to combat cross-border crime and its processing is proportional to the purpose.

Nevertheless, the question stands in the case of the collection of special categories of data in AWFs, data transmission to third parties as well as onward transmission.

Special categories of data perhaps could help to identify the risks of radicalisation or extremism, but certainly do not have too much impact on combatting serious or organised crime. Therefore, its processing shall be, if not totally forbidden, used only in counter terrorism AWFs.

With respect to information transmission to third parties, on the one hand, it is understandable that if Europol needs information from them in order to ensure internal security of the EU, third parties will expect reciprocal actions from Europol. But such practice should be based solely on the basis of operational agreements, with the unique exception of combatting terrorism. In the case of onward data transmission, a third party that does not have an agreement with Europol, should not be able to receive it from another third party. As a general rule, it should send a direct information request to the Agency, and receive a direct response. The only exception could be when a transmitting third state proves that sharing information with another third party is indispensable for joint investigations in which both third parties are involved.

[563] The European Parliament had been consulted, but as according to legislative procedure that was in force, its opinion was not obligatory, the Council did not take it into account.

CHAPTER 5:
SWEDISH INITIATIVE

The established principle of availability would stay only a sound political declaration, without its proper implementation. For this purpose, a new mechanism was needed; one that would establish reasonable balance between obligations, in order to provide information, minimum possibilities to deny it and maximum data protection.

This Chapter presents how the Commission understood the principle of availability (treating it as an opportunity to create an integrated and comprehensive information exchange tool) how Member States (that still, even at the sight of a potential threat of terrorism, showed their protectionism and limited wish to share information) understood the same.

1. First attempt to implement the principle of availability: the Commission's proposal

Following the guidelines of the Hague Programme and implementing the Council and Commission Action Plan, implementing the Hague Programme on strengthening Freedom, Security and Justice in the European Union(564), in October 2005 the Commission presented a Proposal for a Council Framework Decision on the exchange of information under the principle of availability(565) (hereinafter – the Commission's Proposal).

564 OJ C 198, 12.8.2005, p. 1-22.
565 COM(2005) 490 final.

The proposal is worthy of appreciation as it is both comprehensive and ambitious.[566]

Comprehensive because of the intention to present it in the package with a proposal for a legislative act on the protection of data exchanged for the purpose of police and judicial co-operation in penal matters. But after the terrorist attacks of 7th July 2005 in London, the Council of Ministers of the Interior called the Commission to present the proposal on the implementation of the principle of availability, as soon as possible, leaving the data protection proposal for later.

Ambitious because of the attempt to create "direct online access to the available information and to index data for information that is not accessible online"[567] or in other words, complete implementation of the principle of availability.

It would oblige each Member State to grant direct access to its databases to competent authorities of other Member States, and to create index systems when some category of data is not available online. The Annex II of the Commission's Proposal has included exhaustive lists of the categories of data that are supposed to be directly accessible among Member States: DNA profiles, fingerprints, ballistics, vehicle registration information, telephone numbers and other communications data (excluding traffic and content), and persons' identification data.

Information availability would be limited to the exchange of already collected data, without the obligation to collect new data.

According to Articles 2 and 7 of the Commission's Proposal, the information exchange would take place before the commencement of a prosecution, and for the purposes of prevention and detection as well as investigation of crimes for which information has been provided.

As already mentioned, the proposed mechanism would include on-line access to existing databases and to databases of indexes, in cases of information not being stored in automated databases. That would result in the establishment of two modalities of information availability:

- Direct availability: direct access to the information in online databases of other Member States (Article 9);

[566] Although, for example VERVAELE calls it very general. See VERVAELE, John A. E., "Medidas de investigación de carácter proactivo y uso de información de inteligencia en el proceso penal" in PÉREZ GIL, Julio, *El proceso penal en la sociedad…*, op. cit., p. 35.
[567] COM(2005) 490 final, p. 2.

- Indirect availability: direct access to the index system of data not available online and in cases of an index match with the searched data information, receiving upon request and sent to the competent authority of the Member State whose index system was searched (Article 10). According to the Article 11, the requested authority would be obliged to respond within 12 hours.[568]

Article 14 of the Commission's Proposal has foreseen the ending of the list of motives to refuse the provision of information:

- To protect the security of persons and their fundamental rights;
- To protect sources of information or confidentiality;
- Not to prejudice of the on-going investigation;

The application of the aforementioned limitations would be completely possible in cases of indirect availability, as in this case, information would be forwarded by the possessing authority that at any moment can assess whether there are motives of refusal. But the question arises, how to apply these limitations in case of direct access to databases? It would be possible only with the application of a relevant technical solution in a database: either to withdraw information temporally from the database or to block access to it. But in both cases, it would be an additional burden to the data owning authority.

Kietz and Mourer have contemplated that "this decision, if adopted, would replace the reliance on national legal provisions for the exchange of personal data with common criteria that would apply to all EU member states. In contrast to the Prüm provisions, this would overcome the diversity of national legal assistance provisions, which so far have hampered the efficient exchange of information."[569]

But despite sound support for the principle of availability, Member States have refused this ambitious draft as "the regulation of the six key areas of information (DNA; fingerprints; ballistics; vehicle registrations; telephone numbers; other telecommunications data and minimum data for the identification of persons (identity, address) must be developed gradually, one by one."[570]

Both objective and subjective reasons for this rejection can be outlined.

---

[568] If there is a need for authorisation to provide the information, it has to be supplied within 12 hours of it being received.

[569] KIETZ, Daniela, MAURER, Andreas, "From Schengen to Prüm" (Comments, German Institute for International and Security Affairs, May 2006), p. 2, accesses November 14, 2014, http://www.swp-berlin.org/fileadmin/contents/products/comments/Com15_06_Ktz_Mrr_Ks.pdf.

[570] FAZEKAS, Judit, "Development of Justice and Home…", loc. cit., p. 8.

Among the subjective reasons, protectionism of national databases and lack of mutual trust can be pointed out as the main ones. The comprehension of the protection of internal security as a part of a State's sovereignty has been already mentioned in this work, and now we are facing one of the examples: Member States' have wished to keep direct access to their national database only to themselves. But the determining reasons for this refusal have been lack of trust that direct access would be used in a proper way, and only for the pre-established purposes. It would not be precise to talk about absolute mistrust, but more about differentiated treatment among Member States or different levels of mutual trust, as in 2005 seven States (Austria, Belgium, France, Germany, Luxemburg, the Netherlands and Spain) granted such access among themselves for DNA profiles', dactyloscopic's and vehicle registration databases (see the following chapter).

Regarding the objective reasons, of course implementation of such a mechanism would be very expensive and long-lasting due to the need to establish new databases or modify existing ones, and to ensure EU wide interoperability and technical capacity to deal with all searches. For example, the dactyloscopic database of one of the smaller countries would need technical capacity to provide access to the rest of the Member States and handle their requests on a daily basis.

Moreover, on 14th April 2005, the Council of Ministers of the Interior called for the evaluation of technical modalities that would be proper to every one of six information categories, recently included in the Commission's Proposal. As a result, in November 2005 a Report by the Friends of the Presidency on the technical modalities to implement the principle of availability[571] (hereinafter – Report) was issued. Report envisaged that in the case of telephone numbers and related data, as well as data for the identification of persons' direct access, it is not feasible because in many cases, the relevant databases are held by other entities than law enforcement agencies. In the case of persons' identification data, it pointed out, "Where data from such registers is available to a law enforcement officer domestically without judicial authorisation, the transmission of such data overseas should not be subject to judicial authorisation. In the longer term those Member States who require judicial authorisation should revisit this requirement in light of the principle of availability."[572] In the case of direct access to ballistics' databases, it is proposed as a long-term objective due to lack of the evaluation of the current state of play.

At the same time after experiencing terrorist attacks, Member States preferred to enjoy the immediate effect of the principle of availability, even if in limited scope; and that is why the Commission's Proposal were left without deeper analysis, and

[571] Council document 13558/1/05.
[572] Ibid, p. 40.

came back to a draft proposed by Sweden in 2004. As Jonathan FAULL (at that moment the Director General of the Commission's JHA Directorate General) said, "Our proposal [...] is seen by delegations [...] as a longer–term project which will provide for a wider sharing of information between law enforcement authorities of the Member States in the future."[573]

Seeing from another perspective, it was possible to reduce the number of categories of the exchanged information at the first stage, leaving, for example, ballistics and telephone numbers and other communications data for later. Especially taking into account that in the end, in a little bit more than one year, at the beginning of 2007, during the German Presidency of the Council, a draft on the automated access to national DNA, dactyloscopic and vehicle registration files was proposed; and approved in 2008 (see the following Chapter). Essential difference from that proposal was envisaging mutual evaluation of legal and technical, data protection readiness as a pre-condition to direct access.

Curiously, a suggestion made in the Report about the possibility of the effective application of the principle of availability to data related to explosives, synthetic drugs profiling and trade registers has never been taken into account by the Member States; although after the terrorist attack in London in 2005, the Ministers of the Interior agreed on a need to improve information sharing on explosives.[574]

Thus instead of the ambitious and comprehensive Commission's Proposal, the Member States had chosen much more simplified and more easily implemented legislation on information exchange and implementation of the cornerstone principle of police co-operation – the principle of availability.

2. Swedish Initiative – compromise on information availability

Instead of the unsuccessful Commission's Proposal, the Council went back to the Swedish proposal from June 2004, and after multiple rounds of discussions and numerous compromises on 18th December 2006, adopted the Framework Decision 2006/960/JHA, previously mentioned in section 3 of the Chapter III, also popularly called the "Swedish Initiative". As this legal act modifies some provisions of the *Schengen Acquis*, Norway, Island, Lichtenstein and Switzerland also joined it.

[573] HEMPEL, Leon; CARIUS, Michael and ILTEN, Carla, "Exchange of information and data between law enforcement agencies within the European Union" (Discussion paper Nr. 29/09, Zentrum Technik und Gesellschaft, 2009), p. 28, https://www.tu-berlin.de/uploads/media/Nr_29_Hempel_Carius_Ilten.pdf.

[574] See Council document 11116/05, p. 7.

Martínez Pérez and Poza Cisneros define it as "The first approximation in the implementation of the principle of availability that gets beyond the primitive bilateral stage."[575]

The Swedish Initiative, like the Commission's Proposal, foresees broader scope of information availability than only combatting terrorism and it includes other crimes as well.[576] As noticed by Hempel, Carius and Ilten, "In the Framework Decision the key concern of the proposal has been made invisible: the phrase referring to terrorism in the title is deleted. Terrorism is now seen — so to say, normalised — as one serious offence among others."[577]

Article 1(4), 1(5) of Framework Decision 2006/960/JHA establishes what is not covered and what is not required by this instrument: to collect and store information for its transmission, to obtain it by coercive measures or provide it as evidence. As stated by Mitsilegas, "These provisions can be seen as an attempt to safeguard national autonomy in not requiring national authorities to be proactive in obtaining information or intelligence on behalf of their counterparts in other Member States."[578]

Differently from the Commission's Proposal, Article 3(2) of the Framework Decision 2006/960/JHA establishes:

- Information exchange on the basis of requests, i.e. Indirect exchange without the possibility to access other Member States' databases;
- Spontaneous information exchange possibility for prevention, detection and investigation of crimes listed in the previously mentioned Framework Decision 2002/584/JAI.[579]

As correctly pointed out by Leinius, "This system of indirect access and case-specific requests does not completely abolish the autonomy of law enforcement authorities in deciding whether to transfer data, but nevertheless, the Swedish Framework Decision constitutes an important first step towards realizing the principle of availability."[580]

---

[575] MARTÍNEZ PÉREZ, Fernando and POZA CISNEROS, María, "El Principio de Disponibilidad: Antecedentes Penales y Convenio de Prüm". In CARMONA RUANO, Miguel; GONZÁLES VEGA, Ignacio U. and MORENO CATENA, Víctor, *Cooperación Judicial Penal..., o*p. cit., p. 420.

[576] See HEMPEL, Leon; CARIUS, Michael and ILTEN, Carla, "Exchange of information and data…", loc. cit., p. 25.

[577] Ibid.

[578] See MITSILEGAS, Valsamis, *EU Criminal Law*, op. cit., p. 254.

[579] See footnote 382.

[580] LEINIUS, Katharina., *An Imbalance between Security*…, loc. cit., p. 11.

2.1. Scope of information exchange

Although the Swedish Initiative is quite a short legal document (13 articles in total), it is not as simple as it may look at first. For example, in order to identify its scope, four articles should be taken into account:

- Articles 1 and 3(2) that establish as a purpose for information exchange, "Conducting criminal investigations or criminal intelligence operations."
- Article 5 that foresees information requests for the "Purpose of detection, prevention or investigation of offences."
- Article 7 that limits the spontaneous sending of information to assist, "In detection, prevention or investigation of offences to referred in Article 2(2) of the Framework Decision 2002/584/JHA."

This variety of definitions can lead to misunderstandings among law enforcement agencies at the time of practical information exchange, because requesting the country can base its request on the basis of Article 5, and ask the information for crime prevention for non-serious crime, and the requested country can base its answer on Article 3(2) that obliges it to provide information only for the purpose of ongoing investigations or intelligence operations. Thus as a general rule, information will be provided only for the purposes established in the Article 1 and 3(2), but problems can arise in cases of crime prevention. The prevention purpose established in Article 7 does not coincide with Article 1 and 3(2), but limitation to crimes listed in Article 2(2) of the Framework Decision 2002/584/JHA in Article 7 can be justified, as here, the legislator refers to spontaneous submission of information, and in order to make this flow proportionally, it is allowed only in cases of more serious crimes.

2.2. Deadlines for reply

Article 4 of the Framework Decision 2006/960/JHA foresees deadlines in cases of urgent information requests, limiting answers to:

- 8 hours in urgent cases when it is related with the crimes listed in the Art. 2.2 of the Council Framework Decision 2002/584/JHA, and when requested information is directly accessible by the requested law enforcement institution. This time limit can be extended to 3 days when replies would represent a disproportional burden.
- One week in non-urgent cases under the conditions of the previous indent.

- Fourteen days in any other cases, i.e. Crimes not included on the list provided in the Art. 2.2 of the Council Framework Decision 2002/584/JHA, and with irrelevance to the request's urgency.

Unfortunately, apart from the very detailed examination of the draft Swedish Initiative in the Council's preparatory body, the notion of urgency was not determined.

To avoid totally different interpretations of this important term, the Member States tried to establish some framework of urgency in the Guidelines on the implementation of the Council Framework Decision 2006/960/JHA of 18th December 2006, on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union[581] (hereinafter – the Guidelines). They foresee that urgency has to be established on a case by case basis, but taking into account whether it is related to:

- Prevention of risk of death / harm to persons or serious damage to property;
- Short-term decisions about deprivation of liberty;
- Prevention of information loss that can affect the investigation.

Let's analyse how this system of information exchange would work in the case of a person's identity check on his arrival from a third country at Adolfo Suárez Madrid–Barajas Airport.[582] Based on the pre-established criteria or unusual behaviour of a person, a border guard officer can suspect that the presented identification document belonging to another state of the Schengen area is false. A check in SIS does not give a positive result on matching with lost or stolen documents, but it does not eliminate the possibility that the document is misused as there are cases when identification documents are sold by the legal owners and of course, such documents are not declared either as lost or stolen, and will never appear in SIS. In this case, there is a need to check in the database of the country that has issued the document, whether the identity of the person registered in the database matches the identity of the person that presenting the document at the airport, e.g. Coincidence of names and surnames, date of birth, photo and other elements.[583] The person concerned can be detained for identity misuse, or use of

[581] Council document 9512/1/10.

[582] That means that a person has crossed an external border of the Schengen area and despite whether he or she is a national of one of the countries forming Schengen area or not, an identity check has to be performed.

[583] In some cases, none of this information is altered, but the ID is misused and only on the basis of answers to additional questions about the person's identity (such as names, dates of birth of family members, place of issue of the ID document, etc.) is it possible to verify the misuse. The performance of this questioning is possible only by having accessible data from the Civil Registry or equivalent database.

false documents and according to the criteria of urgency established in the Guidelines, it should be treated as urgent. But on the other hand, the use of false documents is not included in the list of Art. 2.2 of the Framework Decision 2002/584/JHA (only falsification and trafficking of administrative documents, but not their incidental use) and thus the situation does not match the legal requirements for urgency, established in the Article 4(1) of the Framework Decision 2006/960/JHA. What should prevail in this case: obligatory provision of the Article 4(1) or non-obligatory Guidelines that refer to the protection of a fundamental human right - liberty?

Of course, limitation of urgency to more serious crimes can be justified by limited resources of every state, to provide information on any kind of investigation or intelligence operation within 8 hours. Another consideration that has to be taken into account is the "fairness" of the state in using urgency, or, in other words, abusing the label of urgency in cases that really can wait.

From another point of view, this problem would not appear in cases of direct access to databases, which would be established as it was foreseen in the Commission's Proposal.

This uncertainty about urgency plays an even bigger role in information exchange, taking into account that according to the Council's Working Party's on Data Protection and Information Exchange (hereinafter – DAPIX group) Report from 2012, participating states use this instrument mainly for urgent information requests and for the rest of the cases, other information exchange instruments are used.[584] With respect to its compliance, the Commission's Staff Working Paper on the implementation of the Swedish Initiative indicates that "Member States do take urgent requests seriously. 26% of Member States report that such requests have always been complied with while 62% of Member States report that they have often been complied with. On the negative side, 9% of Member States see no compliance at all while 3% see compliance as a rare occurrence."[585]

The problem of deadlines only occurs in case of implication of judicial authorisation for information exchange.[586]

2.3. Data exchange and reasons for denial

Article 2(d) of the Framework Decision 2006/960/JHA establishes that the object of exchange could be any type of data held directly by the law enforcement

[584] See Council document 14755/1/12, p. 19-21.
[585] SEC(2011) 593 final, 9.
[586] See Council document 14755/1/12, p. 4.

authorities, or by public or private authorities and available for law enforcement purposes. But on the other hand, unlike the Commission's Proposal, no minimum categories of information that must be exchange are envisaged; i.e. There is no assurance that at least some minimum categories of information and data will be available across the whole EU. It leads to great differences of information availability between countries, as some of them will be obliged to provide many categories of information (everything available), while others would provide very few of them as only those categories are available to law enforcement institutions. It definitely will not help to build common trust and readiness to share information, taking into account that as feedback, very few categories can be received.

As in the Commission's Proposal, Article 3(4) foresees that when judicial authorisation to supply requested information is needed, the requested authority shall apply for it.

In comparison with the Commission's Proposal, Swedish Initiative foresees different motives to withhold information.

Article 14 of the Commission's proposal	**Article 10 of Framework Decision 2006/960/JHA**
- Dispositive - To protect the security of persons and their fundamental rights - To protect sources of information or confidentiality - Not to prejudice the on-going investigation	- Obligatory - Lack of judicial authorisation - Dispositive - Damage of national security interests of the requested MS - Prejudicing the success of ongoing investigation or intelligence operation in requested MS - Individual's safety - Disproportion with the purpose of request - Request on offence with the imprisonment punishment of one year or less in requested MS

Table 19: Obligatory and dispositive reasons to deny provision of information according to the Commission's proposal and Framework Decision 2006/960/JHA.

Both provisions have their advantages and disadvantages:

– The Commission's proposal foresees broader protection of the person and is not limited to safety only. It also foresees the possibility to protect information by itself (confidentiality, sources).

- The Swedish initiative envisages proportionality of information for the purpose and possibility, and to deny provision of information if it jeopardises national security.

Half of the motives foreseen in the current legislation are related to requested Member States and reflect the tendency of protection of its interests. It can be understandable in cases of damage to national security, but it raises doubts about linking availability of information to crimes with punishment of imprisonment of more than one year. It makes investigation, or other actions of the requesting party, conditional to punishments foreseen by legislation of the requested Member State. And as it is a dispositive provision, again it shows disproportion between information that will be provided by different Member States. Besides, all or part of dispositive refusal reasons can be established in national law as obligatory ones. But if such rules are equally applied to information transmission at national level, it does not mean the breach of the principle of availability, as national law enforcement authorities and those of other Member States are put under the same legal requirements.[587]

In relation to reasons of ongoing investigation, the wording of the Commission's proposal was more precise as a request can jeopardise not only investigation carried out by the requesting party, but also by another Member State, and on some occasions the requested Member State can be aware of that (for example when it already provided information to another state).

Despite quite superficial regulations in general, Framework Decision 2006/960/JHA contains two Annexes that provide the forms that have to be used as requests and as denial. The form of request includes twelve comprehensive fields to be filled in. On the one hand, it allows assurance in relation to the purpose of request, but on a the other it discourages the use of this basis of co-operation, especially in non-urgent cases as it is much easier to write a free-text request and to send it through INTERPOL channels.

2.4. Practical use

Despite the hurry of Member States to have a universal instrument allowing information availability, the implementation of the Swedish Initiative took much longer than had been foreseen. As an established indirect information exchange does not suppose complicated and expensive implementation measures, the

[587] As happened, for example, when implementing Swedish Initiative in Germany. See more. BOERGER, Björn, "The transmission of personal data as part of the police and judicial cooperation in criminal matter in the EU: German experience" in COLOMER HERNÁNDEZ, Ignacio and OUBIÑA BARBOLLA, Sabela, *La transmisión de datos personales…, o*p. cit., p. 252, 266.

reason should be to its disadvantages, or lack of strong added value in comparison with the already used information exchange mechanisms.

Article 12(6) envisaged the deadline of the implementation as19th December 2008. Nevertheless, even now, nine years after its adoption, some Member States (Greece, Italy and Luxembourg) are lacking national implementation.

Even Germany, always being the pioneer in police and judicial co-operation measures, only finalised adoption of implementing rules in 2012.[588]

As stated in the Council's Report from 2011, "The general standards for cross-border information exchange asked for by the Decision were often already in place. Therefore, it was stated that the process had not notably been improved. From a specific technical point of view, it has to be noted that the required use of form A and B for submitting and requesting information, complicates information exchange as they are deemed to be cumbersome. [...]"[589]

On this basis, the following question can arise: does the Swedish Initiative really have added value in information exchange and implementation of the principle of availability? Or was it a measure adopted just to demonstrate European political concern about information exchange, and to somehow fulfil tasks established by The Hague Programme?

Of course any draft that needs a unanimous agreement of 25 Member States[590] can be much diluted from content and obligations, and that probably happened with the Swedish Initiative. But is it possible to regulate such broad scope of information exchange by the legal act of 13 articles in total, with 10 of them dedicated to regulate this process?

From another perspective, such aspects as uncertainty of the purpose of its use, or tremendous form for the simplest information request force us to think whether the Council and preparatory body really took their task to facilitate information availability seriously. And should it be implemented by the indirect information exchange that has existed ever since, but now using complicated request forms instead of the free-text messages that every law enforcement agency was used to? What added value does a three-page form have, furthermore, one that has more similarities with European Arrest Warrant that with simple information exchange?

This has made the Swedish Initiative a limited used mechanism only for situations of urgency and additionally, not in all States. Only Slovenia and Sweden use this

[588] See BOEGER Björn, "The transmission of personal data…", loc. cit., p 252.
[589] Council document 15278/11, p. 6.
[590] At the moment of its adoption, Bulgaria, Romania and Croatia were not EU Member States yet.

instrument frequently and other Member States "do not draw on it on a regular basis."[591] But even in this case, Swedish law enforcement authorities use the form only when it is specifically indicated by the requested Member States.[592]

As pointed out in the Study of the International Centre for Migration Policy Development, "Users prefer free text reporting, instead of filling in several pages of modular information, increasing time spent handling the requests. Even the simplified version of form B, developed during the Czech Presidency, has not brought the expected results."[593]

DAPIX group has agreed on the possibility to use a simplified request form that in any case has to include data on:

- Requesting authority and Member State, requested Member States, date and reference number;
- Level of urgency and in cases of urgent request – the reasons for that;
- Indication of what information is requested and for what purpose;
- Crime commission circumstances, identity of persons and the main objects of the investigation (if known);
- Link between requested information and investigation;
- Reasons to believe that the requested Member States may have requested information;
- Limitation on information provided in the request use.

But these modifications were not formally introduced into the Council Framework Decision 2006/960/JHA, so the question of their legality stands. From another angle, some States (Spain, Switzerland, Lichtenstein) literally implemented the official text of the Swedish Initiative in the national legislation and have foreseen obligatory use of the request form and cannot use the simplified one.

In addition to all practical inconveniences and unlike the Commission's Proposal, the Swedish Initiative does not foresee any obligation to gather statistics on its use, and therefore there is no way to measure its real (even little) effectiveness and to identify areas of improvement. As indicated by the Council, "It has to be stated that the majority of Member States does not produce complete and comparable SFD statistics: 14 MS of those having implemented the SFD clearly have no such

591 SEC(2011) 593 final, p. 6.
592 Council document 14755/1/12, p. 17.
593 INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT, "Study on the status of information…", loc. cit., p. 40.

statistics, 5 indicated to keep annual statistics and 5 do so only with regard to information shared with Europol."[594]

In non-automated information exchange, the collection of statistics is an additional burden for law enforcement institutions; in cases of automated information exchange (access to databases) it would be a technical solution that does not require any further efforts and can be used additionally for supervision of data protection.

3. Data protection

As the Swedish Initiative by itself is a very laconic legal instrument, provisions on data protection tend to be too, and are regulated by Articles 8 and 9.

Article 8 foresees a double data protection regime:

- For information exchange as such, data protection rules applied to the channel of communication are used. Thus if information is requested through SIENA, Europol's data protection rules will be obligatory.
- Use of received information, as a general rule, is regulated by the national law of the receiving Member State that must be in conformity with the European Convention on Data Protection, and should take into consideration Recommendation (87) 15.

Nevertheless, the requested Member State can foresee conditions on its use and reporting results. But such special conditions will not be applied to judicial, legislative and other institutions performing supervisory functions of law enforcement authorities. In any case, the opinions of transmitting Member State have to be taken into account as far as possible.

Transmitted information can be processed only for the purpose for which it was transmitted. Its use for other purposes has to be authorised by requested Member State, and envisaged by the national law of receiving one.

With respect to confidential information and intelligence, Article 9 only entails the application of relevant national provisions. Even if the legislator does not explain whether it is applied only in order to reply or also in order to request, it should be applied to both, as request can also contain confidential information in relation to the investigation performed.

[594] Council document 14755/1/12, p. 4.

As already mentioned, the Commission had had an intention to present a package of information availability tools, accompanied by its proposal on data protection, but due to the terrorist attack of 2005 in London, it was encouraged to present just the proposal on the implementation of the principle of availability leaving the data protection proposal for later.

Thus *lex generalis* of data protection for Swedish Initiative Framework Decision 2008/977/JHA was adopted just one month before the deadline of the implementation of the Swedish Initiative, but with its own implementation deadline until November 2010. Thus the Commission's concept of a package of principle of availability and data protection only became real, at least in its form, at the end of 2010.

4. Brief summary and evaluation

The Framework Decision 2006/960/JHA was the first attempt to implement the principle of information availability, where Member States, after sound declaration of the need to significantly improve information exchange, have chosen quite superficial mechanism for its implementation. Regulation does not provide clarity of purpose; it includes very few provisions on data protection and establishes complicated data exchange forms.

The only advantage can be considered an obligatory timeframe to provide information for urgent requests. Notwithstanding, it also has its problems as the definition of urgency is not provided and its misuse cannot be controlled. Additionally, some of the existing information exchange tools can also be effectively used for urgent information exchange. For example, Europol is usually used to getting urgent information as it hosts liaison officers from all Member States, and they normally have access to national data bases; bilateral agreements regulating PCCC and also foresee exchange of any information, and, as they are usually working 24/7, there is no problem in getting information urgently.

As a result, even after almost a decade the information exchange background is not widely used, and instead of being a universal law enforcement information exchange tool, the Swedish Initiative is treated as "an optional / supplementary legal instrument for sending requests for information."[595]

[595] Ibid, p. 16.

Thus to make the principle of availability work effectively, an innovative and open-minded approach is needed[596] and it seems that it had been followed in the Commission's Proposal, but Member States were not ready to accept it.

[596] VERMEULEN, Gert; VANDER BEKEN, Tom; VAN PUYENBROECK, Laurens et al. *Availability of law enforcement information in the European Union. Between mutual recognition and equivalent right of access.* Antwerp: Maklu Publisher, 2005, p. 47.

CHAPTER 6:
EXAMPLE OF NETWORKING: FINANCIAL INTELLIGENCE UNITS AND ASSET RECOVERY OFFICES

The analysis would not be overall without the study of such information exchange tools as networks.

Although the word "network" can appear not to be very serious in the context of law enforcement authorities, well defined and regulated networks are very useful tools to put specialised experts in contact; furthermore, in cases of necessity they can make contact directly and exchange information according to an agreed legal basis. As examples of such network the European Network for the Protection of Public Figures, the European Network of National Officials to Detect and Combat New Cases of Cross-Border VAT Fraud, Contact-Point Network Against Corruption can all be mentioned.

Regarding the EU primary law, Article 85 of the TFEU expressly mentions only European Judicial Network, leaving the rest of the networks up to the necessity of co-operation.

Among different existing networks, as objects for further analysis, the following have been selected:

- Network of FIUs (network of Financial Intelligence Units for the information exchange on suspicious transactions, that can be related to money laundering or terrorism financing) officially created by the Council Decision 2000/642/JHA of 17th October 2000 concerning arrangements for co-operation between the Financial Intelligence Units (FIUs) of the

Member States in exchanging information[597] (hereinafter – Decision 2000/642/JHA)

- Network of AROs (network for the tracing and identification of ill-gotten gains[598]) officially created by the Council Decision 2007/845/JHA of 6th December 2007 concerning cooperation between the Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime[599] (hereinafter – Decision 2007/845/JHA).

These networks were elected for several reasons; first of all, because their aims are directly related to the fight against illegal proceeds that circulate around the world as a side effect of free financial markets. Money laundering was mentioned as one of the factors that gave raise to international police co-operation as it is a "global business" and "The United Nations Office on Drugs and Crime (UNODC) estimates that the sum of money laundered globally amounts to between 2 and 5% of global GDP or between EUR 615 billion and EUR 1.54 trillion each year."[600]

Secondly, because the final goals of FIUs and AROs networks are the same, although they have different regulations and different information exchange rules (for example, in Denmark both units are situated in the State Prosecutor for Serious Economic Crime, but different regulation to their co-operation is applied).[601]

Thirdly, the FIU network has a new regulation that is one of the last legislative developments.

1. Network of Financial Intelligence Units (FIUs)

Although the first anti-money laundering regulation within the European Communities was adopted in 1991 as Council Directive 91/308/EEC, with the aim of establishing links between suspicious financial transactions and underlying criminal activity, in order to prevent and to combat money laundering,[602] (the so called First AML/CFT Directive), at that moment its focus was on obliging credit and financial institutions to identify suspicious financial transactions without any reference to cross-border information exchange.

[597] OJ L 271, 24.11.2000, p. 4-6.
[598] Council document 9741/13, p. 50.
[599] OJ L 332, 18.12.2007, p. 103-105.
[600] EUROPOL, "EU Serious Organised Crime Threat…", loc. cit., p. 27.
[601] Council document 9741/13, p. 27.
[602] OJ L 166, 28.6.1991, p. 77-82.

Within the following decade, Member States established FIUs or endowed already existing competent authorities with this function.

At global level, in 1995 the Egmont Group, as an informal group to facilitate international co-operation in the fight against money laundering and terrorism financing was established. Currently, this group unites FIUs from 151 countries and has stable structure with division by topics and regions. Nevertheless, information exchange within its framework takes place under the principle of reciprocity, which does not always ensure effectiveness.[603]

Therefore, within the EU Decision 2000/642/JHA was made. It provides us with the following FIU definition: "A central, national unit which, in order to combat money laundering, is responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information which concern suspected proceeds of crime or are required by national legislation or regulation."[604] According to its Article 3, depending on national structure, it can be an administrative, police or judicial entity, but its national status does not have to be an obstacle for effective co-operation.

Its Article 1 established possibilities to exchange information on request, or spontaneously between the FIUs of Member State. The scope for information exchange is defined very broadly foreseeing that it is, "any available information that may be relevant to the processing or analysis of information or to investigation by the FIU regarding financial transactions related to money laundering and the natural or legal persons involved."

Requests shall provide requesting Member States with the facts related to the investigation or suspicions, as well as with information on how the received information will be used. For requests sent on the basis of this Decision, relevant information shall be answered without any additional requirement to send another request on the basis of bilateral or multilateral agreements. The receiving Member State has to follow the limitations of use of data, foreseen by the requested Member State.

To make this information as available as possible, Decision 2000/642/JHA establishes only three backgrounds of denial: ongoing criminal investigation in the requested Member State, disproportion between the revealing of information and the legitimate interests of person (data subject) or requested Member State; disagreement with other crucial legal principles of the requested Member State.

---

[603] See The Egmont group of Financial Intelligence Units, accessed August 2, 2015, http://www.egmontgroup.org/membership.

[604] See Article 2 of the Decision 2000/642/JHA.

In the same year France, Italy, Luxembourg, the Netherlands and the United Kingdom started a FIU.NET project that became operational in 2002, and its development will be finished in 2016.

FIU.NET first of all is a secure system connecting all FIUs and allowing di-personalised searches for information through "Ma3tch" tool (Autonomous Anonymous Analysis) and allows data from different FIUs to be matched, retaining its anonymity, detecting similarities and interrelation.[605] Nevertheless, there is no regulation on post-hit information exchange in relation to what conclusion can be made about any of the established information exchange tools being used: information exchange through Europol, on the basis of the Swedish initiative, through liaison officers, and so on. .

Although it was mentioned that the First AML/CFT Directive had not regulated cross-border co-operation and FIUs, the following AML/CFT Directive[606] actually did.

The last one, the Fourth AML/CFT Directive (Directive (EU) 2015/849 of the European Parliament and of the Council of 20th May 2015 on the prevention of the use of financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC)[607] provides very comprehensive regulation of FIUs; first of all drawing attention to their operational independence, i.e., "The FIU has the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and disseminate specific information." It also lays down extensive regulation of co-operation between FIUs.

Thus Article 52 establishes that "Member States shall ensure that FIUs cooperate with each other to the greatest extent possible, regardless of their organisational status."

Unlike Decision 2000/642/JHA, exchanged information is not only related to money laundering, but to terrorism financing as well. Maintaining requirements to provide investigation facts, and how data will be used, it is required to mention reasons for requests being made. Nevertheless, if the type of offence implied is not yet determined, this is not a reason to deny the request.

---

[605] See FIU-net, accessed August 2, 2015, https://www.fiu.net/fiunet-unlimited/match/match3.

[606] See Chapters III and V of Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p. 15-36.

[607] OJ L 141, 5.6.2015, p. 73-117.

With regard to the co-operation channel, FIU.NET is mentioned in particular; but it does not impede the use of others.

Article 53.2 includes a provision that reiterates principles of information availability by establishing that, "Member States shall ensure that the FIU to whom the request is made is required to use the whole range of its available powers which it would normally use domestically for receiving and analysing information when it replies to a request for information [...] from another FIU."

The fourth AML/CFT Directive remains only one reason for the denial of information that is "Fundamental principles of its national law."

Summing up, it can be said that the latest developments related to the FIU network comprehensively cover legal aspects of co-operation and give state-of-the-art technical background to its implementation.

2. Network of Asset Recovery Offices (AROs)

If FIUs are dedicated to analytical, intelligence-led work, specialising in identifying suspicious transactions that can be related to money laundering or the financing of terrorism, AROs are oriented to looking for criminal proceeds, their seizure and confiscation. Thus if the FIUs role is more proactive or warning, the AROs role is more reactive, designed to deprive criminals from benefit, and to ensure that "crime does not pay".

The origins of co-operation in tracing, freezing, seizing and confiscating criminal proceeds can be found in the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (CETS 141) of the Council of Europe.

Within the European Communities, one of the first legal acts on this topic was Joint Action 98/699/JHA of 3th December 1998 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime[608] (hereinafter – Joint Action 98/699/JHA). It entailed an obligation to establish national legal provision that would allow, upon request from other Member States the identification and tracking of criminal proceeds, and foreseeing the necessity of approximation of laws on criminal assets seizure and confiscation.

Later, a range of political declarations strengthened the importance of this issue. For example, the Tampere Conclusions envisaged that money laundering "should

[608] OJ L 333, 9.12.1998, p. 1-2.

be rooted out wherever it occurs", the Hague Programme pointed out, "The monitoring of suspicious financial flows and the freezing of assets" [609]

In September 2004, Austria, Belgium, Germany, Ireland, the Netherlands and the United Kingdom established CARIN – a global network for the purpose of exchange of experience and best practice in order to deprive illicit proceeds.[610] Nowadays, it associates more than fifty national authorities from Europe and the United States, nine international organisations and is linked with equivalent networks in Asia Pacific, Latin America and South Africa.[611] Nowadays its Secretariat is hosted within the Europol Criminal Asset Bureau.[612]

The CARIN network is not authorised in case-related data exchange, and therefore within the EU[613], in 2007 Decision 2007/845/JHA was adopted. It has emphasised the need for effective tracing of assets, that can be reached by rapid and direct information exchange between competent authorities. From its Article 2 a conclusion can be made that, depending on peculiarities of national systems, ARO can be within an administrative, law enforcement or judicial authority. Each Member State can nominate up to two AROs. Thus, for example:

- France, first nominated the Central Department of Judicial investigation and later Agency for Administration and Recovery of Seized and Confiscated Assets as an ARO; managed by the Ministry of Justice and the Ministry of Finance;
- The United Kingdom nominated the Serious Organised Crime Agency (for England, Wales and North Ireland) and Scottish Crime and Drug Enforcement Agency (for Scotland) as AROs.[614]

According to Article 3 of the Decision 2007/845/JHA, information requests to AROs of other Member States can be sent either by national ARO or another authority "charged with the facilitation of the tracing and identification of proceeds of crime". Thus the requested authority will always be an ARO, but the range of requesting authorities is wider.

---

[609] OJ C 53, 3.3.2005, p. 8.

[610] See "Camden Asset Recovery Inter-agency Network (CARIN)", Europol, accessed August 2, 2015, https://www.europol.europa.eu/content/camden-asset-recovery-inter-agency-network-carin-leaflet.

[611] Ibid.

[612] See EUROPOL "Camden Assets Recovery Inter-Agency Network (CARIN): the History, Statement of Intent, Membership and Functioning of CARIN. Manual", 2012, p. 3, accessed August 3, 2015, https://www.europol.europa.eu/content/publication/camden-asset-recovery-inter-agency-network-carin-manual-1665

[613] See EUROPOL. "Camden Assets Recovery…", loc. cit., p. 3.

[614] See CORRAL ESCARIZ, Vicente, "La nueva estrategia económica contra la delincuencia organizada y la corrupción: comiso y recuperación de activos. XXIV seminario "Duque de Ahumada" in *La Guardia Civil en la lucha contra la Delincuencia Económica* (Madrid, 2013), p. 105, 108.

As the legal basis for request Framework Decision 2006/960/JHA was established, from Decision 2007/845/JHA, a conclusion can be made that use of the request form of the Swedish Initiative is obligatory, and shall include reasons for the request, as many details as possible, details on the property looked for and the persons presumed to be involved (or to whom the property could belong).

As reference is made to the Swedish Decision, for denial of information, backgrounds established in its Article 10 are applied, i.e. Offence punished with less than one year of imprisonment, risk to national security, undergoing investigation or intelligence operation in the requesting Member State, jeopardising individuals' safety or disproportionality.

Decision 2007/845/JHA also allows the spontaneous provision of information between the aforementioned authorities when it is considered useful for the performance of the ARO functions of the receiving Member State.

In relation to the recuperation of crime benefits, in 2008, a Communication from the Commission to the European Parliament and the Council, "Proceeds of organised crime: Ensuring that "crime does not pay", was issued. It emphasised the importance of "national agencies charged with tracing assets are a precondition for a successful confiscation, as well as for international cooperation."[615] It also pointed out access to relevant databases, granting of coercive and provisional freezing powers to AROs and effective co-ordination (with suggestion to endow it to Europol) as indispensable elements for effective asset recovery.[616]

Later, illicit proceeds were the object of the Stockholm Programme that called upon their more effective identification and seizure (but within the context of combatting terrorism)[617] ,and an Internal Security Strategy that foresaw the involvement of information from private sector for the tracing of assets.[618]

Although according to Decision 2007/845/JHA, Member States had to establish their ARO until the end of 2008, in 2010 the Council Conclusions on Confiscation and Asset Recovery[619] and in the Communication on Implementation of ISS, obligation to establish fully functioning ARO was still reiterated.[620]

[615] COM(2008) 766, final, p. 3.
[616] COM(2008) 766, final, p. 9.
[617] OJ C 115, 4.5.2010, p. P. 23.
[618] COUNCIL OF THE EUROPEAN UNION, "Internal Security Strategy…", loc. cit., p. 23.
[619] Council document 7769/3/10.
[620] Ibid, p. 6.

In 2011, ARO were not still notified by Malta, Italy, Portugal and Slovenia.[621] In the case of Italy, creation of ARO (National Agency for the Administration and Use of Seized and Confiscated from Organised Crime) was established by the Law 50/2010, but at the moment of the Commission's Report, it was not yet functioning. [622]

In October 2012, there were still two Member States without ARO, and the Council, in its Final report on the fifth round of mutual evaluations - "Financial crime and financial investigations" stated that Member States were still encouraged to promote efficient co-operation through AROs and "when possible, pro-actively and exclusively use this channel in the fight against financial crime as regards asset recovery."[623]

3. Data protection

As both networks have different legal bases. Their data protection regimes are also different.

Decision 2000/642/JHA makes a reference to the European Convention on Data Protection, its Protocol and Recommendation R(87) 15 as principles that have to be followed in information exchange between FIUs. The only specific rule foreseen by Decision 2000/642/JHA prohibits access to submitted information by any other authority than FIU.

The fourth AML/CFT Directive is less strict and foresees the possibility of access to other competent authorities, but only with the prior consent of the requested FIU that can refuse such consent only for the same reasons as applied to information denial for requests for information.

It also established that *lex generalis* applied to the co-operation of FIUs and the implementation of this directive in general is Directive 95/46/EC, and the Regulation is Regulation 45/2001 of the European Parliament and of the Council of 18th December 2000, which focused 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[624] (hereinafter – Regulation 95/46/EC). That means that the European legislator did not treat the Fourth AML/CFT Directive as one falling into the category police and judicial co-operation, because in such cases

[621] See COM(2011) 176, final, p. 2. It also mentioned Romania among those who had not been notified about the national ARO, but the notification was sent in May. See Council document 10218/11. Brussels, 19 May, 2011.
[622] See CORRAL ESCARIZ, Vicente, "La nueva estrategia económica…", loc. cit., p. 107.
[623] Council document 12657/2/12, p. 27.
[624] OJ L 8, 12.1.2001, p. 1-22.

it would be established as *lex generalis* Framework Decision 2008/977/JHA. The inertia probably arose previously, as the First AML/CFT Directive formed a part of the former First Pillar, and did not even mention FIUs. But the actual scope of regulation is different, and includes issues of the former First and Third Pillars.

Article 13 of Directive 95/46/EC allows exceptions from data subject right to be informed, to access and to publicise processing operations in cases where its processing could prevent, investigate or prosecute a crime. Thus in the case of information exchange between FIUs, these exceptions could be applied.

As noticed by the Commission, the application of such data subject's rights "would be particularly contradictory with pursued objectives as it would oblige the FIU to inform the person concerned that a suspicious transaction report concerning them has been integrated in a data processing exercise whose objective is to combat money laundering and terrorism financing."[625]

In the case of AROs, Article 5 of the Decision 2007/845/JHA also makes reference to the principles of the European Convention on Data Protection, its Protocol, Recommendation R(87) 15, as well as to national data protection rules of the Member States and received data has to be protected in the same way as national data related to the same topic.

But as information exchange between AROs takes place under the Swedish Initiative, data protection provisions of the latter shall be applied as *lex specialis*. As already mentioned, information received under Framework Decision 2006/960/JHA can be processed only for the purpose for which it was transmitted and its use for other purposes has to be authorised by the requested Member State and envisaged by the national law of the receiving one.

Additionally to *lex specialis,* the Swedish Initiative also has *lex generalis* that is Framework Decision 2008/977/JHA (analysed in subsection 4.3.3 of the Chapter II). Thus it shall also be applied to information exchange between AROs.

4. Brief summary and evaluation

Although functioning under different legal bases and using different information exchange tools, networks of FIUs and AROs aims to combat illicit proceeds by their elimination from legal financial markets.

[625] EU FINANCIAL INTELLIGENCE UNITS' PLATFORM, "Report on Confidentiality and Data Protection in the Activity of FIUs", April 2008, p. 4, accessed August 1, 2015, http://ec.europa.eu/internal_market/company/docs/financial-crime/fiu-report-confidentiality_en.pdf.

The European legislator leaves it up to Member States to decide whether national FIUs and AROs are administrative, police or judicial entities. The only requirement is to ensure that the nature of the unit will not prejudice effective co-operation.

In different ways, both networks contribute to the implementation of the principle of availability: in the case of FIUs, they are directly established in the Fourth AML/CFT Directive and in the case of AROs – indirectly, through the Swedish Initiative. Nevertheless, the difference lies in time limits for response. In cases of information exchange through AROs, in urgent cases related to serious crime mentioned in Article 2.2 of Framework Decision 2002/584/JHA, the response shall be given within eight hours. In cases of co-operation through FIUs, no deadlines are given. From one angle, this can give an impression of less importance being given by the European legislator to intelligence related to money laundering and the financing of terrorism, but looking at the scope of requests in both cases, it is obvious that requests to FIUs can be much broader than asking for any available information and not for precise criminal proceeds.

CHAPTER 7:
INFORMATION EXCHANGE UNDER PRÜM DECISIONS

On the initiative of the German Presidency of the Council of the European Union in 2007, in a surprisingly short time, 27 EU Member States unanimously adopted the previously mentioned Decision 2008/615/JHA and Council Decision of 23rd June 2008, on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime[626] (hereinafter –Decision 2008/616/JHA) also called Prüm Decisions.

As stated by Bellanova, Prüm Decisions "suppose to offer legal and technological instruments for fight terrorism and international crime more efficiently, compensating potential negative spill-overs of the Schengen area."[627]

Besides updated regulation of "traditional" methods of police co-operation and information exchange (such as the spontaneous provision of information, joint operations), they have also given a legal basis for one of the newest information exchange mechanism, i.e. Direct access to national DNA, dactyloscopic and vehicle registration data bases among EU Member States.[628]

---

[626] OJ L 210, 6.8.2008, p. 12-72.

[627] BELLANOVA, Rocco, "The "Prüm Process": The Way Forward for EU Police Cooperation and Data Exchange?" in GUILD, Elspeth and GEYER, Florian (eds.), *Security versus Justice?...,* op. cit., p. 204.

[628] European criminal record exchange system (ECRIS) based on the Council Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from the criminal record between Member States and Council Decision 2009/316/JHA of 6th April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93, 7.4.2009 ,p. 23-348); it is also a system of direct access and was launched in April 2012. It is a decentralised system based on the criminal records databases in each Member State, linked with the common software and communication infrastructure and accessible by judges and prosecutors of all EU Member States. In addition to data about criminal records, transmission of other personal data such as

This chapter reveals the origins of the Prüm Decisions and analyses its content as far as it is related to the object of this investigation – information exchange, focusing on automated exchange, as they are crime investigation tools and non-automated information exchange will be overviewed more briefly, as it stands only for crime prevention but not investigation.

1. From multilateral convention to European instrument

Prüm Decisions take their origin in the multilateral Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration signed on 27th May 2005 in the German town of Prüm (and therefore called the Prüm Treaty) and considered as, "the maximum possible level of police cooperation."[629]

The initiative came from the German Ministry of the Interior, Otto Schily, who in spring 2003 proposed to his counterparts from France, Belgium, Luxembourg and the Netherlands (lately joined by Austria and Spain).

Factual similarities between the development of the Schengen Agreement and the Prüm Treaty can be noticed as both of them were led by Germany and all the primary parties of the Schengen Agreement (Belgium, France, Germany, Luxembourg and the Netherlands) later made up five of the seven signatures of the Prüm Treaty. Therefore, it is sometimes called "Schengen III".

1.1. Between Multilateral and Enhanced Co-operation

But unlike the Schengen Agreement, adoption of the Prüm Treaty has raised grand discussion about the disobedience of the enhanced co-operation procedure.[630]

As the Prüm Treaty was signed by seven Member States and almost immediately joined by seven more (Bulgaria, Estonia, Finland, Hungary, Romania, Slovenia, Slovakia), it has raised a lot of doubts about "sincerity" in the use of the intergovernmental agreement of the seven Member States, instead of more

fingerprints, amongst others, is allowed which makes it possible to identify the subject, and so this is a possibility with regard to DNA profiles. This system was launched in April 2012.

629 CALESINI, Giovanni, *European Police Law…*, op. cit., p. 193.

630 See section 3 of the Chapter I.

complicated enhanced co-operation procedure that should be used with the implications of eight Member States.[631]

It could be justified if the content and the purpose of the agreement would be outside EU policy, but the content of the Prüm Treaty was in line with EU policies in the security area, as it:

a) Corresponded to the general objective to strengthen internal security;

b) Foresaw measures in line with the objective of the Hague Programme, to intensify co-operation in combatting terrorism, cross-border crime and illegal migration; [632]

c) Made an allusion to the general principle of the Hague Programme on information availability by establishing the goal of "better information exchange" [633] (although availability was limited only to the signatory states instead of all EU Member States).

Mr Peter Hustinx, the European Data Protection Supervisor, directly described this situation as evasion of the substantive and procedural requirements of enhanced cooperation.[634]

Other scholars called it a contribution to the "patchwork" legal system and strengthening of a two speed Europe, for example:

– Guild defended the position that "setting up exclusive and competitive measures that seek to address threats that affect the EU as a whole, [...]

[631] See ZILLER, Jaques, "Le traité de Prüm. Une vraie-fausse cooperation renforcée dans l'Espace de sécurité de liberté et de justice" (Working Paper, LAW No. 2006/32, European University Institute, 2006), p. 3, accessed October 2, 2013, http://cadmus.eui.eu/handle/1814/6401; DE HOYOS SANCHO, Montserrat, "Obtención, registro e intercambio de perfiles de ADN de sospechosos en el espacio de libertad, seguridad y justicia" in CABEZUDO BAJO, María José, *Las bases de datos ..., o*p. *cit.*, p. 67-68. CÁMARA VILLAR, Gregorio, "La garantía de los derechos fundamentales afectados por la Convención de Prüm" in *Revista de Derecho Constitucional Europeo,* Enero-Junio 2007, no 7, p. 98-100; FREIXES SANJUÁN, Teresa, "Protección de datos y globalización. La Convención de Prüm" in *Revista de Derecho Constitucional Europeo,* Enero-Junio de 2007, no 7. P. 11.

[632] See OJ C 53/1, 3.3.2005, p. 7-11.

[633] See MARTÍNEZ PÉREZ, Fernando and POZA CISNEROS, María, "El principio de disponibilidad: Antecedentes…", loc. cit., p. 425; BURGESS, Mark, "The Prüm Process: playing or abusing the system?" in *European Security Review*, 2007, no. 34, accessed April 13, 2014, p. 3, http://esdpmap.org/pdf/2007_artrel_17_esr34prum-process.pdf; KIETZ, Daniela and MAURER, Andreas. "From Schengen to Prüm", loc. cit., p. 2.

[634] HOUSE OF LORDS. "Prüm: an effective weapon against terrorism and crime?" (Report with Evidence, May 2007), p. 31, accessed July 13, 2014, http://www.statewatch.org/news/2007/may/eu-hol-prum-report.pdf.

blurs the coherence of EU action in these fields."[635] And excludes parliamentary scrutiny.

- Balzacq, Bigo, Carrera as well as Guild considered it as a significant countervailing political force against the European Union's area of Freedom, Security and Justice as "signatories do not value the EU as the primary unit for the production of security."[636]
- Even more hard and direct criticism came from Guild and Geyer, as they pondered that "Seven Member States free to turn their backs on eighteen others, to decide among them-selves on a model of police cooperation and data exchange only to return to the originally excluded rest to sell their product as the latest innovation in managing threats, a product that no responsible European government could nowadays afford to miss."[637]
- Ziller drew attention to the fact that the Prüm Treaty was signed two days before the French referendum and four days before the Dutch referendum on the Treaty that established the Constitution for Europe[638], and from this perspective, it can be treated as an additional outrage to the EU and its policies.

All these concerns and criticisms are acceptable and have their grounds, because the Prüm Treaty was not created only as a set of mechanisms of intergovernmental co-operation that were not possible to establish within the EU framework, but as an instrument that in the future, was intended to be compelled on all EU Member States, as its Article 1(4) foresees that "within three years at most following entry into force of this Convention, on the basis of an assessment of experience of its implementation, an initiative shall be submitted, in consultation with or on a proposal from the European Commission, in compliance with the provisions of the Treaty on European Union and the Treaty establishing the European Community, with the aim of incorporating the provisions of this Convention into the legal framework of the European Union."

---

635 GUILD, Elspeth, "Merging Security from Two-Level Game: Inserting the Treaty of Prüm into EU law?", (CEPS Policy Brief, March 2007, no. 124), p. 1, accessed April 16, 2014, http://ceps.be/book/merging-security-two-level-game-inserting-treaty-prüm-eu-law.

636 BALZACQ, Thierry; BIGO, Didier; CARRERA, Sergio et al., "Security and the Two-Level Game: the Treaty of Prüm, the EU and the Management of Threats" (Working Document no. 234, Centre for European Policy Studies, January 2006), p. 3, accessed April 16, 2014, http://www.ceps.be/book/security-and-two-level-game-treaty-prüm-eu-and-management-threats.

637 GUILD, Elspeth and GEYER, Florian, "Getting local: Schengen, Prüm and the dancing procession of Echternach. Three paces forward and two back for UE police and judicial cooperation in criminal matters" (Commentaries, Centre for European Policy Studies, 2006), p. 2, accessed April 16, 2014, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591 =0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=122940.

638 See ZILLER, Jaques, "Le traité de Prüm. Une vraie-fausse… ", loc. cit., p.1.

This indicates deliberate following of the scheme of adoption of the Schengen Agreement and its further incorporation into European *acquis*. However, the institutional and political preconditions of 1985 and 2005 were totally different. The Schengen Agreement and Schengen Convention were adopted out of the framework of the European Communities due to significant delays in the creation of the free movement area by all EC, and they had never included any allusion about its imposition on the EU. It was created as a consequence of an institutional vacuum[639] and when, "the European Communities were still far from being able to agree upon the concept of an area of Freedom, Security and Justice."[640] Nevertheless, the Prüm Treaty was adopted after the tabling by the Commission comprehensive of a proposal on automated information exchange, that also included DNA profiles, dactyloscopic and vehicle registration data.

But to be objective, it should be mentioned that there were also some defenders of conventional regulation instead of European. For example:

- Franklin and Sifflet pointed out that the adoption of the Treaty was a signal of ill-working EU decision making in the Third Pillar.[641]
- Kietz and Maurer argued that "despite some important exceptions, the progress in the sub-area of police and judicial co-operation in criminal matters, however, remains limited due to the unanimity rule in Council decision making ... Therefore, cooperation below the EU-25 threshold continues to play an important role in combatting cross-border crime and terrorism."[642]
- Bulmer stated that the number of signatories together with the provision of the afore-mentioned Article 1(4) had indicated explicitly the intention to circumvent the slow EU procedures.[643]

1.2. Transformation into EU instrument

Special attention deserves the rapidness of the Prüm Treaty's transposition into the EU framework deserves special attention. Although it came into force on 23rd

[639] See BALZACQ, Thierry, "From a Prüm of 7 to a Prüm of 8+: What Are the Implications?", (Briefing Paper, DG Internal Policies, Citizens Rights and Constitutional Affairs, 2006), p. 4, accessed April 14, 2014, http://www.libertysecurity.org/article1189.html.

[640] GUILD, Elspeth and GEYER, Florian, "Getting local: Schengen…", loc. cit., p. 4.

[641] DEHOUSSE, Franklin and SIFFLET, Diane, "Les nouvelles perspectives de la coopération de Schengen: le Traité de Prüm", Egmont European Affairs Publication, 2006, p. 13, accessed April 17, 2014, http://aei.pitt.edu/9091/1/Prum.pdf.

[642] KIETZ, Daniela and MAURER, Andreas, "From Schengen to Prüm", loc. cit., p. 1.

[643] BULMER. Simon, "Shop till you drop? The German executive as venue-shopper in Justice and Home Affairs" in ENDEL. Petra; ETTE, Andreas and PARKES, Roderick, *The Europeanization of Control. Venues and Outcomes of EU Justice and Home Affairs Cooperation* (Berlin: LIT Verlag, 2011), p. 63-65.

November 2006[644] and only between Austria, Germany and Spain, it was already presented at EU level at the beginning of 2007. On 1st January 2007, Germany had taken over the Presidency of the Council of the European Union, and within one month, in February 2007, its Minister of Interior Dr Wolfgang Schäuble presented the Prüm Treaty at an informal meeting of Justice and Home Affairs Ministers, as an instrument that was ready to be transplanted into EU law. He also confirmed deliberate avoidance of the enhanced co-operation procedure by saying that it was an example of avoidance of the bottlenecks of usual EU procedures. Four days later, the Council Secretariat officially published "European-wide Prüm Treaty" as the initiative of fourteen Member States: Austria, Belgium, Bulgaria, Finland, France, Germany, Luxembourg, the Netherlands, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.[645]

The political agreement of the ministers on the proposal was reached in less than half a year - on 12th June 2007 and the Council of the European Union adopted its final version on 23rd June 2008.

From another perspective, as many EU Member States had expressed the wish to join the Convention, it was better to move it to the EU framework and to ensure that EU warranties would be applied to information exchange.[646]

In these circumstances, in May 2007, the European Parliament expressed its regrets that it had not had time for an appropriate review of the proposal, and drew the attention to the absence of an explanatory memorandum, the evaluation of future costs, comprehensive impact assessment and an evaluation of the multilateral agreement, as well as lack of an adequate data protection framework.[647]

By Decision 2008/615/JHA and Decision 2008/616/JHA the Prüm Treaty was not literally integrated into the framework of the EU. Both experts and politicians had expressed concerns about some of its aspects and finally, a compromised text that differs from the original was adopted.

---

644 The same year, parties signed an Administrative and technical implementing Agreement to the Prüm Convention. See Council document 5473/07.

645 BURGESS, Mark, "The Prüm Process: playing…", loc. cit., p. 2.

646 See DE HOYOS SANCHO, Montserrat, "Obtención, registro e intercambio…", loc. cit., p. 67.

647 See EUROPEAN PARLIAMENT, "Report on the initiative by the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (6566/2007 – C6-0079/2007 – 2007/0804(CNS))", p. 6, accessed June 20, 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2007-0207+0+DOC+XML+V0//EN&language=hr>; O'NEILL, Maria. "The Issue of Data Protection…", loc. cit., p. 227.

Both the Treaty and the Decisions seek the same general aim: to step up cross-border cooperation, in particular law enforcement information exchange.[648] Comparing the areas of co-operation covered by the two instruments, the Prüm Treaty foresees more co-operation instruments than Prüm Decisions; this is presented in the table below.

Areas covered by Prüm Treaty	**Areas covered by Prüm Decisions**
Creation of national DNA, dactyloscopic data bases[649]	
Automated searching in national DNA, dactyloscopic and vehicles' registration databases and further information exchange	
Supply of personal and non-personal data for crime prevention, maintenance of public order and security for major events with a cross-border dimension	
Assistance in connection with major events, disasters and serious accidents	
- Combatting terrorism by information supply and exchange, giving the possibility to deploy "air marshals" on the aircraft registered in the deploying country - Cross-border police co-operation through provisional measures necessary to preclude imminent danger to the physical integrity of individuals; common patrols and other joint operations when officers from one Contracting Party should perform their duties within the territory of another - Combatting illegal migration by secondment of document advisers, assistance in repatriation measures - Other co-operation upon request	- Prevention of terrorist offences by information supply - Common patrols and other joint operations when officers of one Contracting Party should perform their duties within the territory of another

Table 20: Co-operation areas covered by Prüm Treaty and Prüm Decisions.

Both the multilateral convention and the EU legal instrument include provisions on their interrelationship.

- Article 47 of the Prüm Treaty foresaw that its provisions shall apply only in so far as they are compatible with the EU law.
- Article 35 of the Council Decision 2008/615/JHA established that for contracting parties of the Prüm Treaty, the relevant provisions of the Decision shall be applied instead of the corresponding provisions

[648] Although the purposes of different categories of information exchange vary and are not equal. See following sections.

[649] At the beginning, there was an idea to create centralised DNA, dactyloscopic and vehicle's registration databases, but it was declined at the ministerial meeting on 26th November 2004 opting for decentralised data bases. See LUIF, Paul, "The Treaty of Prüm: A Reply of Schengen?" (deliverable of the Project within the framework EU-CONSENT "*Wider Europe, Deeper Integration? Constructing Europe Network*", May, 2007), p. 8-9, accessed, June 25, 2014, http://www.eu-consent.net/library/deliverables/D38c.pdf.

contained in the Prüm Treaty. But any other provisions of the latter shall remain applicable between the contracting parties.

2. Prüm Decisions: possibilities given and benefit made

Decision 2008/615/JHA justifies its development and necessity by referring to different strategic and political statements. Its recitals point out a need to improve information exchange, declared by the Tampere conclusions, as well as the principle of availability, innovative approach to the cross-border exchange of law enforcement information, use of new technologies and reciprocal access to national databases established in the Hague Programme.[650]

As has already been presented in Table 20, the Prüm Decisions foresee the exchange of different categories of data:

a) Data related to personal characteristics such as DNA and dactyloscopics;

b) Vehicles' registration data;

c) All data important in prevention of terrorism;

d) All data important in prevention of offences and threats to the security in major events with a cross-border dimension.

With regard to the first two categories, a State has DNA samples, a profile, fingerprints, palm prints, a vehicle registration number or chassis, and is looking for its "owner", or wants to find out more information. Regulation on this kind of data (Articles 3, 9 and 12 of the Council Decision 2008/615/JHA) allows Member States to perform an automated search in the relevant national databases of other Member States.

In the following two categories, the State faces a potential threat and is looking for any information that can prevent it. In this case, a non-automated information exchange takes place and the State under threat, sends a request for any information or to see if another State is aware of the existing threat and can therefore supply information without a previous request.

It should be noted that Prüm Decisions, as well as the Framework Decision 2066/960/JHA, do not oblige States to collect any information, but solely make

[650] As Council Decision 2008/616/JHA deals with technical implementation of the Council Decision 2006/615/JHA, it refers only to the latter.

available already existing information.[651] The only exception is Article 7 of the Council Decision 2008/615/JHA that foresees the possibility of requesting assistance on collection of cellular material and supplying DNA profiles when they are needed for on-going investigations or criminal proceedings.

For the time being, in addition to the 28 EU Member States, Iceland and Norway signed the agreement on the application of certain provisions of Prüm Decisions in November 2009.[652]

2.1. Automated data search

For automated data exchange, Decision 2008/615/JHA obliges the States to establish national databases and provide the search rules in national DNA, dactyloscopic (fingerprints, palm prints or soleprints) and vehicle registration databases by competent authorities of other States, and further information exchange.

Two categories of data are personal characteristics that could lead to the identification of persons involved, and the third can serve as a facilitator or a direct tool in crime commissioning (robberies, assassinations, traffic crimes, trafficking, terrorist attacks, etc.).

Justification for strengthened measures to exchange dactyloscopic data and DNA can be found in forensic science, as both of them are reliable person identification tools:[653]

- Dactyloscopic data is used traditionally as the method to individualise a print as having been made by one and only source,[654] and nowadays it is a leader in persons identification markers;[655]
- DNA, due to its "slight characteristic variances"[656] can conclusively establish the identity of biological fluids and trace substances that are almost inevitably found at crime scenes.[657]

[651] See AGUILERA RUIZ, Luis, "La protección de datos de ADN en la Unión Europea y en España" in CABEZUDO BAJO, María José, *Las bases de datos policiales…*, op. cit., p. 34.
[652] COM(2012) 732 final, p. 2.
[653] See SOLETO MUÑOZ, Helena, *La identificación del imputado: Rueda, fotos, ADN…De los métodos basados en la percepción a la prueba científica* (Valencia: Tirant lo blanch, 2009), p. 89; ASHWORTH, Mike and REDMAYNE, Mike, *The criminal Process* (Oxford: Oxford University Press, 2005, 3rd ed.), p. 124; FRÍAS MARTÍNEZ, Emilio, "AND y privacidad en el proceso penal" in *Diario La Ley*, September 30, 2013, no 8159, p. 17.
[654] See MOENSSENS, Andre A.; HENDERSON, Carol E. and PORTWOOD, Sharon G., *Scientific Evidence in Civil and Criminal Cases* (New York: Foundation Press, 2007, 5th ed.), p. 620.
[655] See HOUCK, Max M. and SIEGEL, Jeffrey A., *Fundamentals of Forensic Science* (Oxford: Elsevier, 2010, 2nd ed.), p. 474.

Although the general aim of the Prüm Decisions is to step up cross-border cooperation, in particularly law enforcement, information exchange and its provisions foresee different information access purposes, depending on the category of data subject to automatic search. Thus according to Article 3, national DNA databases can be accessed and reference data can be obtained only for the investigation of a criminal offence. Article 9 allows automated search and access to the reference data in fingerprint identification systems for the prevention and investigation of criminal offences. Vehicle registration data can be searched and accessed for the prevention and investigation of criminal offences, other offences under the jurisdiction of the courts, or the public prosecution service of the searching Member State and for the maintenance of public security.

The deadline to implement these measures expired on 26th August 2011.

2.1.1. Data search and access

Three categories of automatically searched data are regulated in the same Chapter 2 of the Council Decision 2008/615/JHA. Regulation of DNA profiles and dactyloscopic data is almost the same, but access to vehicle registration data is handled in a different way.

Thus in cases of DNA profiles and dactyloscopic data, the search is directly performed in the national database of the other country and in cases of vehicle registration – access is through centralized European Vehicle[658] and Driving Licence Information System (Eucaris)[659] which offers a multilingual web client, enabling enquiries to other countries to be sent via national web browser.[660]

---

[656] MOENSSENS, Andre A.; HENDERSON, Carol E. and PORTWOOD, Sharon G., *Scientific Evidence in Civil..*., op. cit., p. 1020.

[657] It is not only a feature of violent crimes such as rapes, murders, etc., but also while committing property crimes, offenders usually leave their biological evidence: sweat, hair, etc. and despite being careful and not leaving dactyloscopic prints, reveal their identity. Thus DNA samples recovered from crime scenes in France, Liechtenstein, Switzerland and the United Arab Emirates revealed links between three different types of crime (armed robbery, prison escape and the use of forged travel documents) and between a group of individuals known as the 'Pink Panthers', an organised gang. See more "Forensic", Interpol, accessed July 1, 2015, http://www.interpol.int/INTERPOL-expertise/Forensics/DNA.

[658] It should be noted that Prüm Decisions use a term "vehicle" although officially Eucaris stands for "European *Car* and Driving Licence Information System". See European Car and Driving Licence Information System, https://www.eucaris.net.

[659] Eucaris was established in 1994 by the initiative of 5 European countries (Belgium, the Netherlands, Germany, Luxembourg and the United Kingdom) in order to support data communication between vehicles' registration authorities and to combat exportation of stolen cars as well as driving licence "tourism". Currently Eucaris is expanded with other forms of information exchange between countries, e.g. Prüm Treaty and Prüm Decisions and in 2012, it was appointed as the technical platform for the cross-border exchange of information under Directive 2011/82/EU of the European Parliament and of the Council of 25 October 2011

To carry out queries in relation to DNA profiles and dactyloscopics, reference data is entered. For DNA profiles it means non-coding part of the DNA and reference number, and for dactyloscopics – the dactyloscopic data and reference number. It is disassociated from any data that can lead to direct identification of a person in a search. Both the non-coding part of DNA and fingerprints, palm prints and soleprints help to identify a person and to distinguish them from another. The non-coding DNA part also indicates the gender, but does not provide any other type of genetic information, such as race, ethnic group, diseases, and so on. [661]

While performing an automated search of DNA profile or dactyloscopic data, data stored in databases is not accessed directly. State A can only find out whether there is DNA profile or dactyloscopic data in the relevant database of State B, corresponding to the searched data, and will only receive an automated answer on positive or negative search result. In the case of a positive result together with an automated reply the reference data of the stored DNA profile or dactyloscopics that resulted in match will be sent. Providing personal data and other information will be performed on the basis of the further request of the searching State (Articles 5 and 10 of the Decision 2008/615/JHA), i.e. State A will send a request to state B, indicating reference data of the stored DNA profile or dactyloscopics received with answer on coincidence and explaining the purpose for which the data is requested.

That means that:

- The DNA or dactyloscopic database searching State will never obtain data that does not match that submitted for the search;
- The establishment of separate 'hit' and 'post hit' (data exchange) stages allows absolute control of the possessed data to be maintained and evaluated, whether the reason for the search and other conditions meet the requirements to give the data.[662]

It should be mentioned that in this process, different legislation is used: a search is performed in compliance with the national law of the searching party, an

facilitating cross-border exchange of information on road safety and related traffic offences (OJ L 288, 5.11.2011, p. 1-15). See Council document 13127/13, p. 12.

[660] All connected Member States communicate directly with each other, without any central application or central hub. See Council document 13127/13, p. 12.

[661] See DE HOYOS SANCHO, Montserrat, "Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos." In ARANGÜENA FANEGO, Coral (dir.), *Espacio Europeo de Libertad, Seguridad y Justicia: Últimos avances en cooperación judicial penal* (Valladolid: Lex Nova, 2010), p. 161-162; DE HOYOS SANCHO, Montserrat, "Obtención, registro e intercambio…", loc. cit., p. 74.

[662] See AGUILERA RUIZ, Luis, "La protección de datos ADN…", loc. cit., p. 35.

automated answer on match is regulated by EU law, and the request for further data shall be in accordance with the requested State's national law.

Moreover, it should be taken into account that national rules of DNA and dactyloscopic collection, use and processing can differ among States and affect data exchange and its further use in the process. In many European countries dactyloscopic data is concerned as police data[663] and its collection is treated as not affecting either the fundamental right of physical and moral integrity, or the right of privacy.[664] But talking about DNA profiles and related data, the situation is more complicated as its collection has different restrictions, due to the possible affects of fundamental rights:

- In some States, a judicial authorisation to collect DNA samples is needed (e.g. Spain) and in others, the police can do it without judicial authorization (e. G. The United Kingdom).[665]
- National law differs in relation to categories of crimes in which collection is permitted. For example; in Finland collection is permitted only for crimes with a punishment of imprisonment higher than 6 months. In Netherlands – 4 years.[666]
- Storage and further use of data. It is forbidden to store and use data without conviction in Austria, Belgium, the Czech Republic, Hungary, Slovakia, Slovenia, Sweden and the Netherlands. [667] Other States make some exception from this general rule, for example "Finland [...] which requires the destruction of suspect profiles within one year of criminal acquittal, permits the retention of suspect profiles for ten years if the suspect is deceased. Germany allows the retention of some suspect profiles by the police in cases where an individual is suspected of a serious crime (particularly sexual or homicide) or where they have a previous criminal records for serious crime."[668]

Due to the different rules of legitimacy, DNA collected in the United Kingdom will not always serve as evidence in the Netherlands, or DNA stored in Finland as evidence in Sweden.

---

[663] See MCCARTHNEY, Carole I.; WILSON, Tim J. and WILLIAMS, Robin, "Transnational Exchange of Forensic DNA: Viability, Legitimacy, and Acceptability" in *European Journal on Criminal and Research*, 2011, vol.17, no. 4, p. 310.

[664] See SOLETO MUÑOZ, Helena. *La identificación del imputado…,* op. cit., p. 83.

[665] See more ALCOCEBA GIL, Juan Manuel, "Tratamiento y transmisión de datos genéticos con fines de la investigación penal en la UE" in COLOMER HERNÁNDEZ, Ignacio and OUBIÑA BARBOLLA, Sabela. *La transmisión de datos personales…,* op. cit., p. 624-635; SOLETO MUÑOZ, Helena and ALCOCEBA GIL, Juan, "Protección de datos y transferencia…", loc. cit., p. 338-340.

[666] WILLIAMS, Robin, "Making Forensic DNA Databases: Global Themes and Local Variations" in CABEZUDO BAJO, María José, *Las bases de datos policiales*..., op. cit., p. 366.

[667] See WILLIAMS, Robin, "Making Forensic DNA…", loc. cit., p. 367.

[668] Ibid.

In the case of vehicle registration data, full chassis number or full registration number shall be used for automated search and of course, by itself it does not contain any personal data. In this case, there is no two stages procedure, as the answer for the search (vehicle and insurance information together with the respective vehicle owner and/or holder) is returned directly in encrypted form.

This difference in procedure can be defended by the fact that the backgrounds for vehicle registration search are much broader than for "bio information", and the flow of searches is more intensive. From another angle, data on the vehicle's owner or operator is usually basic: name and surname.

2.1.2. Granting access to national databases

An automated search carried out in the data base of another State means that the searching authority has previously been given access to it. It is a sensitive issue as it supposes actions on law enforcement or the judicial "virtual territory" of another State, and demands strong trust in the partner, its legal system and professionals. Doubts can arise at every stage, for instance: how will the searching State ensure that only authorised staff will have access? Whether data protection rules of another country will guarantee the same protection level as national ones? Are information search and use rules strict enough? Without answering these questions and the disappearance of these doubts mutual access to national databases is hardly imagined.

Therefore, Prüm Decisions establish mechanisms that allow strengthening mutual trust and making information exchange effective and free of mutual suspicions. Article 25(2) of Decision 2008/615/JHA establishes that access to another State's databases is granted when the Council decides that the country has met all the technical, legal, data protection requirements applied to every category of data exchanged (DNA, dactyloscopic and vehicles' registration data).[669] The evaluation mechanism is not applied for Member States where the supply of personal data has already started, pursuant to the Prüm Treaty. According to Article 20 of the Council Decision 2008/616/JHA, the Council's decision is taken on the basis of an evaluation report, developed by the experts of already operational Member States, and based on information from the questionnaire answered by the evaluated State, its evaluation visit and pilot run of the relevant database.

Thus before granting access to the national database, all Member States have the opportunity to assess the State's readiness in this regard. Although evaluation is

[669] It should be noted that this requirement is not applied to Member States that started to exchange data under the Prüm Treaty.

performed and a report is drafted by a limited number of persons representing already operational countries (3-4 persons), other countries can acquaint themselves with the whole evaluation process and documentation through the different bodies of the Council of the European Union, i.e. Through the Working Party on Data Protection and Information Exchange, the Committee of Permanent Representatives (COREPER 2) and Justice and Home Affairs Council.

Unlike Schengen evaluation mechanism, Prüm evaluations are performed only with regard to automated data exchange and only once, i.e. In order to grant access. It does not have any follow-up as in the case of periodical Schengen evaluations.

2.1.3. Implementation measures

As already mentioned, Prüm Decisions' implementation deadline for automated data search expired on 26th August 2011. The earliest available statistics on this issue present the figures of the state of play on 31st December 2011[670], when:

- 14 Member States (Austria, Bulgaria, Finland, France, Germany, Latvia, Lithuania, Luxembourg, the Netherlands, Portugal, Romania, Slovakia, Slovenia, Spain) were entitled to exchange DNA related data and twelve of them were already operational;
- 10 Member States (Austria, Bulgaria, Czech Republic, France, Germany, Lithuania, Luxembourg, Slovakia, Slovenia, Spain) were operational for fingerprint related data exchange;
- 10 Member States (Austria, Belgium, Finland, France, Germany, Luxembourg, the Netherlands, Romania, Slovenia, Spain) were operational for vehicles registration data exchange.

Although at the beginning, the United Kingdom expressed her wish to participate in the implementation of Prüm Decisions, in 2014 she was not included in the list of acts in which the United Kingdom continues to participate.[671]

Even now, some Member States are still not operational. According to the data from July 2015:

- 22 of 27 Member States (not including the United Kingdom) were operational for DNA related data exchange. Denmark, Greece, Croatia, Ireland and Italy were still in the process of preparations.

[670] See Council document 11367/12, p. 2.
[671] OJ L 345, 1.12.2014, p. 6-9.

- 18 of 27 Member States were operational for exchange of dactyloscopic data. Belgium, Denmark, Greece, Croatia, Ireland, Italy, Poland, Portugal and Sweden remain non-operational.
- 20 of 27 Member States exchange data on vehicle registration and Czech Republic, Denmark, Greece, Croatia, Ireland, Italy and Portugal are still at the preparatory stage.[672]

From all non-operational Member States, justification is possible for Croatia who only joined the EU on 1st July 2013.

Nevertheless, there is no information about Island and Norway, as the agreement has been signed, but not entered into force.

As Home Affairs Ministers gather for the Council at least every 2-3 months, and the Council's preparatory bodies meet almost every month, decision-making processes (i.e. Council Decision on granting of access) are not the reason for delays. Problems lie in Member States who face different obstacles to establish or modify databases and to create appropriate legal and data protection regimes. As stated in the Report from the Commission to the European Parliament, and the Council on the implementation of Council Decision 2008/615/JHA of 23rd June 2008, on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (hereinafter – Implementation Report 2012), the main reasons for the delay are technical in nature and caused by a lack of human and financial resources in the Member States.[673]

In 2010, observing Member State's preparations for the implementation, the Belgian Presidency of the European Union made a short study on the state of the implementation of Prüm Decisions and identified the main problems which are presented in the chart below:

[672] See Council document 5010/5/15, p. 11-14, 17-21, 23-25.
[673] COM(2012) 732 final, p. 5.

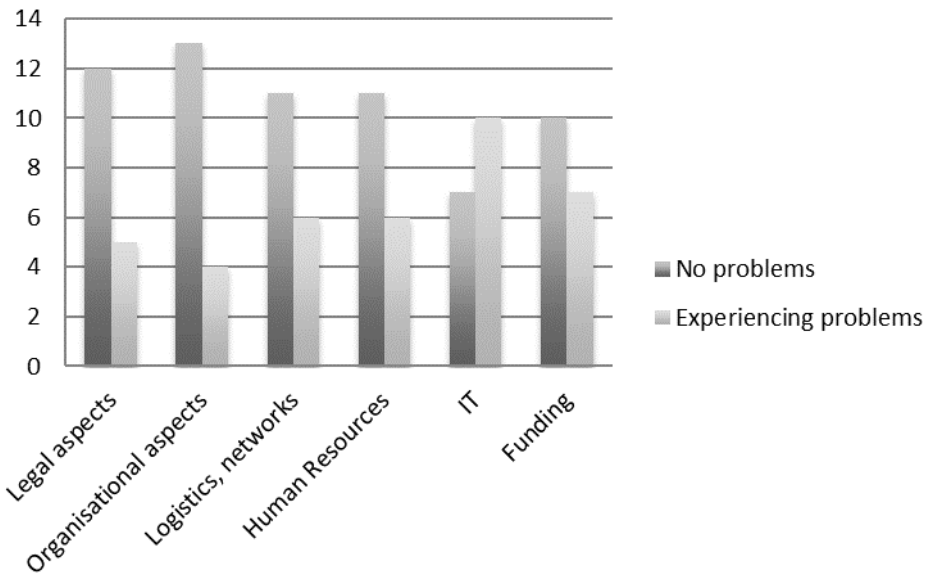

Chart 1: Aspects affecting the implementation of Prüm Decisions.

The above-mentioned Belgian Study also revealed that the average "rough estimation" for a country to access the Prüm network approximates 2 million euros.[674] For countries that had no national DNA database in operation before 2008 – such as Italy, Greece, Malta, or Ireland – the costs are likely to be much higher.[675]

The British Government (which was still considering participation) has estimated that "the total start-up cost for the United Kingdom will be in the region of 31 million pounds for the exchange of fingerprints, DNA and vehicle registration data."[676]

Thus the automated data exchange mechanism is quite expensive and the question stands, whether its use and effectiveness for crime investigation compensates such expenditures. For the time being there are two sources that can reveal, at least partly, the effectiveness and use of the instrument:

- The Implementation Report 2012;
- Annual statistics that must be submitted under Article 21 of Decision 2008/616/JHA and relevant provisions of its Annex (paragraph 2.1 of the Chapter VI).

[674] Council document 14918/10, p. 6.
[675] See PRAINSACK, Barbara and TOOM, Victor. "Performing the Union: The Prüm Decision and the European dream" in *Studies in History and Philosophy of Biological and Biomedical Sciences,* 2013, 44(1), p. 76, accessed April 7 2014, http://www.sciencedirect.com/science/article/pii/S1369848612001033.
[676] HOUSE OF LORDS, "Prüm: an effective weapon…", loc. cit., p. 24.

The Implementation Report 2012 is based on the States' answers to the questionnaire disseminated by the Commission, and reveals that States have "quite positive attitude" towards the Prüm Decisions, with satisfaction of exchange of VRD related data, but in the case of DNA and dactyloscopics "efficiency is considered only acceptable or even inadequate by about 30% [of States]."[677]

States also pointed out the need to improve the follow-up of hits (the stage of personal data exchange) in cases of DNA related data and dactyloscopics without which hits by themselves are useless for the investigation.

Referring to the statistics, it should be pointed out that not all States provide them, or some of them provide incomplete data.

In 2013, operational Member States had made 3,492,601 searches of vehicle registration data that resulted in 1,498,663 hits. Thus more that 42 % of searches were successful. In the case of dactyloscopic data, 128,494 searches gave 4,621 matches, i.e. 3.5 %.

In the case of DNA, statistics providing rules were changed in 2012, requesting Member States to provide an overview of the national situation concerning matches from the owner's point of view. Thus the number of searches is not provided, but only the number of matches. These statistics should coincide in case of cross-checking, i.e. The figures from A and B involved in a match should be equal for stain-stain matches, person-person matches, A stain-person with B person-stain matches and A person-stain with B stain-person matches.[678] Nevertheless, making this analysis in almost all cases, the difference between the data of countries involved is found. Therefore, analysis of these statistics does not contribute too much to this analysis.

In general, the majority of Member States have opted for a statistics model focusing on the number of hits, but not on the data of the influence of this information exchange on the final result of investigation and prosecution. Thus it is not clear what percentage of hits was really significant in finding offenders and bringing them to justice; e. G. Spain's search of DNA profile had resulted in a hit in the German DNA database and was reflected in the statistics, but there is no information on the level of its importance in comparison with other data related to the investigation or on its use as evidence in the trial.[679]

---

[677] COM(2012) 732 final, p. 6.

[678] See Council document 14383/2/12, p. 2.

[679] Such data had been collected, implementing a pilot project in Denver, USA related to DNA evidence use in the investigation of burglaries. From all cases where DNA extraction was possible (about 7% of all burglaries) in 76 %, the crucial element for prosecution was DNA analysis. ASHIKMIN, Simon; BERDINE, Susan G.; MORRISSEY, Mitchel R. et al., "Effectiveness and Cost Efficiency of

The European Commission considers the current situation as an interim solution and encourages Member States to improve statistics and reports including data exchange weight for the final result of investigation and prosecution; [680] but due to different Member States' legal systems and the variety of protagonists involved in investigation and prosecution, it is very difficult to find a common solution suitable for everyone and it demands sometimes unreasonable administrative efforts.

And finally, as noted by Topfer in relation to DNA exchange "Although the establishment of the network was justified by the need to combat serious crime, interim reports reveal another story: most hits on the DNA database relate to property crime and often to anonymous "stains" (DNA from unidentified persons left at a crime scene). [...] Thus, European data exchange has not changed the balance of the national databases: the quantitative criminalistics value lies in the domain of property crime."[681]

2.2. Non-automated data exchange

As mentioned, Decision 2008/615/JHA also establishes some rules on traditional information exchange on request or by own initiative. Its Chapters 3 and 4 regulate such information exchange for:

- Terrorism prevention;
- Prevention of criminal offences and maintaining public order and security in major events with a cross-border dimension.

These provisions are not widely analysed, either by experts or by scholars as all their attention is focused on revolutionary automated data exchange.

Before getting into the analysis of these Chapters of Decision 2008/615/JHA, it is worth trying to find out if there are any other EU legal instruments that regulate exchange of the same categories of data, and to make their comparison.

DNA Evidence in Volume Crime. Denver Colorado Site Summary", p. 2, accessed April 24, 2014, http://www.denverda.org/DNA_Documents/DNABurgrCostEfficiency Reserch1.pdf.

680 See COM(2012) 732 final, p. 6, 11.

681 TOPFER, Eric, "Searching for Needles in an ever expanding haystack: Cross-border DNA data exchange in the wake of the Prüm Treaty" in *Statewatch Journal,* 2008, vol 18, no 3, p. 14-15, accessed may 3, 2014, http://www.statewatch.org/news/2008/dec/eu-dna-statewatch-article.pdf.

2.2.1. Relation with other EU legal instruments

Decision 2008/615/JHA is surely not the first one that regulates information exchange in such important issues as combatting terrorism or events of cross-border dimensions (summits of heads of states, important international sport events, etc.).

Such information can be exchanged on the basis of Framework Decision 2006/960/JHA as general background to any information exchange, as well as on specific bases , such as Council Decision 2005/671/JHA of 20th September 2005 on the exchange of information and cooperation concerning terrorists[682](hereinafter – Decision 2005/671/JHA) or Council Decision 2002/348/JHA of 25th April 2002 concerning security in connection with football matches with an international dimension[683] (hereinafter – Council Decision 2002/348/JHA).

Framework Decision 2006/960/JHA covers information exchange related to any criminal investigation or criminal intelligence operations, including terrorism. From first sight, Council Decision 2008/615/JHA regulates information exchange for terrorism prevention and differs from the Council Framework Decision 2006/960/JHA that covers information exchange on any crime, including terrorism, in the case of criminal investigation or criminal intelligence operations. Nevertheless, as mentioned before, the scope of the Swedish Initiative differs in its articles:

- Article 2(c) defines criminal intelligence as a procedural stage in which information about a crime or criminal activities is gathered in order to establish whether concrete criminal acts have been committed or may be committed in the future. This gives reason to believe that the Swedish Initiative also covers crime prevention matters when it has the form of a criminal intelligence operation;
- Article 5(1) establishes that information and intelligence may be requested for the purpose of detection, prevention or investigation of an offence.

Furthermore, Article 7(1) which has already been mentioned, obliges spontaneous information and intelligence supply to other Member States' law enforcement authorities, where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention or investigation of offences

[682] OJ, L 253, 29.9.2005, p. 22-24.
[683] OJ L 121, 8.5.2002, p. 1-3. Partly amended by the Council Decision 2007/412/JHA (OJ, L 155, 15.6.2007, p. 76-77).

referred to in Article 2(2) of Council Framework Decision 2002/584/JHA on the European arrest warrant, and the surrender procedures between Member States which, among other crimes, also includes terrorism.

Regarding specialised regulation, Article 2(6) of Decision 2005/671/JHA foresees that "each Member State shall take the necessary measures to ensure that any relevant information included in documents, files, items of information, objects or other means of evidence, seized or confiscated in the course of criminal investigations or criminal proceedings in connection with terrorist offences can be made accessible as soon as possible, taking account of the need not to jeopardise current investigations, to the authorities of other interested Member States."

Additionally, as mentioned previously, Europol also carries AWF CT where all relevant information can be submitted, and in cases of urgency, request or provision of the information network of liaison officers can be used.

In case of major events, Article 3 of Decision 2002/348/JHA establishes that "before, during and after a football event with an international dimension, national football information points shall engage, at the request of a national football information point concerned or on its own initiative, in mutual exchange of general information and [...] personal data."

This indicates that Decision 2008/615/JHA is partly overlapping already existing legislation. It would make more sense to expand application of Decision 2002/348/JHA to other sorts of events that establish separate overlapping regulations. In cases of major meetings, such as the European Council, it would be more appropriate to foresee information exchange amending Council Decision 2002/956/JHA of 28th November 2002 setting up a European Network for the Protection of Public Figures[684] as its Article 4 (e) as one of the objective establishes, "Favouring the exchange, in accordance with the national legislation, of operational information, either through the contact points or by means of direct contacts between the responsible services."

This being said, the provisions of Chapters 3 and 4 of Decision 2008/615/JHA seem to be redundant, and do not contribute too much added value in EU regulation regarding information exchange. It is also reflected in the Implementation Report 2012, as Chapter 3 is often used only by eight Member States and Chapter 4 only by five of them.[685]

But given that the regulation is in place, it deserves some analysis.

[684] OJ L 333, 10.12.2002, p. 1–2; OJ L 283, 30.10.2009, p. 62–62.
[685] See COM(2012) 732 final, p. 9-10.

2.2.2. Information supply and exchange

With respect to information exchange and supplying security at major events, Articles 13 and 14 of Decision 2008/615/JHA make a difference between the supply of personal and non-personal data; but in the case of terrorism prevention, Article 16 refers to information as such, without making a previously mentioned division.

Personal data exchange or supply for the security of major events is permitted when there is a reason to believe that, due to conviction or other circumstances, the data subject will commit criminal offences at the events or pose a threat to public order and security.

In the case of terrorism prevention, information (without specifying whether it is personal data or not) exchange and supply is conditioned to the reason to suspect that a person could commit the crime of terrorism.[686]

Article 16(2) foresees that data supplied for terrorism prevention shall comprise surname, first names, date and place of birth and a description of the circumstances giving rise to the belief that a person will commit a crime of terrorism. From the text, it is not clear whether it is minimum or maximum data that is supplied in such circumstances; i.e. Whether supplying a Member State is restricted to providing only the personal data mentioned above, or facilitating other related data as well. Taking into account the information exchange purpose, there should be the possibility to provide any other meaningful data, especially taking into account that surname, name, date and place of birth could be the result of identity fraud. Supplying photos, dactyloscopic and DNA data should be allowed in these cases as well.

[686] For the unified understanding of terrorism, the European legislator makes a reference to the crimes listed in Articles 1-3 of the Council Framework Decision 2002/475/JHA on combating terrorism. (O J L 164, 22.6.2002, p. 3) Those crimes are: attacks upon a person's life which may cause death; attacks upon the physical integrity of a person; kidnapping or hostage taking; causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss; seizure of aircraft, ships or other means of public or goods transport; manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons; release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life; interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life; threatening to commit any of above listed acts. To be recognized as crime of terrorism, the have to be committee with the aim of seriously intimidating a population, or unduly compelling a Government or international organization to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization. As well crime of terrorism is directing or participating in activities of a terrorist group.

When regulating information supply (without a previous request) on terrorism prevention and security at major events, in the first case the legislator uses the term "may" and in the second – "shall". This brings us to the conclusion that in the case of major events, the requested Member State or Member State possessing information is obliged to share it, and in the case of terrorism prevention has the right to do so. Such regulation does not make too much sense taking into consideration the seriousness of both issues.

In summary, the provisions of Chapters 3 and 4 on information exchange and supply are not very comprehensive and leave some question marks on their use and usefulness.

3. Data protection

As in case of Schengen Acquis and Europol's regulation, Prüm Decisions also establish their individual data protection regime instead of applying the *lex generalis* Framework Decision 2008/977/JAI. Unlike the data exchange tools mentioned above, Prüm Decisions' data protection rules do not regulate any central data processing, but establishes minimum standards that have to be applied by Member States that remain data processors and responsible at all stages.[687]

Article 25 of Decision 2008/615/JAI establishes that national rules are applied to the processing of received data and shall ensure at least the data protection level foreseen in the European Convention on Data Protection, its Protocol and Recommendation (87) 15.

As already mentioned in subsection 2.1.2 of this Chapter, before granting access to data bases in other States, and before data processing is started, the application of relevant data protection requirements in each State is evaluated. Thus there is a real control measure to verify the application of relevant data protection principles.

Article 26 of Decision 2008/615/JAI envisages that data processing by the requesting State shall be performed only for the purposes that it was provided. Proceeding for other purposes is subject to the authorisation of the requested Member State and is possible only if its national law permits such use of data.

[687] As mentioned in section 2.1 of this Chapter, the search is performed in compliance with the national law of searching party, an automated answer on match is regulated by EU law and request for further data shall be in accordance with the requested State's national law.

Prüm Decisions also establish that data provided at the first automated information exchange stage (verification of hit / no hit), can be processed by the searching State only for establishing the existence of a match, preparation and the sending of a request for personal data related to the match, and for recording that will be used only for data control. The searched State can process data received as a result of comparison only for this purpose and delete it immediately after comparison has taken place. Exception is made only when it is necessary for the preparation of a request or recording for the control, and the data is deleted after such action.

Such detailed provisions are quite unusual, because in search and automated responses on match, no personal data is involved, but nonetheless , the European legislator has established its special treatment.[688]

Unlike Europol and Schengen Acquis, Prüm Decisions do not establish any precise term for received data deletion, but envisage that it shall be carried out as soon as the data is no longer necessary for the aim that it was submitted, or when the storage term is over, according to the national law of the submitting State. There is also the possibility to block data instead of its deletion if the latter would affect the data subject.

Despite including regulation on information exchange with respect to terrorism, Prüm Decisions do not make any reference to classified information, although theoretically it could also be the object of exchange.

3.1. Persons included

According to Articles 2 and 8 of Decision 2008/615/JAI, a national DNA data base shall be created to investigate criminal offences and a national dactyloscopic data base – to prevent and investigate them.

There is no reference to categories of persons that shall be included or excluded from them, and it is left up to national legislation.

Thus depending on the State, data of convicted persons, suspects, victims and other categories of persons (the examples of such diversity were given in subsection 2.1.1 of this Chapter) can be legally stored and processed. The only supranational criteria in this regard is the case law of the ECtHR, although it does not cover all sensitive aspects.

[688] The same rule was established in the Prüm Treaty. See ACED FÉLEZ, Emilio, "Ejercicio y garantía del derecho…", loc. cit., p. 84, 85.

As a general rule, in the case *Van der Velden v the Netherlands* ECtHR recognised that, "the Court further has no difficulty in accepting that the compilation and retention of a DNA profile served the legitimate aims of the prevention of crime and the protection of the rights and freedoms of others. This is not altered by the fact that DNA played no role in the investigation and trial of the offences committed by the applicant. The Court does not consider it unreasonable for the obligation to undergo DNA testing to be imposed on all persons who have been convicted of offences of a certain severity."[689]

Thus ECtHR does not insist on DNA collection and storing of DNA profiles during the investigation, but it could be done at any time when the convicted person is concerned. Nevertheless, it is not precise when DNA can be collected from other persons, for example suspects. In this respect it has been established on different occasions that there is a risk of stigmatisation[690] and:

- No systematic data retention shall be done.
- Data processing shall maintain proportion between public and private interests.
- Collected and stored data shall match its purpose, i.e. Be relevant and not unreasonably excessive. Distinctions between data storage related to minor and similar offences shall be made.[691]
- Different treatment of data of convicted and non-convicted persons shall be introduced, especially taking into account data of minors.[692]

3.2. Access

As Prüm Decisions envisage rules for automated and non-automated data exchange, as a consequence different rules of access are applied.

In cases of automated data search and its double stage procedure, two types of access have to be taken into account:

- At the stage of automated comparison (direct access to depersonalised data in national data bases of other States), access is granted only to national contact points designated by each State. It means access very limited in terms of numbers of authorities and persons. According to Article 30(2), every State shall have a list of persons authorised to make

[689] ECtHR, *Van der Velden v the Netherlands* [2006].
[690] ECtHR, *M. K. V France* [2013], paragraph 36; *S and Marper v United Kingdom* [2008], para 122.
[691] ECtHR, *S and Marper v United Kingdom* [2008], paragraph 103.
[692] ECtHR, *M. K. V France* [2013], paragraph 36, 42; *S and Marper v United Kingdom* [2008], paragraphs 22, 124.

searches and every search has to be recorded, including an entry giving its reason. National contact points make searches on requests of other national authorities responsible for crime investigation in cases of DNA search, for crime prevention and investigation in case of dactyloscopic data search and crime prevention, its investigation and maintaining public order in cases of vehicle registration data.

- At the stage of receiving data related to an automated match, first of all it is available to a national contact point that lately transmits it to the authority that has requested a comparison.

In case of non-automated data exchange, for each category of data (terrorism, public order and security) a network of contact points is also established and every data exchange shall be recorded according to Article 30(1) of Decision 2008/615/JAI. National contact points make further transmission of data to requesting authorities or in case of spontaneous data supply – to the authority that could be interested. In these circumstances, it is very important to forward information to the right institution and to avoid any unnecessary data (including personal) diffusion. Nonetheless, this aspect is not regulated by the Prüm Decisions.

3.3. Third Parties and onwards transmission

Unlike the Europol Decision, Prüm Decisions do not foresee the possibility of data transmission to third parties or onwards transmission to other than requesting institutions, to other Member States or to third parties.

Such restriction allows the identification at any time of an institution that has misused data, as the circle of subjects that process the data is very limited. It is important with respect to any data and in particular to that related to DNA.

Comparing the "destiny" of data related to terrorism and processed under Prüm Decisions and in AWF, the same data in the first case will never be transmitted onward or to the third party and in the second case – it will be.

This is one of the examples when competent institutions would prefer to use Decision 2008/615/JHA than submit information to Europol and lose control over it.

3.4. Data subject's access right

Article 31 of Decision 2008/615/JAI includes a data subject's access right without unreasonable expenses, within "comprehensible" terms and "without unacceptable delays". The scope of the access right is not precisely defined, but bearing in mind the established right to obtain information about data origin and receiving authorities, it seems to be limited to the data received from other Member States; as a consequence, the data of a search and not access to data on a national data base. In addition, it is not clear whether the data subject can make a general request about all processed data according to Prüm Decisions, or shall specify whether it concerns DNA, dactyloscopic or other data. Article 31 envisages an obligation to ensure effective judicial protection for data subjects whose data protection was violated. Thus in comparison with the right of access regulated by Europol Decision, it is a big step forward.

Establishing these minimum guarantees of access right, the regulation of the whole process is left to the national law of every country, meaning that different procedures, authorities, appeal systems and reasons for denial will be applied.[693] Without any doubt, that would place the data subject in a discriminated position, and condition his or her right to access, depending on the State where the request is be made.

Prüm Decisions do not foresee any rules on consultation with the States from which data was received, although as previously mentioned, the data subject has a right to know about the origin of his or her data. Thus situations where the State of the data's origin has a reason not to reveal information to the data subject (such as an ongoing investigation, public or state security) are not taken into account.

According to Article 28(2), the data subject can ask to flag his or her data when the accuracy or inaccuracy of data cannot be established.

3.5. Supervising authorities

Unlike Europol and Schengen Acquis, Prüm Decisions do not foresee any Joint Supervision Body, leaving control to the independent national data protection of competent judicial authorities. They are authorised to perform checks of legality of data submission to other States on their own initiative, and of the legality of processing on requests of the data subject.

[693] See ACED FÉLEZ, Emilio, "Ejercicio y garantía del derecho…", loc. cit., p. 91.

No existence of a central data supervision body makes sense taking into account the decentralised nature of data exchange under the Prüm Decisions and the States' responsibility for data at every stage of its processing.

4. Brief summary and evaluation

The Prüm Treaty and Prüm Decisions are very controversial instruments of information exchange. On the one hand, they establish direct access to certain national data bases, creating in this way, new information exchange methods and contributing to the principle of availability. On the other hand, they were adopted in such a hurry and in the process, disrespecting the applicable legislative rules of the EU that raise the question of their legality; first of all, with respect to the procedure of enhanced co-operation, deliberately omitted by seven States and then the "pushing of drafts" in record time, and without even giving enough time for the European Parliament to formulate its opinion. Thus such a restriction of fundamental rights is questionable, due to the lack of a fair and transparent legislative process.

New information exchange methods require at least full compatibility of national databases, legislation on minimum standards on data protection and legalization of foreign searches, trust in searching States, authorized and trained human resources responsible for information searches and exchange. These requirements brought together technical, legal, financial and human resources problems, that States are overcoming at different paces and with varying success and until now, not all States have implemented them.

If automated searches for DNA profiles, dactyloscopics or vehicle registration data represent a new tool for competent authorities, non-automated information exchange on terrorism and major events with cross-border dimension is repetitive and brings about confusion among its users.

Despite the declaration of quantities of hits produced in automated data exchange, nobody can estimate its real added value in investigation, as no such statistics exist. In these circumstances, a question of proportionality should be raised.

In respect to proportionality of purpose, its differentiation in each category of data (only crime investigation, crime investigation and prevention, etc.) shows that both in Treaty and Decisions, it was considered carefully enough and took into account the speciality and sensitiveness of each data base.

From a positive angle, strict prohibition of information transmission to other an authority other than requesting one should be appreciated.

PART III:
PROJECTS IN THE PIPELINE: REASONS, CONTENT, PROBLEMS AND STATE OF PLAY

CHAPTER 8:
PROJECTS IN THE PIPELINE

After the first decade of the century, where initiatives on information exchange were springing up like mushrooms, with the Stockholm Programme and the IMS came an attitude to first evaluate already existing co-operation possibilities and only then look for new ones. Thus in Stockholm Programme the Council recognised "the need for coherence and consolidation in developing information management and exchange."[694]

Following this idea, it can be noticed that currently, apart the Draft Directive on Data Protection and Draft Europol Regulation (that are foreseen by the Lisbon Treaty and therefore obligatory) only a few weighty initiatives are under consideration.

The first, the European Passenger Name Record (hereinafter – PNR) takes its inspiration out of the EU borders and is a very controversial initiative. The second – Information Exchange Platform is a pragmatic attempt to put in order everything carried out so far. And the third one is a long lasting discussion on the improvement of the principle of availability for which Member States seem not to be ready even more than 10 years after the establishment of this principle.

1. Data protection

In 2010, the Commission, in its Communication "A comprehensive approach on personal data protection in the European Union", analysed the established data protection system and as deficiencies of Framework Decision 2008/977/JHA indicated its application only to cross-border data exchange, too wide exceptions of purpose limitations, fragmentation of regulation by exceptions for Europol,

[694] OJ C 115, 4.5.2010, p. 18.

Eurojust, the Schengen Information System and other mechanisms.[695] Additionally, it can be said that due to the legislative form of framework decision, there is no effective tool to ensure its proper implementation and application across the EU.

A need for new data protection provisions has also been taken into account in the previously mentioned Article 16 and Declaration 21 of the Lisbon Treaty; this foresees that due to the specific nature of the police and judicial co-operation, separate data protection regulation in this area may be needed.[696] The need for separate legislation in this area was also reiterated by the Commission, emphasising that application to police and judicial co-operation in the criminal matters data protection regime, equal to other areas could jeopardise police and judicial work.[697] And as has been pointed out by the Committee of Legal Affairs of the European Parliament, "It should also be borne in mind, in the field of police and judicial cooperation, that legal traditions have developed very differently in the EU Member States in the course of the centuries, and any alteration to well-established national structures and traditions in this sensitive area through European rules should therefore be introduced cautiously and gradually."[698]

Bearing this in mind, on 25th January 2012, the Commission adopted a data protection package that consists of:

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Safeguarding Privacy in a Connected World a European Data Protection Framework for the 21st Century"; [699]
- Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data[700] (hereinafter – Draft Data Protection Regulation),
- Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal

695 See COM(2010) 609 final, p. 13-14.
696 See OJ C 83, 30.3.2010, p. 345.
697 See COM(2010) 609 final, p. 14. GONZÁLEZ FUSTER, Gloria. "Protección de datos y cooperación policial y judicial en material penal en la UE". In PÉREZ GIL, Julio. *El proceso penal en la sociedad…*, op. cit., p. 595.
698 EUROPEAN PARLIAMENT. Committee on Civil Liberties, Justice and Home Affairs "Report on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD))", p. 114, accessed September 4, 2015, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0403&language=EN.
699 COM(2012) 9 final.
700 COM(2012) 11 final.

> data by competent authorities, for the purposes of prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, and the free movement of such data[701] (hereinafter – Draft Data Protection Directive).

Deliberations on the Draft Data Protection Regulation are more advanced than on the Draft Data Protection Directive, as its first draft is already subject to a dialogue between the Council, the European Parliament and the European Commission. The trialogue is expected to be finalised before the end of 2015 and to adopt the legislative act in 2016, establishing transitional period of two years.[702] In the case of the Draft Data Protection Directive, the European Parliament issued its Resolution on 14th March 2014[703]. The Council agreed on its negotiating position with the European Parliament on 9th October 2015, and now trialogues will be started. Nevertheless, the text presented to the ministers still contains 129 comments and reservations, including eight Member States (Finland, Germany, Hungary, Italy, the Netherlands, Slovenia, Spain, the United Kingdom) that have general reservation about the whole text.[704]

1.1. Novelties of Data Protection Directive

The Commission with the Draft Data Protection Directive "aims to ensure a consistent, high level of data protection to enhance mutual trust between police and judicial authorities of different Member States, thus contributing further to a free flow of data, and effective cooperation between police and judicial authorities."[705]

Thus the proposed text is more ambitious, solid and comprehensive than current regulations provided by the Framework Decision 2008/977/JAI.

Regarding the scope of the proposal, the Commission has proposed applying the EU data protection rules, not only to cross-border information exchange, but also

---

[701] COM(2012) 10 final.

[702] See EUROPEAN DATA PROTECTION SUPERVISOR, "Europe's big opportunity. EDPS recommendations on the EU's options for data protection reform" (Opinion 3/2015), accessed, September 4, 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_EN.pdf.

[703] See European Parliament legislative resolution of 12 March 2014 on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, accessed, September 2, 2015, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0219+0+DOC+XML+V0//EN.

[704] See Council document 12643/1/15, p. 2.

[705] COM(2012) 9 final, p. 10.

to intra-state.[706] Some Member States[707] question whether this does not contradict the principle of subsidiarity and still keep this question open for further considerations. In October 2015, Croatia, Czech Republic, Germany, Denmark, Sweden, Slovenia, and the United Kingdom were still opposing to it.[708] According to Article 2, it is not applied for data exchange in activities that are outside EU law (such as national security), data exchange of EU institutions and its other entities.

In respect to subject matter, it is the same as the Framework Decision 2008/977/JAI, i.e. Prevention, detection and investigation of criminal offences and execution of criminal penalties. But the Council proposed broadening the scope and including prevention of threats to public security.

Article 4 of the Draft Data Protection Directive foresees the following protection principles: fair and lawful processing, collection for legitimate and specified purposes, relevance and minimum data necessary for the purpose, accuracy and updating, storage limitation, responsibility and liability of controllers.

Equal to the proposal of the Framework Decision, this time the Commission again included a provision on differentiation between distinct data subjects' categories: (suspects, convicted persons, victims, third parties (as witnesses) and other persons). But having previous experience with the position of Member States, this time it added a clause "as far as possible". Nevertheless, in the last version of Council amendments, this article and its division into different categories of data subject has been deleted.[709]

It would not be surprising if such a proposal would be revolutionary, but the same principle of differentiation is foreseen in the Recommendation (87)15 and applied in Europol and Eurojust.

The Draft Data Protection Directive envisages, as a general rule, the prohibition of processing the following categories of special data, "Revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, of genetic data or of data concerning health or sex life." Exceptions are permitted only when they are foreseen by law and with the application of the necessary safeguards or in order to protect a person's vital (data subject's or other) interests, or when the data subject has made it public.

An important novelty is the inclusion of genetic data into special data. The Council proposes to change general prohibition in order to process this data with strict

[706] It had been initially included in the draft of the Framework Decision as well, but rejected by the Member States.
[707] Croatia, Czech Republic, Denmark, Romania, Slovenia, Sweden, the United Kingdom.
[708] See Council document 12643/1/15, p. 33.
[709] See Council document 10335/15, p. 54.

permission under EU or national law and with the application of relevant safeguards as well. On the other hand , the Council modifies a person's vital interests into the broader concept of the prevention of the immediate threat to public security.[710]

The Council also seeks to increase the flexibility of an obligation to every controller or processor to appoint data protection officers, foreseen in Article 30 of the Draft Data Protection Directive in the same way as it has been made in Europol. Such an officer would have monitoring, advising and contacting functions with supervisory authority.

In relation to the information transfer to third countries, the Commission has proposed maintaining the same transfer purpose as previously[711], and with the fulfilment of the following alternative conditions:

- The European Commission has issued a Decision on the adequacy of data protection in the third country, territory or processing sector; [712]
- The Member State transferring the data provides the information on the third country, territory or organisation, binding law with satisfactory data protection level or control on the basis of performed assessment can confirm the existence of such safeguards.
- In exceptional cases, when it is necessary to: protect any person's vital interests or legitimate interest of data subject; prevent an immediate threat to public security; in individual cases for prevention, investigation or prosecution of crimes or execution of criminal penalties or for legal claims related to these activities.

It has to be taken into account that unlike the Framework Decision 2008/977/JAI, it regulates not only onward information transmission to the third country (i.e. Transmission by one Member State of information received from another Member State), but any transmission of data, meaning both proper and that received from another Member State. The Council considers the inclusion of provision on transfer only to those institutions of the third country that are responsible for crime prevention, detection, investigation or execution of penalties (equally as in the Framework Decision 2008/977/JAI), as well as to maintain the requirement of the consent of the Member State, where data originated for onward transmission (with the exception of cases when it is necessary to prevent an immediate threat to public security or essential interests). It also suggests that the Commission's

[710] See Council document 10335/15, p. 62.

[711] Prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

[712] It has also to evaluate third countries and to publish a list of those that do not provide an adequate level of data protection.

decision on adequacy would be approved, taking into account the opinion of the European Data Protection Board, i.e. A body envisaged in the Draft Data Protection Regulation to replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC and consisting of a head of a supervisory authority of each Member State.[713]

1.2. Weaknesses and critics

The Commission's Proposal in general puts forward quite a rational, effective and balanced set of data protection measures which, due to the proposed scope would ensure more protection than current the Framework Decision 2008/977/JHA.

Nevertheless, a "patchwork" or "kaleidoscope" system still remains, as exceptions of regulation for SIS, Europol, Eurojust and other data protection mechanisms are foreseen.[714]

The main horizontal criticisms from the European Data Protection Supervisor about the proposal, concern the form of the legislative act directive. The EDPS agrees that Declaration 21 has foreseen that for data protection in the area of police and judicial co-operation, special rules can be established, but it has not foreseen their legislative form. Therefore, the European Data Protection Supervisor is of the opinion that the form of regulation would be much more effective than directive, as it would be the act of direct application and would not depend on implementation measures.

Additionally, it underlines that "whilst the law enforcement area requires some specific rules, every departure from the general data protection rules should be duly justified based on a proper balance between the public interest in law enforcement and citizens' fundamental rights."[715]

The European Union Agency for Fundamental Rights acknowledges such a position and on this basis builds its own.[716]

[713] See Council document 9565/15, p. 59, 174 (Recital 110, Article 64).

[714] PEYROU, Sylvie, "Algunas reflexiones sobre la protección de datos en el ELSJ o la crónica de una esperanza frustrada" in GOIZUETA VÉRTIZ, Juana; GONZÁLEZ MURUA, Ana Rosa and PARIENTE DE PRADA, Iñaki, *El Espacio de Libertad, Seguridad...,* op. cit., p. 148-149.

[715] EUROPEAN DATA PROTECTION SUPERVISOR, "Executive summary EDPS Opinion of 7 March 2012 on the data protection reform package", OJ, C 192, 30.6.2012, p. 8

[716] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, "Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package", October 2012, p. 2, 7, accessed September 3, 2015, http://fra.europa.eu/en/opinion/2012/fra-opinion-proposed-eu-data-protection-reform-package.

Of course, in the case of non-implementation or incorrect implementation of the directive, the previously mentioned infringement procedure can be started. But it takes a lot of time and it means that in one or more Member States, relevant data protection measures would not be in place and would not guarantee equal rights to data protection across the whole of the European Union.

Guasch Portas additionally reminds us that the Commission itself has criticised Directive 95/46/EC for its indirect application. [717]

Bearing in mind that data protection is a fundamental right, it would be more reasonable to approve a directly applicable regulation, especially taking into account that the legislative procedure would be similar.

The European Parliament has gone even further, declaring that is in favour of regulating all data protection (including the area of police and judicial co-operation) within the unique regulation. Such a position is not lacking reasons, because there are some areas in which both new draft regulations and draft directives could be applied, such as customs, immigration or environment.[718]

Regarding precise modifications, the three aforementioned subjects have proposed the following main modifications:

- The European Data Protection Supervisor has insisted on the establishment of the obligation (not only foreseeing the possibility) to make differences in distinct categories of persons.

  It has suggested introducing periodic evaluation mechanisms on how the provisions on data protection are applied. It should be appreciated as a very useful tool that would ensure that data protection rules are not only transposed, but also effectively applied on a daily basis.

  In the case of data transfer to a third country, it has pointed out the weakness of the provision in relation to the assessment performed by the Member State. It has advised to specify that for such an assessment, it is obligatory to receive an opinion of the supervisory authority of that Member State. If such a suggestion would not be admissible by Member States, then it proposes to delete all provision on assessment.[719]

- The European Union Agency for Fundamental Rights has proposed explicit prohibition of the transmission of data to third states, where, on the basis

[717] See GUASCH PORTAS, Vicente, *Las transferencias internacionales de datos…,* op. cit., p. 293.
[718] Ibid, p. 294.
[719] EUROPEAN DATA PROTECTION SUPERVISOR, "Executive summary EDPS…", loc. cit., p. 13-14.

of human rights records, it can be concluded that transferred data could be used to interfere in human rights.[720]

- The European Parliament has adopted 98 amendments[721] and the most significant of them are the following:

  a) To include Europol and Eurojust under the regulation of this legal act;

  b) To introduce provisions on data storage terms and revision;

  c) Similarly to the European Data Protection Supervisor, to make obligatory differentiation between distinct categories of persons;

  d) To establish separate article regulating processing of genetic data;

  e) To strengthen requirements of data transfer to the third countries.

These criticisms were addressed to the Commission's proposal. Supposedly, criticisms of the modifications that take place in the Council would be much stronger as in general, they do not carry any advance, but try to maintain the current *status quo*. Thus the time will show the results of trialogues.

In the light of the amendments proposed by the Council, it has even more sense to keep Europol and Eurojust outside of the scope of the Draft Data Protection Directive as these agencies have more restrictive data protection rules than the ones proposed by the Council, for example, the agencies already have rules on differentiation between distinct categories of persons. Adoption of the Draft Data Protection Directive as proposed by the Council would mean that different data protection rules would be applied to the same information, depending on whether it is transmitted through Europol (it would be categorised) or directly (it would not pass any process of categorisation). In such a situation, it would be more beneficial for victims or witnesses that Europol would process their data instead of direct transmission between national competent authorities.

2. The future of Europol

As already mentioned, Article 88(2) of the TFUE envisages that Europol has to be regulated by means of regulations adopted by applying ordinary legislative procedure.

The TFUE foresees Europol's:

[720] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, "Opinion of the European Union…", loc. cit., p. 11.

[721] See EUROPEAN PARLIAMENT. Committee on Civil Liberties, Justice and Home Affairs, "Report on the proposal for a directive…", loc. cit.

- Possibility to collect, store, process, analyse and exchange of information;
- Possibility to coordinate, organise and implement investigative and operational actions carried out jointly with the Member States;
- Scrutiny by the European Parliament;
- Impossibility to apply coercive measures.

Following the TFEU, as time dictated necessities, the Draft Europol Regulation foresees 5 goals:

a) To fulfil the requirements of the Lisbon Treaty of parliamentary control,

b) To implement the provision of the Stockholm Programme, making Europol "a hub for information exchange between the law enforcement authorities of the Member States"[722];

c) To ensure more comprehensive support for the Member States by over taking functions of CEPOL, and the elaboration of specialized expertise in certain types of crime (such as the establishment of European Cybercrime Centre);

d) To improve data protection regime;

e) To improve governance.

It has to be stressed that both the Council and the European Parliament rejected the idea to merge the two agencies (Europol and CEPOL), and therefore this aspect will not be analysed further. At the end of June, the Council of the European Union and the European Parliament reached a compromise on the Proposal of the Regulation of European Parliament and of the Council, by establishing a European Union agency for law enforcement training (Cepol), repealing and replacing the Council Decision 2005/681/JHA[723] presented by the Commission on 30th September 2014, to be voted in Plenary of the European Parliament and adopted by the Council.[724]

One of the most important changes that has been raised for years is Europol's democratic control by the European Parliament. The first time it was mentioned was in 1999, and as Puntscher Riekmann states, "Developments [...] from an initial focus on specific crimes towards organized crime in general, and from an initial role of handling information towards operative powers. In view of these

[722] OJ C 115, 4.5.2010, p. 20.
[723] COM(2014) 465 final/2.
[724] See COUNCIL OF THE EUROPEAN UNION. "CEPOL: Council and Parliament agree on updated rules" (Press release 30 June 2015), accessed, September 3, 2015, http://www.consilium.europa.eu/en/press/press-releases/2015/06/30-cepol-updated-rules/.

developments, and due to the important and sensitive nature of Europol's activities, the question of its accountability seemed unavoidable." [725]

In the context of the scrutiny of Europol's activities, the Draft Europol Regulation established the European Parliament's right:

- To receive organisational documents, such as multi-annual and annual working programmes, activity reports, budget accountability reports;
- To receive strategic products: threat assessments, strategic analyses and general situation reports, agreements with third parties, reports on quantity and quality of information provided by Member States;
- To invite candidates for the Director and for his or her Deputies for hearing, as well as the Director to reply to the questions;
- To discuss with the Executive Director and the Chairperson of the Management Board matters relating to Europol.

For the effectiveness of these contacts, a working arrangement between Europol and the European Parliament on access to confidential information has to be concluded.

Corresponding to this proposal, the European Parliament has proposed establishing a Joint Parliamentary Scrutiny Group to perform a review of Europol's activities and added more documents that have to be submitted to parliamentary control.[726]

In order to enhance Europol's role as an information hub, it is proposed to strengthen Member States' obligations to provide information and to establish monitoring mechanisms of their contributions.

Another novelty related to the processing of information was the elimination of provisions on pre-defined information systems and adopting a "privacy by design" approach and full transparency towards the Data Protection Officer at Europol and the European Data Protection Supervisor.[727]

To improve data protection regime, the Commission offered to strengthen the role of external supervision of data protection by granting more direct supervision functions.

---

[725] RUIZ DE GARIBAY, Daniel, "Coordination Practice in the Parliamentary Control of Justice and Home Affairs Agencies: The Case of Europol" in CRUM, Ben and FOSSUM John Erik, *Practices of interparliamentary coordination in international politics* (Colchester: ECPR Press, 2013), p. 89-90.

[726] The annual report of the European Data Protection Supervisor in relation to Europol, the Commission's report on the effectiveness and efficiency of Europol as well as any other document necessary for the fulfilment of the control task.

[727] COM(2013) 173 final, p. 8.

With respect to the main changes in management, according to the Draft Europol Regulation, a representative of the Commission would take a place on the Management Board. The latter would have the right to establish its Executive Board that "could be more closely involved in the monitoring of Europol's activities with a view to reinforcing supervision of administrative and budgetary management, in particular on audit matters."[728]

The following subdivisions will analyse in more depth the Draft Europol Regulation, and the positions of the Council and the European Parliament on questions related to changes of Europol's status in general, and information exchange in particular.

2.1. Strengthening Europol's role

As already mentioned, the Draft Europol Regulation has a goal to strengthen Europol's role as an information hub, by imposing a strong obligation to provide information on Member States, and giving it powers to coordinate investigations.

Moreover, Europol's possibility to provide not only technical, but also financial support to cross-border operations and to maintain direct contacts with competent authorities and not only ENU is also foreseen. That supposes making co-operation with Europol more attractive to national law enforcement institutions, and guarantees its involvement in more operations. On the one hand, it could be treated as a positive development that will ensure Europol's visibility and "closeness" to national competent authorities (that not always shows total trust to the Agency), as well as one more step towards real support to Member States in their fight against serious crime. On the other hand, it can be treated as an attempt "to buy" the trust and co-operation of sceptical law enforcement institutions by the scheme: direct contact, financing of operations and as a consequence – obtaining its coordination. This novelty also diminishes the role of the ENU that until now, was a unit aware of all on-going operations of the Member States considered with Europol. With direct contacts in the way, as proposed by the Commission, this thread is lost.

Such a development can be appreciated by those Member States that have many separate police authorities (like France, Italy or Spain), and due to the requirement of a single ENU per Member State, only one of them has to be included in its structure. Thus the rest of the authorities, in order to get involved in co-operation with Europol, have to reveal their operations to one which has an ENU, and not in every case are they ready to do that; this is due to competitiveness or other

[728] Ibid, p. 12.

reasons. In such situations, they prefer to use other co-operation tools such as bilateral agreements, liaison officers, and so on. But for these Member States, a better solution would be allowing the establishment of an ENU in every police force, and not to maintain the current model of a single ENU allowing direct contact with national authorities.

The proposed decentralisation of co-operation at the level of direct contacts with law enforcement institutions can be considered as a perverse development, and could even provoke negative consequences to investigation. Not all competent authorities (especially at territorial level) are properly aware of the peculiarities and limitations on cross-border co-operation, and can agree on actions that in the end, in the best case scenario, will not serve for the prosecution and in the worst case scenario, could ruin the investigation. Let's take as an example crown witness's protection, or use of undercover officers and the involvement of the local competent authority (not the central one). The legislation of every country regulates these actions and will be perfectly known to local authorities; Europol can inform them about the existence or not of EU level regulations; but what about bilateral and multilateral agreements? The situation with bilateral agreements will be perfectly known to the central competent authority, and to units dealing with international co-operation (including ENU), but not necessarily to the local authority. Without such knowledge, the local authority could agree to measures that are not allowed in cross-border co-operation between some states. Let's imagine that an undercover officer is sent to a country where his status is not regulated by bilateral or multilateral agreements. In the best case scenario, information gathered by him or her will not have evidential power in the process, in the worst case scenario, if he or she were discovered by the criminal organisation, who would be responsible for his or her security, and on which basis?

The Council, in its first reading, has changed Article 4, proposing Europol's coordinating role, into a supporting role [729], and has modified strong wording about the financing of operations into a position of possibility; it has also established that Europol's direct contacts with competent authorities can take place with prior authorisation by ENU, and can be subject to other conditions foreseen by the national legislation of involved Member States. The European Parliament also has suggested leaving co-operation through ENU as a general rule.

[729] Even if the term of coordination is established in Article 88 of the TFEU, it does not have an obligatory nature.

Following Article 88(3) of the TFEU, the Council and the European Parliament have agreed on the inclusion of a clear general statement of non-application of coercive measures by Europol.[730]

Article 7 of the Draft Europol Regulation also includes a controversial statement, "Member States shall cooperate with Europol in the fulfilment of its tasks."[731] It goes against the wording of the Article 88(1) of the TFEU that is clearly supportive of Europol's position in relation to Member States' law enforcement agencies and not the contrary. Therefore, the Council has changed this wording into cooperation in the fulfilment of the tasks of Member States and Europol. The position of the European Parliament in this question is ambiguous because in general, it considers Europol as "back-up for national law enforcement bodies"[732], but on the other hand, has not proposed any amendments to the proposed Article 7.

The Council and the European Parliament also softened Member States' obligation to provide information to Europol with foreseeing exceptions in following cases "(a) harm national security interests; (b) jeopardise the success of a current investigation or the safety of individuals; or (c) disclose information relating to organisations or specific intelligence activities in the field of national security."[733]

It can be concluded that having an Area of Freedom, Security and Justice as supranational, and no longer intergovernmental, the Commission decided to try to give to Europol maximum of prominence, in some cases going even beyond and against the provisions of the TFEU.

2.2. New legislative approach to regulate Europol's data bases

As already mentioned, the Draft Europol Regulation does not regulate specific Europol databases, but just establishes the purposes for which the information can be processed. After some Council's suggestions, the purposes are the following "(a) Cross-checking aimed at identifying connections between information; (b) Analyses of a strategic or thematic nature; (c) Operational analyses in specific cases**;** (d) Facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations."[734]

[730] In Europol Decision, as well as in the Draft Europol Regulation, such prohibition refers only to participation in joint investigation teams.
[731] COM(2013) 173 final, p. 29.
[732] Council document 6745/1/14, p. 2.
[733] Council document 10033/14, p. 38.
[734] Ibid, p. 64.

The European Parliament has considered that for cross-checking, only information about persons suspected of already having committed a crime, or of its future commission should be processed. It makes perfect sense, because the current Europol Decision establishes the same limits for the content of EIS, whose function by its nature is similar to cross-checking. The European Parliament has also proposed that the European Data Protection Supervisor should draft guidelines in respect of the first three information exchange purposes.

From one angle, it is reasonable to establish only information processing purposes, leaving out the regulations of EIS, AWF and other possible systems, as they depend on the necessity of changing the situation or new technological developments, and can need some modifications or new solutions. Envisaging their rules in Regulation would mean a need for its modification every time a need to develop or change the system occurs.

From another angle, it is surprising that support for modifications did not foresee any rules at all on the creation of such systems: neither in relation to who has to take the decision, nor which criteria have to be taken into account in this process. It seems that Europol has "untied hands" to decide when and what system to create, and it is totally contrary to IMS, discussed in section 3 of Chapter I. As in the creation of any new information processing system, not only the business needs have to be defined; the involvement of Member States and multidisciplinary coordination (with other bodies and systems) has to be respected. Without clear rules, direct parliamentary control would also be diminished as it could lead to influence only through the budget (that is indispensable for the creation of any tiny system).

In order to avoid unilateral decision in this respect, the Council at least has introduced into the tasks of the Management Board the adoption of "procedures and business processes required for the processing of information by Europol [...] having obtained the opinion of the European Data Protection Supervisor."[735]

Supposedly, such procedures can previse criteria and steps to establish any new system.

The European Parliament has proposed an assessment, not from the perspective of coherence with IMS, but from data protection, "Prior to any set of processing of personal data, Europol shall carry out an assessment of the impact of the envisaged

[735] Ibid, p. 48.

processing systems and procedures on the protection of personal data and notify it to the European Data Protection Supervisor."[736]

Regarding the processing of the personal data of victims, witnesses, contacts, associates, informers and minors (that under Europol Decision (except minors) is possible in AWF, i.e. For the purpose of analysis), Article 38 of the Draft Europol Regulation prohibits it, with the exception "strictly necessary cases". But the Council has proposed to change this wording to make it more flexible and to allow it, not only for the purpose of analysis, but also to facilitate the exchange of information.[737] Such position has double aspect: on one hand it is understandable wish to make the biggest benefit from Europol as information hub, from another side the question of proportionality and conformity with fundamental rights occurs. In this respect, the wording proposed by the Commission seems to be more appropriate.

2.3. Co-operation with the EU bodies and third parties

The Draft Europol Regulation foresees that for the exchange of non-personal data Europol can conclude working arrangements with EU bodies and third parties that do not bind the EU or its Member States. Nevertheless, no regulation of processing of classified information between these entities is foreseen.

It also envisages granting Eurojust and OLAF with hit/no hit based access to information, including personal data, processed by Europol. But the European Parliament considers that only Eurojust should have such access, and it can be justified by the existence of the operational work arrangement between only Europol and Eurojust. As far as OLAF is concerned, the co-operation is based on strategic working arrangement that do not foresee personal data exchange.[738] The Council considers the possibility of hit/no hit access of both EU bodies "while such access would by technical means be limited to information falling within the respective mandates of these Union bodies."[739] Taking into account that OLAF's task is to investigate fraud, corruption and other crimes related to the financial interests of the EU, it cannot be discarded that OLAF's investigation would be related to some organised group, and that Europol has information on it. It would help to co-ordinate actions and to avoid redundant use of human resources.

Article 30 of the Draft Europol Regulation expressly permits personal data transmission to the EU bodies, although previously it was allowed only under

[736] Ibid, p. 61.
[737] Ibid, p. 137.
[738] See Subsection 2.2.1 of the Chapter IV.
[739] Council document 10033/14, p. 67.

operational working arrangements that Europol, for the time being, only has with Eurojust. Such transmission shall be related to the competence of Europol or other participating EU bodies, and concern a person suspected or convicted of a crime, or the commissioning of a suspect of future commission. The personal data of other categories of persons, as well as special categories of data can be revealed to other EU institutions only if it is necessary to prevent or combat a crime. Subject to Europol's competence.

In relation to third parties, new regulations foresee three backgrounds for personal data exchange:

- The commission's decision that the data protection level of the third state or a territory is adequate;
- EU agreement with a third party;
- Europol's and third parties' already existing operational agreements.

As the first two bases would include very general provisions, Europol and the third party concerned can conclude administrative arrangements that would specify rules on information exchange and its further processing.

In addition to the already applied reasons for personal data transmission to a third state without relevant agreement, new regulations specify what necessity means in individual cases[740]; it widens the motives of imminent terrorist attack threat on Member State into "immediate and serious threat to public security of a Member State or a third country", and envisages new reasons for transfer:

- In order to protect the vital interests of the data subject or another person; or
- To safeguard the legitimate interests of the data subject where the law of the Member State transferring the personal data so provides.[741]

A big novelty is the establishment of the possibility of the Management Board with the authorisation of the European Data Protection Supervisor, in order to allow a set of transfers during one year. It can be done in cases of where the above mentioned reasons exist and permit data transmission without agreement, or the Commission's Decision, and if third states apply rules safeguarding data protection and fundamental rights. Although this solution is not perfect, it is at least more objective and reasonable that Europol's unilateral decision to transfer data to third

[740] Purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions; or the establishment, exercise or defence of legal claims related to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal sanction.

[741] Council document 10033/14, p. 74.

states, especially taking into account that the biggest part of data processed by Europol comes from Member States, and they keep responsibility for it use and misuse.

2.4. European Cybercrime Centre (EC3)

Unlike the current regulation, the Draft Europol Regulation in its Article 4 expressly mentions EC3, defining it as one of Europol's task developments of "union centres of specialised expertise for combating certain types of crime falling under Europol's objectives, in particular the European Cybercrime Centre".[742]

Additionally, in 2013, the Proposal of the Draft Europol Regulation was complemented with the Commission staff working document "Ex-Ante Evaluation: Resources needed to fulfil the tasks set forth in the Commission's Communication on the establishment of a European Cybercrime Centre (EC3)"[743] (hereinafter – Working Document on EC3) that among the specific objectives of EC3 foresees "more extensive, faster information exchange among all stakeholders (Member States, third countries, leas, industry etc.) And more effective management of information flows (i.e. data fusion, helpdesk and reporting mechanisms)".[744]

Nevertheless, no more clarity on rules of information exchange within EC3 is provided, and that again leads to the conclusion that it works on the same information exchange basis as Europol in general.

In the Draft Europol Regulation, it is foreseen that information from private parties and persons is received by Europol trough ENUs. Notwithstanding, in the Working Document on EC3, it is already considered that such an information delivery chain results in substantial delay, an additional burden to the private sector, and is "a potential stumbling block" and the flexibility of such data exchange should be considered.[745]

For the time being, the Council has not made any differences in the regulation of data exchange with the private sector, but it has not approved its final position either.

[742] COM(2013) 173 final.
[743] SWD(2013) 100 final.
[744] Ibid, p. 9.
[745] Ibid, p. 7, 11, 12.

3. Passengers Name Records (PNR)

An indispensable element of free movement of persons is the abolishment of controls on internal borders and the strengthening of external ones. As already explained, at every crossing point of the external border of the Schengen area it is obligatory to use SIS. To review its functions it should be said that it works on the basis of alerts in relation to some categories of persons and objects.[746] That means that previous to placing an alert, a competent authority of a Member State should have information in relation to that person or object. But what to do with those crimes that remain undetected, and those persons that commit them, but do not fall under suspicion due to lack of information? In these cases, the active intelligence work of competent authorities can be more helpful; and to some extent the use of PNR, i.e. Data possessed by air carriers related to bookings, carrying out the check-in process and used to control flows of passengers. In particular, it includes personal data, means of payment, passengers' meal and other preferences.

PNR use for law enforcement purposes is based on the transmission of data related to passengers obtained from air carriers by national passenger information units, where it is evaluated on the basis of the risk criteria, and transmitted to the competent law enforcement institution. Air carriers do not have to collect any additional data, only that which they have been collecting until now. Their additional expenditures would only be related to the transmission of collected data to law the enforcement authority competent to carry out its processing.

As a general rule, it is applied for the processing of information of air travellers, but it does not eliminate the possibility to apply it to railway or water transport.

It can be used as a pro-active, real-time and re-active measure. Its biggest advantage would be pro-active and real-time use.[747] When it stands for re-active measures, without denying the importance that PNR can have in some specific cases, on a large scale it would not be such an effective investigation tool as others (for example biometric data).

[746] Persons wanted for extradition or surrender, sought to assist with a judicial procedure, missing persons, persons and objects for discreet and specific checks, objects for seizure or use as evidence.

[747] According to the information presented by Belgium in 2009, 95% of all drugs seizures in airports were made thanks to PNR data. See COM(2011) 32 final, p. 6. Nevertheless, this data is questionable by the European Data Protection Supervisor, as at that moment Belgium had not finished the implementation of systematic PNR collection scheme. See EUROPEAN DATA PROTECTION SUPERVISOR, "Opinion of the European Data Protection...", loc. cit., p. 25.

To apply it at EU level, on 6th November 2007, the Commission presented a "proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes".[748]

As Member States had not found a common agreement on this proposal until the entrance into force of the Lisbon Treaty, the Commission had to present a new proposal according to the requirements of the new legislative procedure. It was achieved on 2nd February 2011 by presenting 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"[749] (hereinafter – Commission's Proposal on PNR).

In respect to the progress of legislative procedure of this draft, the Council of the European Union has not issued yet a text as an outcome of the first reading, but on April 2012 reached general approach with numerous reservations of Member States.

On 24th April 2013, LIBE had rejected the Commission's Proposal on PNR, but then the Plenary returned the file to LIBE.

This initiative is included in this work because after the terrorist attacks in France in January 2015, and taking into account recruitment by the so called Islamic State, the Council declared its determination "to create without further delay an effective EU PNR framework in line with Council general approach and at the same time ensuring solid data protection safeguards".[750]

On 11th February 2015, the European Parliament adopted a Resolution on anti-terrorism measures and declared its commitment to work in order to finalise the PNR legal act until the end of 2015, and encouraged the Council to make progress on the Data Protection package in order to have trialogues on both initiatives in parallel.

3.1. Commission's Proposal on PNR

As the main reason for the proposal, the Commission took the political will expressed in the Stockholm Programme "to propose a Union measure, that ensures a high level of data protection, on PNR for the purpose of preventing, detecting,

[748] COM(2007) 654 final.
[749] COM(2011) 32 final.
[750] Riga Joint Statement following the informal meeting of Justice and Home Affairs Ministers in Riga on 29 and 30 January, p. 2, accessed 5 September 2015, https://eu2015.lv/images /Kalendars/IeM/2015_01_29_jointstatement_JHA.pdf.

investigating and prosecuting terrorist offences and serious crime, based on an impact assessment."[751]

Within the scope established by the Stockholm Programme, the Commission's Proposal on the PNR aim is to apply its processing from flights between a third country and a Member State (from Member State or to Member State) or so called extra-EU flights. Thus at least at this stage, only air carriers are considered. This provision was the subject of numerous discussions.

The opinion of the European Parliament and European Data Protection Supervisor differ about including intra-EU flights, as the latter is concerned it represents an even bigger limitation of privacy and data protection.

The Council's preparatory bodies have included a provision on the possibility of using it for all intra-EU flights, or selected ones if a Member State so wishes.

On the one hand, only controlling extra-EU flights does not mean the full use of the system for the prevention of and combatting terrorism and crime, as monitoring intra-EU flights can also serve for these purposes. Additionally, a person can face different treatment from his or her PNR travelling from the Canary Islands to Amsterdam (which is one of routes used for drug trafficking) and from the Canary Islands to Monaco. Additionally, the creation of such a system is costly[752] and the question of economic efficiency should be taken into account: to use it to its full potential or not to start at all.

On the other hand, the Commission's Proposal is totally understandable and the position of EDPS as a collection of PNR data of intra-EU flights would not only mean a disproportionate limitation of privacy and data protection, but it also contradicts to the essence of free movement.

The Commission proposed the following information processing scheme:

- Each Member State (or a few of them) has to establish a Passenger Information Unit (hereinafter – PIU) that will be responsible for receiving information from the air carrier and its processing.
- As the main method to receive information was elected "push", meaning that air carriers transfer it to PIU, leaving the "pull" method (the extraction

[751] OJ C 115, 4.5.2010, p. 19.

[752] For the time being it is possible to apply to the EU for funds and this has been done by Austria, Bulgaria, Denmark, Estonia, Finland, France, Hungary, Latvia, Lithuania, Portugal, Romania, Slovenia, Spain, Sweden and the total amount granted reaches 50 million euros. See BĄKOWSKI, Piotr and VORONOVA, Sofija, "The Proposed EU Passenger Name Records (PNR) Directive: Revived in the New Security Context" (Briefing, European Parliamentary Research Service, April 2015), accessed July 14, 2015, http://www.europarl.europa.eu/EPRS/EPRS-Briefing-554215-The-EU-PNR-Proposal-FINAL.pdf.

of information from the air carriers' data bases) only in exceptional cases. According to Article 6(1), if the flight is co-shared between different air carriers, the airline that operates the flight has to ensure information transmission. In this manner, PIU will not have direct access to all information processed by air carries, but only to the one sent to it. On the one hand, it strengthens the right to privacy and data protection, but on the other hand requires the establishment of an electronic system that would not allow air carriers to delete information on certain passengers and transmit it to PIU only on behalf of them. This observation should not be understood as general mistrust of air carries, but nobody can be sure that a person responsible for data transmission is not involved in a terrorist organisation or does not form part of a drug or human trafficking network. Therefore, there should be technical means that do not allow the manipulation by the air carrier of the received PNR.

– It always has to be transmitted immediately after the flight closure and when the air carrier agrees to do so, before the scheduled departure (within 24-48 hours).

PIU, applying assessment (risk) criteria, determines suspicious movements, repetition of the same itinerary, and so on. And in the case of their detection, transmits the relevant information to national competent authorities[753] and when there are links with other Member States and it would help it to prevent, detect, investigate and prosecute terrorist offences and serious crime - to its PIU. The PIU is also authorised to request information from other PIUs. Direct contact between the PIU of one Member State and the competent authorities from another, are allowed only in urgent cases.

Talking about the scope of the Commission's Proposal on PNR, it has continued to state that it is terrorism, serious crime and serious transnational crime within the scope of the already mentioned Framework Decision 2002/584/JHA, and the maximum sentence is at least three years' imprisonment. The fact that it refers not only to international (different states involved), but national serious crime as well deserves special attention. Nevertheless, the Council's preparatory organs have added Annex II with the explicit list of offences in which PNR can be used.[754] A

[753] According to Article 5 of the Commission's Proposal on PNR, those authorities which are competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime.

[754] Participation in a criminal organisation, trafficking in human beings, sexual exploitation of children and child pornography, illicit trafficking in narcotic drugs and psychotropic substances, illicit trafficking in weapons, munitions and explosives, fraud, laundering of the proceeds of crime, computer-related crime, environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties, facilitation of unauthorised entry and residence, illicit trade in human organs and tissue, kidnapping, illegal restraint and hostage-taking, organised and armed robbery, illicit trafficking in cultural goods, including antiques and

discussion remains as to whether a requirement of a three year sentence should be applied or not, due to differences in national legislations.

Article 8 of the Commission's Proposal on PNR also foresees possibilities (although limited) to transmit data to third countries. It can be done on a case-by-case basis for the same purposes as PNR processing within the EU, and respecting the data protection rules established in Article 13 of Framework Decision 2008/977/JHA (see Chapter II, Subsection 5.3).

In addition, there is also provision on onward transmission for the same purpose and with the authorisation of Member States, where PIU has processed the data.

According to Article 18, Member States are obliged to collect statistics at least about the total number of collected and exchanged PNR, the number of persons elected for scrutiny and further actions of competent law enforcement institutions.

As indicated by Bąkowski and Voronova "The proposed EU PNR scheme departs from the widely accepted form of using personal data for law enforcement purposes whereby data transfer is requested [...] for a specific person, suspected of a specific crime, or at least representing a specific threat. The PNR scheme enables, on the contrary, proactive systematic checks on large sets of data concerning all passengers."[755]

Regarding storage rules, the Article of the Commission's Proposal on PNR foresees that from air carriers, received data is stored in the PIU data base for 30 days. Afterwards it is masked out from data that can reveal the identity of a person and stored for five years. The storage term can be extended only if the data is used for crime investigation or prosecution. Only a limited number of PIU officers can have access to masked data and access to full data (revealing identity details again) is only possible with the permission of the Head of PIU, and only on a case-by-case basis in order to answer the request of the competent authority for the purpose for which the PNR is processed.

The Commission's Proposal on PNR for data protection dedicates only two articles. Articles 11 and 12 provide only the general framework that shall be forwarded, but as PIU and data processing will take place in each country separately without any centralised data base, it is left up to the national legislation of each Member State.

works of art, forgery of administrative documents and trafficking therein, illicit trafficking in hormonal substances and other growth promoters, illicit trafficking in nuclear or radioactive materials, unlawful seizure of aircraft/ships, sabotage and trafficking in stolen vehicles. Council document 8448/2/12, p. 36-37.

[755] BĄKOWSKI, Piotr and VORONOVA, Sofija, "The Proposed EU Passenger Name…", loc. cit.

Article 11 foresees the obligatory application of Articles 17-22 of the Framework Decision 2008/977/JHA that establishes rules on the data subject's right to access, rectification, deletion, blocking and rectification as well as rules on data confidentiality and security.

As specific data protection rules are established:

- Prohibition to process sensitive data (although as already mentioned, the categories do not coincide fully with the ones established in Article 21 of the EU Charter).
- Lodging or documentation of all data processing and keeping it for 5 years. If PNR data is not deleted after 5 years, the logs will be kept until the deletion of that data.
- Proportioning of information to each passenger, about PNR processing for law enforcement purposes.
- Prohibition of transmission of data to private parties.

The Commission's Proposal on PNR foresees the deadline of its implementation two years since its coming into force. It seems to be unrealistic that all Member States would put in place the whole system, especially taking into account that two parts of them have never used PNR on a daily basis, and do not have either technical or expert preparation.

3.2. Weak points and critics of the proposal

As previously indicated , in 2013, the LIBE rejected the Commission's Proposal on PNR voting 30 to 25,[756] although the Rapporteur did not propose that in its Report.[757] The Rapporteur proposed only 35 amendments, recognising the added value of the initiative and pointed out that the Commission had taken into account recommendations made by the Parliament in its Resolution of 20th November 2008, on the proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes[758], even if that Resolution had considered, in general, that while combatting crime "the same or even better

[756] See EUROPEAN PARLIAMENT, "Civil Liberties Committee rejects EU Passenger Name Record proposal Fundamental rights" (Press release 24 April 2013), accessed September 2, 2015, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BIM-PRESS%2B20130422IPR07523%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN.

[757] EUROPEAN PARLIAMENT, Committee on Civil Liberties, Justice and Home Affairs, "Report on the proposal for a directive…", loc. cit.

[758] EUROPEAN PARLIAMENT, "Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes", OJ C 16E, 22.1.2010, p. 44-50.

results could be obtained by improving mutual legal assistance between law enforcement authorities."[759]

Nevertheless, the same Resolution did not eliminate the possibility of the PNR system, but with much more limited scope and purpose, a strong data protection regime and establishing that "Profiling based on PNR data should only be intelligence-led, based on individual cases and factual parameters".[760]

The Resolution also envisaged a sunset clause in which national parliaments would participate, the European Parliament, the EDPS, the Article 29 Working Party and the FRA.

To return to the Commission's Proposal on PNR, after the Resolution of 11th February 2015, the Rapporteur increased its amendments from 35 to 47 retaining his initial position, but the rest of the Members of Parliament proposed 789,800 amendments[761], starting from the proposal to the rejection of the initiative, proposing the inclusion of intra-EU flights, limiting the purpose to certain types of serious crimes, strengthening data protection and access provisions, etc.[762]

The EDPS has noticed the improvement of data protection regulation in the Commission's Proposal on PNR, compared with the draft from 2007;, reduction in the scope of the instrument and better impact assessment for example, but it has highlighted that it "still fails to find in these new justifications a convincing basis to develop the system, especially with regard to large scale 'prior assessment' of all passengers."[763]

The PNR is in use, or prepared to be use, in only six Member States, thus it is not data usually gathered at national level and that means that:

- Crime prevention and prosecution can be performed by using other means;

[759] Ibid, p. 45.

[760] Ibid. The same was pointed out in the opinion of the EDPS, See EUROPEAN DATA PROTECTION SUPERVISOR "Opinion of the European Data Protection Supervisor 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" OJ C 181, 22.6.2011, p. 26.

[761] With 179 amendments only on recitals.

[762] EUROPEAN PARLIAMENT, Committee on Civil Liberties, Justice and Home Affairs, "Amendments 48-329 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, accessed September 6, 2015, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/am/1058/1058388/1058388en.pdf.

[763] EUROPEAN DATA PROTECTION SUPERVISOR, "Opinion of the European Data Protection…" (2011), loc. cit., p. 25.

– Member States that do not use PNR and do not have such a system will be obliged to establish it.

In these circumstances, a question of necessity and proportionality to limit passengers' privacy becomes more and more relevant.

In the use of PNR for law enforcement purposes, the FRA sees the limitation of the fundamental right to privacy, to data protection and to non-discrimination. With respect to non-discrimination, it indicates that even not processing sensitive data does not eliminate non-discrimination as the list of sensitive data presented in the Commission's Proposal on PNR is shorter than the one foreseen in Article 21 of the Charter.[764] It also refers to the sunset clause foreseen in the Resolution of the European Parliament from 2008 and stresses that for this purpose, not only statistics on all collected data, persons identified for scrutiny and further law enforcement action, but also the number of persons "unjustifiably flagged as suspicious" by the PNR system has to be part of it.

When it comes to proportionality and necessity, the FRA notices that examples provided by the Commission on different occasions do not prove its indispensability to terrorism and all serious crime, but only a few of them: drug trafficking and trafficking in human beings.

In these circumstances, a question occurs: is PNR use for law enforcement purposes proportional and indispensable?

From the examples provided by the Commission, itis not clear where the PNR data helped more, in investigations of drug or human trafficking or through advanced passenger information (hereinafter – API), collected and transmitted to law enforcement agencies as well. The Commission states that API is more limited than PNR as it is "the biographical information taken from the machine-readable part of a passport and contain the name, place of birth and nationality of the person, the passport number and expiry date."[765]

What is even more appealing is Europol's position on this issue, given that it offers its infrastructure to "help national competent authorities to maximise their use of targeted PNR information, to achieve a better intelligence picture and ultimately to

[764] See EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, "Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final)", p. 7, accessed September 5, 2015, http://fra.europa.eu/sites/default/files/fra_uploads/1654-FRA-PNR-Opinion-June2011.pdf.

[765] COM(2011) 32 final, p. 6-7.

close security gaps which purely national PNR systems would fail to address (by making links and obtaining additional transnational information)."[766]

This proposal seems to be very provocative, because on the one hand, it impugns the effectiveness of "purely national PNR systems" and on the other it proposes "maximising "the use of target information that goes absolutely in contradiction to fundamental rights, especially taking into account that among targeted PNR information will be information about persons who have never been under none suspicion. What can be allowed in this case is checking by competent authorities on hit / no hit basis information of some of the targeted PNR with Europol's data bases, and only in cases of a match, to proceed with finding out links. Nevertheless, not all targeted PNR information should be checked, but only that which gives sufficient background to suspect a person's involvement into terrorism or serious crime; for example, repetitive itineraries on dates that coincide with repetitive crimes that have the same modus operandi.

Such PNR data as frequent traveller or billing address do not constitute obligatory information to be supplied about a passenger. It means that a passenger that supplies it runs more probability of being subject to scrutiny. Also, information on travel agencies is not as reliable as the majority of reservations are made through Internet. As pointed out by Brouwer, PNR data "are less reliable, being dependent on what the traveller submitted him- or herself when making a reservation. In addition, as has been pointed out by the Association of European Airlines, with respect to the identification of passengers the PNR data are not always consistent with the persons actually on board the air carrier."[767]

Some other categories of information that have to be transmitted to PIU also raise questions of their necessity, for example providing an e-mail address or telephone number. What advantage can a person's telephone number or e-mail offer for risk assessment? It can be useful only in cases of coincidence with a number or email already discovered in another investigation. But by putting together such information, it is impossible, without previously informing PIU of such a number or e-mail. But in such cases it will not be PNR analysis on that basis, or risk criteria, but a precise information search.

However, already mentioned, after the terrorist attacks in France, there is a high probability of agreement on the EU PNR mechanism. Thus if it is not unavoidable, and in any case it means limitations of fundamental rights, at least it has to be well balanced.

---

[766] Council document 9422/1/15.

[767] BROUWER, Evelien, "Ignoring Decent and Legality. The EU's proposal to share the personal information of all passengers" (Paper, Centre for European Policy Studies, June 2011), p. 3, accessed July 14, 2015, http://aei.pitt.edu/32073/1/No_40_Brouwer_on_PNR_Directive.pdf.

In 2014 the FRA issued "twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data" which points out the twelve elements needed to create a proper European PNR system.[768] This document basically reflects its opinion issued in 2011. As one of the elements is emphasised: foreseeing a clear definition of terrorism and serious crime that should be made with reference to:

- The Council Framework Decision 2002/475/JHA of 13th June 2002 on combating terrorism; [769]
- Europol Decision:
- Rome Statute of the International Criminal Court.

Even presuming that the scope of the Commission's Proposal on PNR would be reduced, and it would be used only for individual cases, uncertainties remain about the data assessment criteria that, according to Article 4(3) shall be established by PIUs with cooperation with national competent authorities. As the EDPS indicates, "The development of such a system on a European scale, involving the collection of data on all passengers and the taking of decisions on the basis of unknown and evolving assessment criteria, raises serious transparency and proportionality issues."[770]

In addition, it is not clear whether such criteria have to be established by all PIUs as general ones and applicable at EU level or if it is left to each PIU. In the first case, no mechanism of PIUs meetings or decision making process is foreseen. For example; Should PIUs meetings mean meetings of their chiefs? What should the voting procedure be (unanimity, qualified, absolute or simple majority)? Any term for reviewing established criteria? The second case would mean different use of PNR systems in Member States that is contrary to equality, non-discrimination and

[768] 1. Use PNR data only to combat terrorism and serious transnational crimes.
2. Limit access to the PNR database to a specialised unit.
3. Do not request direct access to airlines' databases.
4. Delete sensitive PNR data.
5. Set strict security and traceability safeguards against abuse.
6. Reduce the likelihood of flagging false positives.
7. Be transparent towards passengers.
8. Allow persons to access and rectify their PNR data.
9. Do not permit identification of data subjects or retention of data for longer than necessary.
10. Transfer data extracted from PNR only to competent national public authorities.
11. Only transfer data extracted from PNR to third countries under strict conditions.
12. Carry out objective and transparent evaluation of the PNR system.
See EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, "Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data", p. 2, accessed September 4, 2015, http://fra.europa.eu/sites/default/files/fra-2014-fundamental-rights-considerations-pnr-data-en.pdf.

[769] OJ L 164, 22.6.2002, p. 3-7.

[770] EUROPEAN DATA PROTECTION SUPERVISOR, "Opinion of the European Data Protection…" (2011), loc. cit., p. 26.

difficulties in the control of legality and the proportionality of use of PNR. For example, the same person traveling from Brazil to Spain or from Brazil to Germany would be the object of an application of different risk assessment criteria, even if his or her PNR data was be the same (except itinerary) in both cases. From the opinion of Brouwer, it can be assumed that the Commission's Proposal talks about the second option as "the PNR proposal allows variations among the member states with regard to the assessments carried out on passenger data, the use and new creation of "pre-determined criteria" for the PNR assessments."[771]

What could be done in this situation is the establishment of criteria by already existing formats for police co-operation; this could be Europol's Management Board or the Standing Committee on Operational Cooperation on Internal Security. These high level formats are proposed because of the sensitivity of the issue with respect to human rights.

Article 7 of the Commission's Proposal on PNR establishing information exchange is also criticised due to its ambiguity and lack of clarity. As a general rule, information requests and exchanges have to take place through the PIU's of Member States. Information can be provided without any request when it is considered necessary "for the prevention, detection, investigation or prosecution of terrorist offences or serious crime."[772]

In case of requests, the purpose is almost the same, but for a "specific case". This is understandable as requests for the purpose mentioned above would, in general, be disproportionate l and have s to be linked to a specific case under consideration of PIU or the competent authorities.

The real confusion appears in the regulation of exceptions where different terms such as "exceptional circumstances", "specific and actual threat" and "immediate and serious threat" are used without specification of their content.

What should be done in this respect is to clarify or unify the conditions for information exchange.

3.3. Agreements between the European Union and third states on PNR

After the terrorist attack of September 2001 in the United States, the national legislation of some countries was supplemented by provisions that put an obligation on air carriers flying to, from or through their territory, to provide their

[771] BROUWER, Evelien, "Ignoring Dissent and Legality…", loc. cit., p. 5.
[772] COM(2011) 32 final, p. 24.

competent authorities with access to PNR for law enforcement purposes. Thus the Aviation and Transportation Security Act from 19th November 2001 established that not providing of PNR data would mean a fine of $ 6000 per passenger or the loss of landing rights in territory belonging to the USA.

Under these circumstances, air carriers had two options: to agree with such an obligation or, not to operate flights in those countries, and as a result to see a decrease in their profits and competition capabilities. Consequently, a lot of air carriers have fulfilled this obligation.[773]

Bearing this in mind, and not too many other options, the Commission and the Council decided to sign the agreement with these countries to regulate this data flows, at least to some extent. As noticed by Heisenberg, "Power disparities had forced the EU to accede to an agreement that did not reflect many of its fundamental demands. Even the language of negotiation was brusque on the US side."[774]

This received a lot of reasonable criticism, as a step back from the protection of privacy and data, but looking at it from another angle, it was the best of the worst options, because laws adopted by third states would be applied anyway, both to carriers and all passengers, including EU citizens.

The first agreement on PNR was concluded with the United States of America in 2004 by approval of:

- Council Decision 2004/496/EC of 17th May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection,[775]
- Commission Decision 2004/535/EC of 14th May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection.[776]

[773] See more CATALINA BENAVENTE, María Ángeles, "La transmisión de datos PNR entre la Unión Europea, Estados Unidos, Canadá y Australia" in COLOMER HERNÁNDEZ, Ignacio and OUBIÑA BARBOLLA; Sabela, *La transmisión de datos personales...,* op. cit., p. 306-307.

[774] HEISENBERG, Dorothee, *Negotiating Privacy: the European Union, the United States and personal data protection* (London: Lynne Rienner Publishers, Inc., 2005), p. 141.

[775] OJ L 183, 20.5.2004, p. 83. Corrigendum at OJ L 255, 30.9.2005, p. 168.

[776] OJ L 235, 6.7.2004, p. 11.

Both acts were annulled by the European Court of Justice due to the lack of Communities' competence in this field,[777] but the application of the latter Commission Decision was maintained until 30th September 2006. In the judgment of 30th May 2006, in joint Cases C-317/04 and C-318/04 brought by the European Parliament it was stated that:

- Even if primary PNR collection is made by private operators and air carriers' activities fall within the scope of Community law, the purpose of agreement is public security that which is outside of the Community competence and the Commission could not base its Decision in Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995, on the protection of individuals, with regard to the processing of personal data, and on the free movement of such data that is applicable to the First Pillar.
- As the purpose of the agreement and use of PNR is public security, the Council incorrectly based its Decision in Article 95 of the Treaty Establishing the European Community that is devoted to the establishment and functioning of the internal market.

Thus the problem was related to data the processing purpose (security), different from the original purpose of its collection (commercial).

In 2006, a provisional 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,[778] was signed and in 2007[779] replaced by another provisional agreement, finally substituted by the permanent version in 2012.[780]

In the context of the judgment of the European Court of Justice in Case C-362/14 that recognised Decision 2000/520/EC as invalid and in a such way disclaiming evaluation of data protection level in United States as adequate the future of the PNR agreement and other data transmission mechanisms is under the question mark.

[777] In the case of the Commission's Decision, the European Parliament pleaded ultra vires to Directive 95/46/EC breach of its fundamental principles, breach of fundamental rights and principle of proportionality. For annulment of the Council's Decision it pleaded incorrect choice of Article 95 of the Treaty establishing European Community for its decision, breach of its Article 300(3), Article 8 of the ECHR, principle of proportionality and statement of reasons and principle of co-operation in good faith. Nevertheless, conforming ultra vires and incorrect choice of Article 95 the European Court of Justice did not analyse other pleas.

[778] OJ L 298, 27.10.2006, p. 27–31.

[779] OJ L 204, 4.8.2007, p. 16–25.

[780] OJ L 215, 11.8.2012, p. 4–14.

In 2012, the new 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 also entered into force.[781]

On 25th June 2014, a new Agreement between Canada and the European Union on the transfer and processing of Passenger Name Records was signed but still needs the approval of the European Parliament in order to enter into force. Nevertheless, the European Parliament, before final voting, asked for the preliminary opinion of the European Court of Justice on its compatibility with the EU Charter.[782]

These agreements are based on Communication from the Commission on the global approach to transfers of Passenger Name Records (PNR) data to third countries: the key objective of this communication is to establish, for the first time, a set of general criteria which should form the basis of future negotiations on PNR agreements with third countries[783] that, in 2010, decided to establish common criteria and negotiable areas concluding new agreements on PNR:

- Limitation of the use of data: fight against terrorism and serious transnational crime, clearly established key notions of these crimes.
- Scope of data: minimum, proportionate and with an exhaustive list of categories.
- Sensitive data: not used, only well-defined exceptions with appropriate safeguards and authorization of higher authority are possible.
- Data Security: appropriate legal, technical and organisational guarantees in place.
- Supervision: by independent data protection authority.
- Transparency, access, rectification, deletion, redress: information about gathering and use of PNR, access right with rectification, deletion and redress.
- Data retention: no longer than necessary for the established purpose.
- Onward transfer to other authorities or third countries: on a case-by-case basis to the third country that provides with the same data protection level as foreseen in the agreement.

[781] OJ L 186, 14.7.2012, p. 4-16.

[782] See EUROPEAN PARLIAMENT. "Resolution of 25 November 2014 on seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data. Available at European Parliament resolution of 25 November 2014 on seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data", accessed September 6, 205, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2014-0058+0+DOC+XML+V0//EN

[783] COM(2010) 492 final, p. 3.

– Restrictions on onward transfers to other government authorities: on a case-by-case basis, only purposes established in agreement and with guarantees to apply the same protection level.[784]

Of course, depending on the third state involved, the results of negotiations could differ, but either way, all negotiable agreements have the same pattern and equal primary position of the EU.

The table below presents comparisons of the main provisions of three concluded agreements; even if the entrance into force of the agreement with Canada is still under the question mark.

	USA	**Australia**	**Canada**
Method used to transmit PNR data from air carries	Push	Push	Push
Use of PNR	Prevention, detection, investigation and prosecution of: - Terrorism and related crimes, - Other transnational crimes punishable by three years of imprisonment at least. Also may be used: - Case-by-case for the protection of vital interests of any individual (when there is obvious threat) or in case of court order. - To identify persons subject to closer examination upon arrival to or departure the US.	Prevention, detection, investigation and prosecution of: - Terrorism, - Serious transnational crime. Also may be used: - To protect the vital interests of any individual (with not exhaustive list that includes risk of death, serious injury or threat to health), - To supervise misuse of data on a case-by-case basis foreseen by Australian law.	Prevention, detection, investigation and prosecution of: - Terrorism, - Serious transnational crime. Also may be used: - To protect the vital interests of any individual (with not exhaustive list that includes risk of death, serious injury or threat to health, public health risk), - To supervise accountability of the public administration, - To fulfil court order.
Sensitive data	Use on a case-by-case basis with the approval of Department of Homeland Security senior manager in case of danger to life of an individual. As a general rule is	Prohibition of use and processing. Deletion once received.	Masked, not further processed. Exception: use not by automatic systems, but by specifically authorised official on a case-by-case basis with

[784] Ibid, p. 9-10.

	USA	**Australia**	**Canada**
	deleted after 30 days from the last receipt.		the approval of Head of the Canadian Competent Authority in case of danger to life of an individual. As a general rule it is deleted after 15 days from the last receipt.
Decision taken on PNR basis	No decision of significant adverse action based only on PNR.	No decision of significant adverse action based only on PNR. No automated processing based on sensitive data.	No decision of significant adverse action based only on PNR.
Data retention	Active period: 5 years, depersonalisation and masking after 6 months. Dormant database: 10 years.	5.5 years: years 0-3 all data, years 3-5,5 masking out personal data.	5 years: after 30 days masking out names, after 2 years masking out other personal data.
Domestic sharing	With governmental authorities only for the purpose foreseen in the agreement and to support investigation or examination, following internal laws and agreements on information exchange and ensuring the same or comparable safeguards.	With governmental authorities only for the purpose foreseen in the agreement, ensuring the same or comparable safeguards. If it is not depersonalised, only on a case-by-case basis. Before sharing the Australian Customs and Border Protection Service assesses the relevance sharing and its scope (minimum data). Further sharing by the receiving authority is prohibited without the permission of the Australian Customs and Border Protection Service.	On a case-by-case basis minimum data with governmental authorities whose functions are related to a purpose of the agreement and only for these purposes, ensuring the same or comparable safeguards. Further sharing by the receiving authority is prohibited I without the permission of the Canadian Competent Authority.
Onward transfer	Following the conditions of the agreement in support of those cases under examination or investigation and informing Member State if information shared is about its citizen or resident. If it is not an urgent case	On case-by-case basis only to authority directly involved in prevention, detection, investigation and prosecution of terrorism and serious international crime for these purposes and that ensures the same safeguards. Before sharing the Australian Customs and	Minimum data on case-by-case basis for the purpose foreseen in this agreement to authority that performs functions related to that purpose and that ensures the same safeguards as established in this

	USA	Australia	Canada
	and understanding agreement with proper safeguards is concluded between the US and the third state.	Border Protection Service assesses the relevance of sharing and its scope (minimum data). If information shared is about citizen or resident of Member State, this state is informed. If it is appropriate, the passenger is informed as well. The receiving state has to agree to delete data as soon as it is not necessary for the purpose that it has been transmitted and do not make any further transmission.	agreement or applied in the EU. If information shared is about a citizen of a Member State, this state is informed.
Supervision	Department Privacy Officers, The DHS Office of Inspector General, The Government Accountability Office, The US Congress.	Australian Information Commissioner	Not specified, just indicated as "an independent public authority".
In force	7 years with reviews and evaluations. Reports on review are presented to the European Parliament.	7 years with renewal for same periods, unless specific notification envisages a different solution.	7 years, automatic renewal for the same period unless specific notification envisages a different solution.

Table 21: Comparison of main provisions of EU agreements on PNR with USA, Australia and Canada.

From three agreements, the one with Australia has more safeguards and stricter rules on data use as established: prohibition of sensitive data, stricter rules on transferring to other national competent authorities and third countries, although the time of retention of personal data (without masking out) is longer than in other agreements.

The agreement with Canada has more flexible rules which are found on use, sensitive data, but stricter rules on transferring and retention than the agreement with United States.

3.4. As a summary

As third states had adopted laws obligating air carriers that operate flights to or from their country, to provide them with PNR data for public security reasons, it

seems that the European Union had no other choice but to conclude agreements with them in order not to harm the competition of European air carriers and to some extent, protect the data of travellers.

On the other hand, once having once established this agreement, the question arises, why not use it as well within the EU where stricter data protection rules can be ensured? It would be dishonest towards EU internal law enforcement authorities not to endow them with a new tool that the EU has already given to law enforcement authorities of some third states and is negotiating with others.

Thus the EU is in a trap from it which has to get out, in order to achieve maximum possible benefit.

Due to the fact that there is even a lack of proof that PNR data is indispensable for the fight against terrorism and serious crime (although its added value cannot be denied), and there is a collection of "everyday personal data"[785], most probably the Commission's Proposal on PNR will be adopted.

That would mean mass data processing and a disproportionate limitation of the right to privacy. Comparing personal data processing in existing systems and PNR, the differences will be immense: if SIS has 1 million new records annually, PNR will have 500 million. [786]

Nevertheless, the process of adoption seems to divert away from the IMS established practice, firstly to in order to evaluate the real need of the new instrument before its development.

4. Information Exchange Platform

In 2010, following the provision of the Stockholm Programme to make better use of existing information exchange tools, the Spanish Presidency of the Council proposed creation an Information Exchange Platform. The specificity of this proposal is not in the establishment of a new information exchange mechanisms or granting broader access to existing ones, but in the centralization of all of them in one platform, as, for the time being they "are disparate in every way, displaying major differences in their nature (e.g. Database, communications system, network of contact points), legal basis (e.g. International treaty, European legislation,

[785] MITSILEGAS, Valsamis, *EU Criminal Law*, op. cit., p. 279.
[786] See EUROPEAN PARLIAMENT, Directorate General for Internal Policies, "Developing an EU Internal Security…", loc. cit., p. 143.

bilateral agreement) scope (e.g. Terrorism, drug trafficking, organised crime, violence in sport), technical characteristics, etc."[787]

This initiative had been included as one of the measures of the implementation of IMS and has received approval for its development from all Member States and is in line with the strategic guidelines. In addition to Spain in the development of the project Bulgaria, Cyprus, Germany, Italy, Lithuania, Hungary, Poland, Slovakia and the Commission are participating.[788]

Proposed by the Spanish Presidency, the leadership of this action was taken by Europol that concluded that, "the establishment of the IXP will make it easier for end-users to benefit from the existing opportunities for cross-border law enforcement cooperation, while respecting the national and international processes in place."[789]

Initially it was proposed to develop at least three levels of platform:

- "Bookshop" that would contain basic information on all information exchange tools: legislation, manuals, guidelines, procedures, national contact lists and fact sheets, where necessary – national legislation, training materials, and so on. At this level the end-user would get a picture of all the possibilities of international cooperation.
- "Communications" meaning a secure e-mail system that could be used between all authorised users. Europol considered it has "huge advantages from a business perspective. It enables the user to go (in accordance with his access rights) to all relevant sources, tools and platforms."[790]
- "Queries" or "Gateways" to various databases according to existing access rules and without any type of interconnection of existing databases, if they are separated under current legislation. It was foreseen that large scale systems, such as SIS, VIS and EURODAC will not be integrated into the platform.[791] But Europol proposed at the last stage of the project, to integrate search functions across the SIS, Europol systems and Interpol databases, provided that the user in question is authorised to query these sources with a so-called *single sign-on*.[792] Such a proposal would be acceptable so far as access rules would remain the same, as it would mean only a technical solution to facilitate the daily work of the competent authorities.

[787] Council document 5281/10, p. 2
[788] Council document 13032/14, p. 4
[789] Council document, 11117/3/10, p. 5.
[790] Council document 7840/13, p. 6.
[791] See Council document 7819/13, p. 2.
[792] Council document 7840/13, p. 2, 7.

As there would be three levels of platform, three categories of users are distinguished:

- The general user (every law enforcement official) with access to non-restricted data, meaning open resources of "Bookshop",
- The law enforcement officials with access to "Bookshop" and other levels if he or she already has such authorisation,
- The international coordination staff that have access to all levels. But each access will depend on individual authorisations obtained previously, for example a person can be authorised to search in SIS, but not Europol's databases.

Bearing in mind the complexity of the project and the need for human and financial resources, a step by step approach is applied with a provision to finish the first stage (Bookshop) at the end of this year. The following term of development will depend on human and financial possibilities.

As Jones points out, "The idea that individual rights to privacy and data protection will be better safeguarded through the use of a single website in some ways makes sense, allowing as it does one route through which data protection authorities can monitor access and usage logs for each individual instrument. However, the technical hurdles that would need to be overcome in order for such a project to work –let alone to work securely– are vast."[793]

5. European Police Records Information System (EPRIS)

Following the initiative of the European Criminal Records Information System (ECRIS), in April 2007 during the Police Chiefs Task Force meeting, the German Presidency raised the idea of a European Police Records Information System that would allow access to databases run by police in performing their functions.

This initiative was taken on the agenda of different Council preparatory groups, but as to date, it has not resulted in a clear project. Some Member States were not totally convinced of its necessity, due to already existing mechanisms but finally, in the Stockholm Programme, the Commission was called to present a feasibility study in 2012.

[793] JONES, Chris, "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, September 2011), p. 31, accessed May 19 2015, http://www.statewatch.org/analyses/no-145-ecris-epris-ixp.pdf.

The Commission ordered a comprehensive study that was presented in October 2012 with the main conclusion-suggestion, "If the need for a more efficient exchange of police records related information is not fully addressed by the better use of the existing systems and tools in the course of three years, then a pilot project should be initiated with the aim to evaluate the technical feasibility and impact of a new, specific EPRIS system."[794]

In December 2012, the Commission in its Communication to the European Parliament and the Council, "Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)" recognised that at that moment creation of the EPRIS was unjustified.[795]

This discussion and decision seems to be quite complicated, as to start with, there is no single or approximate understanding of what a "police record" is.

Going back to the findings of a Study on possible ways to enhance efficiency in the exchange of police records between the Member States, by setting up a European Police Records Index System EPRIS (hereinafter – Feasibility Study) made with 27 Member States[796] only thirteen have a legal definition of "police record", the rest have only a functional one, or none at all.

For the sake of continuation of a Feasibility Study, it was suggested that *police record* should be understood as "any information available in the national register or registers recording data of competent authorities, for the prevention, detection, investigation and prosecution of criminal offences."[797]

In these circumstances, it is not clear at all what data and its categories would be accessible through EPRIS. Any at all? It would mean total disproportion and inequity as far as the data subject is concerned, as the police record of one Member State would include only suspects, and in another, any questioned person, witness and victims.

Thus without a clear and explicit definition of *police record*, a discussion cannot go forward as this is a key issue on which to take a decision of its necessity.

The Feasibility Study indicated that a majority of Member States would stick to inclusion of suspects and perpetrators. In this case, EPRIS would partially overlap with EIS and AWF and would have added value only in relation to those crimes that are out

[794] EUROPEAN COMMISSION. DG Home "Study on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European Police Records Index System EPRIS" (Final Report, 8 October 2012), p. 2-3, accessed June 3, 2014, http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/police-cooperation/general/docs/epris-final_report_en.pdf.

[795] COM(2012) 735 final, p. 9.

[796] At the time of the study, Croatia was not yet an EU Member State.

[797] EUROPEAN COMMISSION, DG Home, "Study on possible ways…", loc. cit., p. 38.

part of Europol's competence. But is it really worth establishing a new system for the remaining criminal offences? As was pointed out at an Expert Meeting on EPRIS, if it would be established, then the question of EIS's added value should be reconsidered.[798]

In the same Study, four technical solutions for EPRIS were proposed: no new system, decentralised (as in case of Prüm Decisions), semi-centralised, centralised system. Fourteen Member States have pronounced in favour of a semi-centralised system that would mean that all data would remain in Member States' data bases, but at central level, would be in index data bases.[799] That would allow optimising query, i.e. To make a single one to all Member States, and not one by one as in the case of a decentralised system. From a technical point of view, it is a complicated structure, as Member States will need to create an index system or interface and to ensure its compliance with the central one. Additionally, maintenance of the central system will be needed.

According to a very preliminary estimation, the interface at central level would cost 2,000,000 euros and the connection of national databases and data extraction from 250,000 to 1,000,000 euros for each Member State, depending on its size.[800]

As the current situation shows, there is no agreement about the content of the central system, should in include only indexes or some basic data categories as well?

In the first case, the added value of such a system can be questioned. Only two advantages of it can be identified: the single query to all Member States and the work burden for requesting Member States.

France and Finland expressed the same idea in their joint document from 2012, "It is estimated that currently 65% of the requests are not replied to at all and only 35 % get a positive or negative answer [...] However, if it is proven that information on the person in question is available from a law enforcement authority in certain Member States, a well-directed request would be made. It is most likely that a positive answer would be given to these requests and that in this respect the activities in all Member States concerned would have been worthwhile."[801]

But after the automatic index query, personal data would be received on the basis of already existing Swedish Initiative as is the case with DNA and dactyloscopic

[798] See EUROPEAN COMMISSION, DG Home, "Summary Report of Expert Meeting on EPRIS, 19.04.2012", p. 6, accessed June 3, 2014, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=6238&no=1.

[799] EUROPEAN COMMISSION, DG Home, "Study on possible ways…", loc. cit., p. 28-29.

[800] See EUROPEAN COMMISSION, DG Home, "Summary Report of Expert…", loc. cit., p. 5.

[801] Council document 14944/12, p. 3.

data under the Prüm Decisions. It raises a question of proportionality of creation of such a system to its practical efficiency.

In the second case a concern would be about the new legal basis and data protection. Including real data into central system, Member States would have to agree what categories of data would be included, who would be responsible for data security, deletion, and so on. This brings us to the question: what is the ratio between results that will be achieved in the fight against crime and the necessity and proportionality to limit privacy and data protection?

Although one can argue that creation of EPRIS will not mean gathering different data from an already available one, but harmonisation or at least approximation of the definition of "police record" could force some Member States to collect new categories of data. Without definition of the term *police record* again, data that could be accessed by different Member States could vary a lot. It should also be borne in mind that national information of police interest is not usually centralized and different law enforcement institutions have different access rights and their own databases.[802]

In both cases it is not clear what would be the search criteria, for instance: name and surname? ID Number? Any other criteria?

In comparison with other initiatives, although it would much less intrusive as the initiative on PNR, it also lacks added value that would compensate for other limitations of fundamental rights and the costs of its implementation.

Besides, until now nobody has declared the impossibility of obtaining this information. Under current legal and technical solutions such information can be queried on the basis of the Swedish Initiative and using SIENA, or any other co-operation channel. It is true that the requesting Member State would have to ask all Member States separately, but from a technical point of view, it does not mean sending 27 separate requests, just to use one channel and send it with one mailing list as is done with other requests.

But the solution of co-operation gaps or inefficiency cannot be solved every time by the creation of a new database and spreading access rights. These problems have other solutions from addressing them in proper meetings, or finally, as a last case scenario, filing a case to the European Court of Justice for non-fulfilment of obligations foreseen in EU law.

Although for the time being no clear statement on insufficiency of actual information exchange mechanisms has been made, in April 2015, the Commission

[802] See DEL MORAL TORRES, Anselmo, *Cooperación policial en la Unión…,* op. cit., p. 495.

committed itself to supporting the pilot project where a group of Member States would create national index systems and give access to other participating Member States for automated searches on a "hit / no hit" basis.[803]

[803] COM(2015) 185 final, p. 8.

CONCLUSIONS

The security of modern society is threatened by such direct threats as terrorism, and indirectly by the spill over of technological progress and facilitated cross-border movement that have resulted in moving criminality into virtual space, and easier meeting in the international environment.

This challenged a need for approximation of *ius puniendi,* to free movement as well, and to change to some extent, general perception of the limits of competence of law enforcement and judicial authorities, although their functions generally were treated as an indispensable element of state sovereignty.

With respect to information exchange between law enforcement authorities for the purposes of investigation, the EU took this topic onto its agenda very actively, firstly by the establishment of compensatory mechanisms for the abolition of control of internal borders, and later by opposing to intensified criminal mobility and increased terrorism threats.

In these endeavours to protect persons, ensure their safe movement and stay in the EU, different initiatives saw daylight. Mechanisms analysed in this work allow the conclusion that the provenance of initiatives in this area, and the "engine" of their promotion is Germany, with political ideas to approximate co-operation to the functioning of the federal model of police forces. Nevertheless, it faces a cautious position from some Member States who do not oppose to co-operation as such, but pronounce for its moderate development and use.

Many (but not all) legislative acts on information exchange were created in an atmosphere that mixes political obligation with reaction to some threat, rapid preparation of legislative draft, political and time pressure for its analysis, necessity to conciliate different and sometimes contrary positions of Member States. That resulted in some deficiencies outlined below.

1. Conclusions about the regulation of each information exchange instrument that has been analysed

Each analysed instrument has its advantages and problems, but in the light of effectiveness, precision of regulation and balance with human rights some are more successful than others. Thus:

- SIS II (and previously SIS) is a data base that includes quite precisely defined categories of persons and objects. Being a centralised data base it allows: quite comprehensive access control as each search (check) has to be logged, automated data deletion after the term of storage expires (if no actions on extension of storage has been taken) and avoidance of storage of excessive information, collection of precise statistics.

  A comprehensive *lex especialis* on data protection is applied to SIS II, including the establishment and functioning of supervising authorities.

  Nevertheless, the regulation of actions on alerts on discreet or specific checks as well as Europol's and Eurojust's access to SIS are not precisely regulated, leaving possibilities to redundant intervention into a checked person's privacy in the first case, and overuse of search possibilities in the second.

- PCCC is an entity used as a general rule for the investigation of crimes in states' border areas. It is does not have detailed regulation at EU level, leaving it to neighbouring Member States' that establish such PCCC on their borders.

  That results in a lack of common provisions on the working scheme and on the control of data flows. On the other hand, it can be justified by the peculiarity of each EU region that provokes difficulties in establishing the same framework across the EU.

- EU regulation of liaison officers is also quite general. The two most important provisions concern the common use of the liaison officers posted abroad and prohibition to perform operational activities on the territory of a hosting country. Information exchange takes place within the limits of national law of the hosting country and of the competence of the liaison officer established by its national law. From the perspective of the dispositive nature of this instrument (Member State has freedom to post liaison officers abroad or not) and bearing in mind differences of bilateral

relations that can result in more restrictive or more flexible regulation, it would be difficult, as in the case of PCCC established EU level detailed rules. Nevertheless, due to the lack of general lines about competence, it is not clear to what extent a hosting country can limit it and make the figure of liaison officer ineffective.

- Europol is comprehensively regulated by EU legislation, with a quite precise definition of purpose of information exchange between Europol and Member States. Nevertheless, it gives unlimited flexibility to Member States to use their liaison officers posted in Europol and SIENA for other information exchange between Member States that is outside of Europol's mandate.

  Despite comprehensive rules on data protection, the biggest criticism is reserved for the transmission of personal data to third parties as an exception, when Europol does not have operational agreements. Regulation of onwards information transmission is even more fragmented as it has different regulations depending on the agreement concluded between Europol and the third party and in addition, exceptions to make such transmission without concluded agreement were also allowed.

- The Swedish Initiative that sets out to be a flagship of the implementation of the principle of availability, in the end merely has added value by the establishment of deadlines for reply. But even in this respect, it does not provide the content of urgency.

  It is full of question marks and ambiguities, beginning with the lack of a clear definition of the purpose for which information can be exchanged, and finishing with the complicated request form that discourages competent authorities to use it as a legal basis for requests, and limits use of this instrument only to cases of urgency.

- Despite being brief, the regulation of FIUs and AROs is quite clear with a well-defined but narrow purpose as well as a limited list of authorities that participate in information exchange. Nevertheless, with respect to data protection rules, reference to different legal acts is confusing to competent authorities and makes the effectiveness of data protection difficult.
- As compensation for giving direct access to national data bases, Prüm Decisions foresee quite extensive guarantees to their proper use, such as evaluation of each Member State before authorising access of its national contact points. By giving hit / no hit access, it is ensured that data not matching search criteria will never be seen by the searching authority and in cases of hit, personal data will be provided only after proper checks of

the basis of the request. Nevertheless, having 28 separate data bases in case of DNA for the moment, it is impossible to gather coherent statistics.

Provisions of non-automated data exchange on terrorism prevention and security of major events with a cross-border dimension are redundant, due to the existence of other legislative tools.

On this basis, as a general conclusion, it can be said that despite some disadvantages, the best regulated option is SIS II. It is merited by both the European legislator and the nature of the tool itself, as a centralised data base (despite its expense) its equivalent use across all countries, equal control and supervision of data protection requirements is ensured.

Giving access to national data bases on a hit / no hit basis also results in the establishment of quite high standards of their use, as each Member State seeks the best possible protection of its data base.

2. Conclusions about clarity on use of totality of the EU information exchange tools

The analysis carried out has revealed that the EU pool of information exchange mechanisms is fragmented and incoherent. As a summary, it is presented in the following tables which show the purpose of each tool, data subject and data categories included, with special mention of sensitive data, possibilities of transmission to third parties or forwarding, and the data protection regime applied.

	PURPOSE
CISA	**SIS** - General: To ensure a high level of security in the territories of the Member States. - Special: Each category of alert has its own purpose depending on category of person or object. **PCCC** Individually established by bilateral or multilateral agreements. As a general rule should: - include prevention, detection, investigation and prosecution of petty crime committed at border area, - not interfere with the competence of central information exchange units. **Liaison Officers** Individually established by bilateral or multilateral agreements or on the basis of the national law of hosting country and competence of liaison officer established.
Europol	Prevention and combatting of organised crime, terrorism and other forms of serious crime affecting two or more Member States.
Swedish Initiative	As it is not defined unambiguously, the broader provision is Detection, prevention or investigation of offences. Use for other purposes it has to be authorised by requested the Member State and envisaged by the national law of the receiving one.
FIUs and AROs	**FIUs** Money laundering and financing of terrorism. **AROs** Tracing and identification of crime related property for its further freezing, seizure or confiscation.
Prüm Decisions	- DNA databases: investigation of criminal offence. - Dactyloscopic databases: prevention and investigation of criminal offences. - Vehicle registration data: prevention and investigation of criminal offences, other offences under the jurisdiction of the courts or the public prosecution service of the searching Member State and for the maintenance of public security. - Non-automated data exchange: prevention of terrorism, prevention and security of major events with a cross-border dimension.

Table 22: Purpose of information exchange within the analysed information exchange tools.

	DATA SUBJECT
CISA	**SIS** - Wanted for surrender, i.e. Prosecuted or convicted; - Missing or in need of special protection due to their physical or mental conditions; - Sought for assistance in judicial procedure; - Needed to be checked; - Not allowed to enter one of the members of the Schengen zone; - Persons whose identity is misused (with previous consent). **PCCC** Depends on bilateral and multilateral agreements. **Liaison Officers** Depends on bilateral and multilateral agreements and national law of sending and hosting countries.
Europol	**EIS** - Persons suspected of already committed a crime, being accomplices or, of its future commission when crime is subject to Europol's competence; - Convicted persons. **AWF** - Persons suspected of already having committed a crime, being accomplices, or of its future commission when crime is subject to Europol's competence; - Convicted persons; - Witnesses; - Victims; - Contacts and associates of suspects; - Informers.
Swedish Initiative	Not specified.
FIUs and AROs	Not directly specified, but a conclusion can be made that they are natural, legal persons involved in money laundering or terrorism financing.
Prüm Decisions	Subject to national legislation.

Table 23: Data subjects whose information exchange within the analysed information exchange tools.

DATA CATEGORIES

CISA	**SIS** - Surname and forenames, any aliases possibly entered separately; - Any specific, objective physical characteristics not subject to change; - First letter of second forename; - Date and place of birth; - Sex; - Nationality; - Whether the persons concerned are armed and/or violent; - Reason for the alert; - Action to be taken; - Photographs; - Fingerprints; - Authority issuing the alert; - A reference to the decision giving rise to the alert; - Links to or alerts in SIS II; - The type of offence. **PCCC** Depend on bilateral and multilateral agreements. **Liaison Officers** Depends on bilateral and multilateral agreements and the national law of the sending and hosting countries.
Europol	**EIS** - Surname, maiden name, given names, alias, assumed name; - Date and place of birth; - Nationality; - Sex; - Where necessary other characteristics likely to assist in identification as dactyloscopic data and DNA profiles; - Place of residence and whereabouts; - Profession; - Social security numbers; - Driving licences; - Identification documents. **AWF** General to all data subjects: - Present and former surnames (i.e. Real and alias, nickname, residence, nationality, parents (if it necessary, etc.); - Physical description; - Identification means (i.e. Documents, ID and other official numbers, images, fingerprints and DNA profiles, etc.). Additional data categories: Differ depending to data subject and are provided in the Table 15.
Swedish Initiative	Any type of information or data which is held by law enforcement authorities.

FIUs and AROs	**FIUs** Any available information useful for FIU for analysis and investigation of money laundering and financing of terrorism. **AROs** Any information considered necessary for the execution of the tasks of another ARO.
Prüm Decisions	- Data related to personal characteristics such as DNA and dactyloscopics; - Vehicles' registration data; - All data important in prevention of terrorism; - All data important in prevention of offences and threats to the security in major events with a cross-border dimension.

Table 24: Data categories that can be exchanged within the analysed information exchange tools.

SENSITIVE DATA

CISA	**SIS** Transmission prohibited **PCCC** Depends on bilateral and multilateral agreements. **Liaison Officers** Depends on bilateral and multilateral agreements and national law of sending and hosting countries.
Europol	**AWF** Permitted if it is strictly necessary for the purposes of the file concerned, and unless such data supplements other personal data already input in that file.
Swedish Initiative	Not specified.
FIUs and AROs	Not specified, but by the nature of purpose, not very relevant.
Prüm Decisions	Does not occur in automated data search, because in cases of dactyloscopic or vehicle registration, data is not collected and in cases of DNA non-coding part of DNA is used that allows identification of sex, but not any other sensitive data. Nevertheless it is not specified for non-automated data exchange and data transmission after hit.

Table 25: Possibilities to exchange sensitive data within the analysed information exchange tools.

ACCESSING AUTHORITIES

CISA	**SIS** - Police; - State Border Guards; - Customs; - Vehicle registration entities; - Europol and Eurojust (access limited to alerts related to their mandate); - When it is allowed by the national legislation, also judicial authorities participating an in investigation and their coordinators can be granted an access. **PCCC** As a general rule, police and customs authorities or other authorities performing their functions (i.e. State Border Guard). **Liaison Officers** Not defined, depends on bilateral and multilateral agreements and the national law of sending and hosting countries.
Europol	**EIS** - Duly empowered Europol staff (including the Director and his Deputies); - Liaison officers; - ENUs. - Member States can decide to give an access to EIS to other competent authorities, but it will be limited to the possibility of verifying whether requested information exists (hit / no hit). **AWF** Participants of AWF after Europol's accreditation and special training. The Director, his or her Deputies, Europol staff, liaison officers and ENUs that do not participate in AWF are authorised to access only index of the AWF and make a search on hit / no hit basis.
Swedish Initiative	- Police; - Customs; - Other authorities that are authorised by national Law to detect, prevent and investigate offences or criminal activities.
FIUs and AROs	**FIUs** - FIUs; - Other authorities combating money laundering. **AROs** - AROs; - Other authorities with the competence of tracing and identification of property obtained as a result of crime.
Prüm Decisions	At the stage of automated comparison: - National contact points designated by each State. At the stage or receiving data related to automated matches: - Firstly, is available to national contact point that lately is transmitted to the authority that has requested a comparison. In case of non-automated data exchange: - Network of contact points for each for each category of data (terrorism, public order and security).

	- National contact points make further transmission of data to requesting authority or in case of spontaneous data supply – to the authority that can be interested in it.

Table 26: Authorities that have access to information within the analysed information exchange tools.

DATA PROTECTION REGIME

CISA	**SIS** Lex generalis: - For all alerts except on persons not allowed to enter the Schengen zone – European Convention on Data Protection. - For alerts on persons not allowed to enter the Schengen zone - Directive 95/46/EC and Regulation 45/2001. Lex especialis: - Decision 2007/533/JHA and Regulation 1987/2006. **PCCC** - Lex generalis: Framework Decision 2008/977/JHA. - Lex especialis: provisions of bilateral or multilateral agreements if applicable and national law of sending and hosting country. **Liaison Officers** - Lex generalis: Framework Decision 2008/977/JHA. - Lex especialis: provisions of bilateral or multilateral agreements if applicable and national law of sending and hosting country.
Europol	Individual set of provisions established by Europol Decision and other complementary decisions.
Swedish Initiative	- *Lex generalis*: European Convention on Data Protection, its Protocol, Recommendation (87) 15, Framework Decision 2008/977/JHA and national law. - *Lex especialis:* rules applied to data transmission channel.
FIUs and AROs	**FIUs** - European Convention on Data Protection, its Protocol and Recommendation R(87) 15. - For AML/CFT: Directive 95/46/EC and Regulation 45/2001. **AROs** - European Convention on Data Protection, its Protocol, Recommendation R(87) 15 as well as to national data protection rules of Member States. - Also rules applied to Swedish Initiative (as it serves as the basis for information exchange).
Prüm Decisions	Lex especialis: Decision 2008/615/JHA and national law.

Table 27: Data protection regulation within the analysed information exchange tools.

TRANSMISSION TO THIRD PARTIES	
CISA	**SIS** Not permitted. Foreseen exception of data submission to the Interpol database on stolen or missing travel documents is not applied. **PCCC** Depends on bilateral or multilateral agreements. **Liaison Officers** Depends on bilateral or multilateral agreements of sending and hosting Member States.
Europol	Allowed on the basis of agreement between Europol and Third party with the consent of the Member State that has provided information. In certain circumstances (defined by the law) data transmission is possible without afore mentioned agreement.
Swedish Initiative	Not foreseen.
FIUs and AROs	Not foreseen.
Prüm Decisions	Not foreseen.

Table 28: Possibility to transmit information to third countries within the analysed information exchange tools.

ONWARD TRANSMISSION, USE FOR OTHER PURPOSES	
CISA	**SIS** Use for other purposes is possible only to prevent serious threats to public policy or security, to national security or to prevent serious crimes. In such cases consent from the Member State that has issued the alert has to be obtained. **PCCC** Depends on bilateral or multilateral agreements that can permit so called "chain requests". **Liaison Officers** Information related to serious criminal threats can be requested on behalf of other Member States or Europol that do not have their liaison officers in that country.
Europol	Depends on provisions of agreement between Europol and third party. In certain circumstances (defined by the law) data transmission is possible without afore mentioned agreement.
Swedish Initiative	Not foreseen.
FIUs and AROs	Not foreseen.
Prüm Decisions	Not foreseen.

Table 29: Possibilities of onward transmission and other use of information within the analysed information exchange tools.

This comparison brings us to the conclusion that law enforcement authorities as a rule, face dilemmas in which tools should be used; as for the same purpose to obtain information related to a committed robbery as when there are indications

of involvement of nationals or residents of other Member States, a choice between simple use of the Swedish Initiative, PCCC, a liaison officer posted in that country or Europol, shall be made. In those cases, when it would be a single (the first and the last) request, the choice maybe will not be so important because the information could probably be obtained using any tool, and the difference could be noticed only at the time of the response. But when the possibility of further requests exists, there is no warranty that further information could be obtained using the same tool or channel. For example, primary information was obtained on the basis of an automated search in a dactyloscopic data base; to get personal data, the Swedish Initiative was used; received information revealed a person's involvement in organised crime and after checking in the index system of AWF, a hit was received, the competent authority joined AWF, and further information was exchanged through Europol. Having all the pieces of data on one person received using different tools of law enforcement, an officer should be very careful taking decisions on possible onward transmission, transmission to a third party and use of sensitive data. And the most important question is which data protection regime has to be applied to data related to one investigation, but received using different information exchange tools, in order to ensure its further effective use by obeying the requirements of the due process.

Comparing all the above mentioned aspects of information exchange, deficiency of provisions of some mechanisms on sensitive data, and transmission to third parties and forwarding deserve special attention. Such a lack of clear regulation can easily result in violation of fundamental rights.

3. Proposals

As the main problem of the current information exchange tools is their overlapping and confusion at the time of their use, there is a need of revision of the whole data exchange *acquis* and of its consolidation. In those areas where consolidation is not possible, a more comprehensive handbook on information exchange than current one has to be elaborated. It should not be structured according to existing information exchange tools, but to data categories, for example instead of description of what can be obtained using SIS or EIS, an explanation about all possible mechanisms to obtain DNA related data or data related to terrorism should be given.

The general proposal for the future initiatives of information exchange would be maintance of coherence with the existing ones and when possible going back to abandoned provisions of Commission's proposal from 2005.

In respect to the data protection, the proposal totally coincides with the comments of the European Parliament, EDPS and FRA on the need for a single data protection regime for all exchanged data, as it is an indispensable condition in avoiding confusion on data protection regimes that have to be used on data received, using different information exchange mechanisms.

And finally the following improvements of the existing tools could be considered as contributing added value and quality to information exchange within EU:

- European ”information hub”, i.e. Europol, which should remain “European”, as far as possible, by the prohibition of personal data transmission to third parties with whom it does not have operational agreements. If it would significantly damage efforts to maintain security, only limited categories of personal data should be subject to such transmission, and in any case should not include transmission of sensitive data or data on victims and witnesses. Such data exchange could take place only between Member States that have submitted it to an AWF and a third party.
- Europol’s access to SIS II shall be limited only to the necessity to obtain information for AWF with the establishment of access of a limited number of staff and the possibility of the effective supervision of use of data by Europol.
- In order to avoid duplicity, provisions of Prüm Decisions on non-automated data exchange shall be merged with the relevant legislative acts, regulating the fight against terrorism and public security in relation to mass events of a transnational nature.
- With respect to liaison officers posted within the EU there should be EU level minimum requirements on the activities of liaison officers in order to avoid inequality in their actions, depending on the posting and hosting Member States, and allowing the possibility to establish by bilateral agreements with more favourable conditions to perform their functions.

BIBLIOGRAPHY

1. Scientific literature

ACED FÉLEZA, Emilio, "Principio de Disponibilidad y protección de datos en el ámbito policial". Noticias Jurídicas, April 1, 2010, accessed September 25, 2013, http://noticias.juridicas.com:8080/articulos/15-Derecho-Administrativo/322-principio-de-disponibilidad-y-proteccin-de-datos-en-el-mbito-policial-.html.

AGUILERA RUIZ, Luis. "La protección de datos de ADN en la Unión Europea y en España". In CABEZUDO BAJO, María José. *Las bases de datos policiales de ADN ¿Son una herramienta realmente eficaz en la lucha contra la criminalidad grave nacional y transfronteriza?* Madrid: Dykinson S.L., 2013, p. 27-42.

ALBRECHT, Hans-Jörg (translation GUERRERO PERALTA, Oscar Julián). *Criminalidad transnacional, comercio y lavado de dinero.* Bogota: Universidad externado de Colombia, 2001.

ALCOCEBA GIL, Juan Manuel. "Tratamiento y transmisión de datos genéticos con fines de la investigación penal en la UE". In COLOMER HERNÁNDEZ, Ignacio and OUBIÑA BARBOLLA, Sabela. *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea".* Navarra: Aranzadi, 2015, p. 609-652.

ALMAGRO NOSETE, José, CÓRTEZ DOMÍNGUEZ, Valentín, GIMENO SENDRA, Vicente, et al. *Derecho Procesal. Parte general proceso civil. (1).* Valencia, Tirant lo Blanch, 1989.

ALVARGONZÁLES SAN MARTÍN, Fernando, 2000. Hacia un nuevo escenario de cooperación en asuntos de justicia e interior. In Ministerio del Interior. *El espacio Europeo de libertad, seguridad y justicia*. Madrid: Secretaría General Técnica, 2000.

AMBOS, Kai. *Temas de Derecho Penal internacional y europeo.* Madrid: Marcial Pons, 2006.

AMICI, Victoria. "Europol et la nouvelle décision du Conseil: entre opportunités et contraintes". *Revue du Droit de L'union Européenne*. 2010(1), p. 77-100.

ANDERSON, Malcolm. Trust and Police Co-operation. In ANDERSEN, Malcolm and APAP, Joanna. *Police and Justice Co-operation and the New European Borders.* Kluwer Law International: The Hague, 2002, p. 35-46.

ARNÁIZ SERRANO, Amaya. Evolución de la Cooperación Judicial Penal Internacional: en especial, la Cooperación Judicial Penal en Europa. In CARMONA RUANO, Miguel, U. GONZÁLEZ VEGA, Ignacio and MORENO CATENA, Víctor. *Cooperación Judicial Penal en Europa.* Dykinson: Madrid, 2013, p. 1-40.

ARROYO ROMERO, Francisco Javier. *La influencia de EUROPOL en la comunitarización de la policía europea.* Madrid: Akal, 2006.

ASHIKMIN, Simon; BERDINE, Susan G.; MORRISSEY, Mitchel. R. Et al. "Effectiveness and Cost Efficiency of DNA Evidence in Volume Crime. Denver Colrado Site Summary", accessed April 24, 2014, http://www.denverda.org /DNA_Documents/dnaburgrcostefficiencyreserch1.pdf.

ASHWORTH, Mike, REDMAYNE, Mike. *The criminal Process.* 3rd ed. Oxford: Oxford University Press, 2005.

BALZACQ, Thierry, BIGO, Didier, CARRERA, Sergio, GUILD, Elspeth. "Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats". (Working Document no. 234, Centre for European Policy Studies, January 2006), accessed April 16, 2014, http://www.ceps.be/book /security-and-two-level-game-treaty-prüm-eu-and-management-threats

BANTEKAS Ilias, NASH Susan. *International Criminal Law*. 2nd ed. Coogee: Cavendish Publishing Limited, 2003.

BARONA VILAR, Silvia. *Seguridad, celeridad y justicial penal.* Valencia: Tirant lo Blanch, 2004.

BASSIOUNI, Cherif. *Introduction to International Criminal Law.* Ardsley, New York: Transnational Publisher, Inc, 2003.

BĄKOWSKI, Piotr; VORONOVA, Sofija. "The Proposed EU Passenger Name Records (PNR) Directive: Revived In The New Security Context." (Briefing,

European Parliamentary Research Service, April 2015), accessed July 14, 2015, http://www.europarl.europa.eu/EPRS/EPRS-Briefing-554215-The-EU-PNR-Proposal-FINAL.pdf.

BELLANOVA, Rocco. "The "Prüm Process": The Way Forward for EU Police Cooperation and Data Exchange?". In GUILD, Elspeth, GEYER, Florian. Geyer (eds.) *Security versus Justice? Police and Judicial Cooperation in the European Union*. Hampshire: Ashgate Publishing Limited, 2008, p. 203-221.

BENYON, John. Policing the European Union: The Changing Basis of Cooperation on Law Enforcement. *International Affairs (Royal Institute of International Affairs 1944-)*, July 1994, Vol. 70, No. 3, p. 499-517.

BERTOZZI, Stefano, "Schengen: Achievements and Challenges in Managing and Area Encompassing 3.6 million km^2 (Working document no. 284, Centre for European Policy Study, 2008), accessed October 2, 2013, http://papers.ssrn.com/sol3/papers.cfm?Abstract_id=1337624

BIGO, Didier; BRUGGEMAN Willy; BURGESS, Peter et al., "The principle of information availability", Challenge Liberty & Security, 2007, accessed January 26, 2013, http://www.libertysecurity.org/article1376.html.

BIONDO, Francesco. Emergencia y garantías (en el pensamiento jurídico de Luigi Ferrajoli). In MASFERRER, Aniceto. *Estado de Derecho y derechos fundamentales en la lucha contra el terrorismo.* Navarra: Aranzadi, 2011, p. 515-544.

BLASI CASAGRAN, Cristina. "El papel de Europol como actor normativo de la UE en el intercambio de datos con terceros estados". In PI LLORENS, Montserrat, ZAPATER DUQUE, Esther. *La dimensión exterior de las agencias del espacio de libertad, seguridad y justicia.* Madrid: Marcial Pons, 2014, p. 101-123.

BLOCK, Ludo. "Bilateral Police Liaison Officers: Practices and European Policy". *Journal of Contemporary European Research*, 2010. Vol. 6, issue 2, p. 196, accessed October 16, 2013, http://www.jcer.net/ojs/index.php/jcer/article/view/266/205.

BOEHM, Franziska. *Information Sharing and Data Protection in the Area of Freedom, security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU Level.* Verlag Berlin Heidelberg: Springer, 2012.

BOEHM, Franziska, D. COLE, Mark. "Data Retention after the Judgement of the Court of Justice of the European Union" (Study. Greens/EFA Group in the European Parliament, 2014), accessed September 17 2014, http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

BOERGER, Björn. "The transmission of personal data as part of the police and judicial cooperation in criminal matter in the EU: German experience". In COLOMER HERNÁNDEZ, Ignacio and OUBIÑA BARBOLLA, Sabela. *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea".* Navarra: Aranzadi, 2015, p. 187-214.

BONN, Marjorie. "EL Programa de La Haya. El espacio de Libertad, Seguridad y Justicia en la Unión Europea". In ARROYO ZAPATERO, Luis, NIETO MARTÍN, Adán. *El Derecho Penal de la Unión Europea. Situación actual y perspectivas de futuro.* Universidad de Castilla-La Mancha: Cuenca, 2007, p. 29-36.

BOSCH MOLINÉ, Alba. "La dimensión exterior de Europol desde el punto de vista de la protección de datos. El caso del acuerdo TFTP". In PI LLORENS, Montserrat and ZAPATER DUQUE, Esther. *La dimensión exterior de las agencias del espacio de libertad, seguridad y justicia.* Madrid: Marcial Pons, 2014, p. 125-160.

BROUWER, Evelien. "Ignoring Decent and Legality. The EU's proposal to share the personal information of all passengers". (Paper, Centre for European Policy Studies, June 2011), accessed July 14, 2015, http://aei.pitt.edu/32073/1/No_40_Brouwer_on_PNR_Directive.pdf.

BRUGGEMAN, Willy. "Los procesos de construcción de una inteligencia europea". In MONTERO, Julián, ROMERO, Francisco and VALIENTE, Elena. *¿Hacia una Policía Europea?* Madrid: Fundación Policía Española, 2002, p. 215 (215-226).

BRUGGEMAN, Willy. "Policing in a European Context". In APAP, Joanna. *Justice and Home Affairs in the EU. Liberty and Security Issues after Enlargement.* Cheltenjam: Edward Elgar Publishing Limited, 2004, p. 151-166.

BRUGGEMAN, Willy. "A Vision of Future Police Cooperation with Special Focus on Europol". In DE ZWAAN, Jaap W. And GOUDAPPEL, Flora A.N.J. *Freedom, security and Justice in the European Union: Implementation of The Hague Programme.* Asser Press: The Hague, 2006, p. 203-220.

BRUGGEMAN, Willy. "Europol and the Europol Drugs Unit: Their Problems and Potential for Development". In BIEBER, Roland; MONAR, Joerg. *Justice and Home Affairs in the European Union. The Development of the Third Pillar.* European Interuniversity Press: Brussels, 1995, p. 217-230.

BULMER. Simon. "Shop till you drop? The German executive as venue-shopper in Justice and Home Affairs". In ENDEL. Petra, ETTE, Andreas, PARKES, Roderick. *The Europeanization of Control. Venues and Outcomes of EU Justice and Home Affairs Cooperation.* Berlin: LIT Verlag, 2011, p. 41-76.

BUNYAN, Tony, "The "principle of availability", Statewatch, December 2006, , accessed January 26, 2013, http://www.google.es/url?Sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0cceqfjaa&url=http%3A%2F%2Fwww.statewatch.org%2Fanalyses%2Fno-59-p-of-a-art.pdf&ei=7Jm_vlbdmywuu9izgoap&usg=afqjcnfrlx_0fukec9zczwlutuivfablga&bvm=bv.83829542,d.d24.

BURES, Oldrich. "Europol's Fledging Counterterrorism Role". *Terrorism and Political Violence.* 2008, vol. 20 (4), p. 498-517.

BURGESS, Mark. "The Prüm Process: playing or abusing the system?". European Security Review, 2007, no. 34, accessed April 13, 2014, http://esdpmap.org/pdf/2007_artrel_17_esr34prum-process.pdf

CABEZUDO BAJO, María José. "La protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal". In DE LA OLIVA SANTOS, Andrés (dir.), AGUILERA MORALES, Marien and CUBILLO LÓPEZ, Ignacio (coord.). *La Justicia y la Carta de Derechos Fundamentales de la Unión Europea.* Madrid: COLEX, 2008, p. 327-342.

CALESINI, Giovanni. *European Police Law Handbook*. Roma: Laurus Robuffo, 2007.

CÁMARA VILLAR, Gregorio. "La garantía de los derechos fundamentales afectados por la Convención de Prüm". *Revista de Derecho Constitucional Europeo.* Enero-Junio 2007, no 7, p. 97-118.

CASSESE, Antionio. *International Criminal Law.* 2nd ed. New York: Oxford University Press, 2008.

CASTILLEJO MANZANARES, Raquel. "Europol y las investigaciones transfronterizas". *Dereito.* 2008, vol. 17-2, p. 91-104.

CATALINA BENAVENTE, María Ángeles. "La transmisión de datos PNR entre la Unión Europea, Estados Unidos, Canadá y Australia". In COLOMER

HERNÁNDEZ, Ignacio and OUBIÑA BARBOLLA, Sabela. *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea".* Navarra: Aranzadi, 2015, p. 301-356.

CRAWSHAW, Ralph, DEVLIN, Barry and WILLIAMSON, Tom. *Human Rights and Policing. Standards for Good Behaviour and a Strategy for Change.* Dordrecht: Kluwer Law International, 1998.

DE HERT, Paul. "Division of Competencies between National and European Levels with regards to Justice and Home Affairs". In APAP, Joanna. *Justice and Home Affairs in the EU.* Cheltenham: Edward Elgar, 2004.

DE HERT, Paul; PAPAKONSTANTINOU, Vagelis and RIEHLE, Cornelia, "Data protection in the third pillar: cautious pessimism". MAIK, Martin. *Crime, rights and the EU: the future of police and judicial cooperation.* London: Justice, 2008, p. 121-194.

DE HOYOS SANCHO, Montserrat. "Obtención, registro e intercambio de perfiles de ADN de sospechosos en el espacio de libertad, seguridad y justicia". In CABEZUDO BAJO, María José. *Las bases de datos policiales de ADN ¿Son una herramienta realmente eficaz en la lucha contra la criminalidad grave nacional y transfronteriza?* Madrid: Dykinson, S.L., 2013, p. 63-94.

DE HOYOS SANCHO, Montserrat. "Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos." In ARANGÜENA FANEGO, Coral (dir.) *Espacio Europeo de Libertad, Seguridad y Justicia: Últimos avances en cooperación judicial penal*. Valladolid: Lex Nova, 2010, p. 152-183.

DE LA OLIVA SANTOS, Andrés and DÍEZ-PICAZO GIMÉNEZ, Ignacio. *Derecho Procesal. Introducción.* 3rd ed. Madrid: Ramón Areces, 2004.

DEHOUSSE, Franklin, SIFFLET, Diane. "Les nouvelles perspectives de la coopération de Schengen: le Traité de Prüm". Egmont European Affairs Publication, 2006, accessed April 17, 2014, http://aei.pitt.edu/9091/1/Prum.pdf.

DEL CASTILLO VÁZQUEZ, Isabel-Cecilia. *Protección de datos: cuestiones constitucionales y administrativas (el derecho a saber y la obligación de callar).* Madrid: Civitas, 2007.

DEL MORAL TORRES, Anselmo. *Cooperación policial en la Unión Europea: la necesidad de un modelo de inteligencia criminal eficiente.* Madrid: Dykinson, S.L., 2011.

DÍAZ CABIALE, José Antonio and MARTÍN MORALES, Ricardo. *La garantía constitucional de la inadmisión de la prueba ilícitamente obtenida.* Madrid: Civitas, 2001.

DÍAZ MATEY, Gustavo, "Hacia una definición de Inteligencia", *Revista Inteligencia y Seguridad*, no. 4 (July – November 2008), p. 59-84.

DÍAZ-PINTADO MORALEDA, Pedro. "El modelo de inteligencia en la organización policial". In MONTERO, Julián, ROMERO, Francisco and VALIENTE, Elena. *¿Hacía una Policía Europea?* Madrid: Fundación Policía Española,2002, p. 227-239.

DISLEY, Emma; IRVING, Barrie; HUGHES, William et at. "Technical report on Evaluation of the implementation of the Europol Council Decision and of Europol's activities makes a majority of information exchange." Cambrige: RAND Corporation, 2012.

DONAIRE VILLA, Francisco Javier. *La Constitución y el Acervo de Schengen*. Valencia: Tirant lo Blanch, 2002.

DREWER, Daniel and GUTIÉRREZ ZARZA, Ángeles. "Intercambio de información y protección de datos personales en el ámbito de Eurojust, Europol y OLAF". In GUTIÉRREZ ZARZA, Ángeles. *Nuevas tecnologías, protección de datos personales y proceso penal.* Madrid: La Ley, 2012, p. 131-194.

ESPIGARES MIRA, Jesús. "Instrumentos internacionales de cooperación". In MONTERO, Julián, ROMERO, Francisco, VALIENTE, Elena. *¿Hacía una Policía Europea?* Madrid: Fundación Policía Española, 2002, p. 117-138.

ESQUINAS VALVERDE, Patricia. *Protección de datos personales en la Policía Europea.* Valencia: Tirant lo Blanch, 2010.

ETXEBERRÍA, GURIDI, José Francisco. "La identificación de personas mediante pruebas genéticas y bancos de perfiles de ADN: evolución normativa en el contexto europeo". *Revista de Derecho y Genoma Humano*. Número extraordinario, 2014, p. 135-156.

- "La protección de los datos de ADN en la Unión Europea y en España". In CABEZUDO BAJO, María José. Las bases de datos policiales de ADN ¿Son una herramienta realmente eficaz en la lucha contra la criminalidad grave nacional y transfronteriza? Madrid: Dykinson, S.L., 2013, p. 95-119.
- "Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo".

Eguzkilore: Cuaderno del Instituto Vasco de Criminología. 2009, no. 23, p. 351-366.

- "Los derechos fundamentales en el espacio de libertad, seguridad y justicia penal". *Revista Vasca de Administración Pública*. 2008, no. 82, 2, p. 103-164.
- Los análisis de ADN y su aplicación al proceso penal. Granada: Comares, 2000.

FAZEKAS, Judit. "Development of Justice and Home Affairs Cooperation between 2004 and 2009 in the European Union". *European Integration Studies*, 2009, vol. 7, no 1, p. 3-28.

FELSEN, David, KALAITZIDIS, Akis. "A Historical Overview of Transnational Crime". In REICHEL, Philip. *Handbook of transnational crime and justice*. California: Sage Publications, Inc., 2005.

FERNÁNDEZ-PITA Y GONZÁLEZ, Rafael. "El Tratado de Amsterdam y el Acervo de Schengen". In MINISTERIO DEL INTERIOR. *El espacio Europeo de libertad, seguridad y justicia.* Madrid: Secretaría General Técnica, 2000.

FIJNAUT, Cyrille. "Police Co-operation and the Area of Freedom, security and Justice". In WALKER, Neil. *Europe's Area of Freedom, security and Justice*. Oxford University Press: Oxford, 2004, p. 201-282.

FREIXES SANJUÁN, Teresa. "Protección de datos y globalización. La Convención de Prüm". *Revista de Derecho Constitucional Europeo.* Enero-Junio de 2007, no 7. P. 11-19.

FRÍAS MARTÍNEZ, Emilio. "ADN y privacidad en el proceso penal." Diario La Ley, September 30, 2013, no 8159, p. 11-19.

G. VIADA, Natacha. *Derecho penal y globalización. Cooperación penal internacional.* Marcial Pons, Madrid, 2009.

GALÁN MUÑOZ, Alfonso. "La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea". In COLOMER HERNÁNDEZ, Ignacio and OUBIÑA BARBOLLA, Sabela. *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea".* Navarra: Aranzadi, 2015, p. 37-70.

GARCÍA BORREGO, José Antonio and FERNÁNDEZ VILLAZALA, Tomás. *Introducción al Derecho Procesal Penal.* Madrid: Dykinson, S.L., 2007.

GARCÍA VÁZQUEZ, Sonia. "La cooperación policial y judicial como ejes de consolidación del espacio de Libertad, Seguridad y Justicia e instrumentos de protección de los derechos fundamentales en la Unión Europea". In GOIZUETA VÉRTIZ, Juana and CIENFUEGOS MATEO, Juan. *La eficacia de los Derechos Fundamentales de la UE.* Navarra: Aranzadi, 2014, p. 417-472.

GARCÍA SÁNCHEZ, Manuel. "El Sistema de Información Schengen: estructura, funcionamiento y evolución del sistema de supervisión conjunta en protección de datos". In GOIZUETA VÉRTIZ, Juana; GONZÁLEZ MURUA, Ana Rosa and PARIENTE DE PRADA, Iñaki. *El Espacio de Libertad, Seguridad y Justicia: Schengen y Protección de Datos.* Navarra: Aranzadi, 2012, p. 217-236.

GARRIGA DOMÍNGUEZ, Ana. *Tratamiento de datos personales y Derechos Fundamentales*. Segunda Edición. Madrid: Dykinson, 2009.

GASCÓN INCHAUSTI, Fernando. "Los procesos penales en Europa: líneas de evolución y tendencias de reforma". *Revista de Derecho Procesal*, 2009, no. 1, p. 469-498.

GIMENO SENDRA, José Vicente. *Manual de Derecho Procesal Penal.* Madrid: Colex, 2008.

– *Fundamentos del Derecho* Procesal. Madrid: Civitas, 1981.

GLANCY, Dotorhy J. "The invention of the right to privacy". *Arizona Law Review.* 1979, vol. 21(1), p.1-39.

GLESS, Sabine. "Mutual recognition, judicial inquiries, due process and fundamental rights". In VERVAELE, John A.E. Vervaele. *European Evidence Warrant. Transnational Judicial Inquiries in the EU.* Antwerpen: Intersentia, 2005, p. 121-130.

GÓMEZ AMIGO, Luis and BLANCO SANTOS, Gemma. *Fuentes de prueba y nuevas formas de criminalidad.* Almería: Universidad de Almería. Servicio de Publicaciones, 2001.

GÓMEZ-JARA DÍEZ, Carlos. "¿Federalismo jurídico-penal en la Constitución Europea? Un diálogo con el profesor Silva Sánchez". In ARROYO ZAPATERO, Luis and NIETO MARTÍN, Adán. *El Derecho Penal de la Unión Europea. Situación actual y perspectivas de futuro.* Cuenca: Universidad de Castilla-La Mancha, 2007, p. 87-105.

GONZÁLEZ FUSTER, Gloria. "Protección de datos y cooperación policial y judicial en material penal en la UE". In PÉREZ GIL, Julio. *El proceso penal en la sociedad de la información*. Madrid: La ley, 2012, p. 587-604.

GUASCH PORTAS, Vicente. *Las transferencias internacionales de datos en la normativa española y comunitaria.* Madrid, Agencia Española de Protección de Datos, Agencia Estatal Boletín Oficial del Estado, 2014.

GUILD, Elspeth and GEYER, Florian. "Introduction: The Search for EU Criminal Law – Where is it Headed?". In GUILD, Elspeht and GEYER, Florian (eds.) *Security versus Justice? Police and Judicial Cooperation in the European Union*. Hampshire: Ashgate Publishing Limited, 2008, p. 1-16.

– "Getting local: Schengen, Prüm and the dancing procession of Echternach. Three paces forward and two back for UE police and judicial cooperation in criminal matters. (Commentaries, Centre for European Policy Studies, 2006), accessed April 16, 2014, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?Ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=122940.

GUILD, Elspeth. "Merging Security from Two-Level Game: Inserting the Treaty of Prüm into EU law?", *CEPS Policy Brief,* March 2007, no. 124, accessed April 16, 2014, http://ceps.be/book/merging-security-two-level-game-inserting-treaty-prüm-eu-law.

GUILLE, Laure, "Policing in Europe: An Ethnographic Approach to Understanding the Nature of Cooperation and the Gap between Policy and Practice", *Journal of Contemporary European Research,* vol. 6, no. 2, 2010, accessed January 30, 2013, http://www.jcer.net/index.php/jcer/article/view/192.

GUTIÉRREZ ZARZA, Ángeles. *Exchange of Information and Data Protection in Cross-Border Criminal Proceedings in Europe.* Berlin: Springer, 2015.

– "Conceptos básicos. Marco legal europeo sobre protección de datos en materia penal". In GUTIÉRREZ ZARZA, Ángeles. *Nuevas tecnologías, protección de datos personales y proceso penal.* Madrid: La Ley, 2012.

HAYES, Ben. "EU-SIS Schengen Information System Article 99 report: 33,541 people registered in SIS for surveillance and checks" (Statewatch Analysis, February 2008), accessed October 13, 2013, http://www.statewatch.org/analyses/no-67-sis-art99.pdf.

- "SIS II: fait accompli? Construction of EU's Big Brother database underway" (Statewatch Analysis, May 2005), accessed October 14, 2013 http://www.statewatch.org/news/2005/may/sisii-analysis-may05.pdf.
- "From the Schengen Information System to SIS and the Visa Information (VIS): proposals explained", (Statewatch analysis, February 2004), accessed October 13, 2013, http://www.statewatch.org/news /2005/may/analysis-sisii.pdf.

HEISENBERG, Dorothee. *Negotiating Privacy: The European Union, the United States and personal data protection.* London: Lynne Rienner Publishers, Inc., 2005.

HEMPEL, Leon; CARIUS, Michael and ILTEN, Carla. "Exchange of information and data between law enforcement agencies within the European Union". (Discussion paper Nr. 29/09, Zentrum Technik und Gesellschaft, 2009), https://www.tu-berlin.de/uploads/media/Nr_29_Hempel_Carius_Ilten.pdf.

HOUCK, Max M. and SIEGEL, Jeffrey A. *Fundamentals of Forensic Science.* Second Edition. Oxford: Elsevier. 2010.

HREBLAY, Vendelin. *Les accords de Schengen: Origine, Fonctionnement, Avenir.* Bruxelles: Bruylant, 1998.

HUSTINX, Peter. "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation" (article based on the course given at the European University Institute's Academy of European Law in July 2013), accessed January 20, 2015, https://secure.edps. europa.eu/EDPSWEB/webdav/site/mysite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf.

JENKINS, Brian Michael. "When Jihadis Come Marching Home. The Terrorist Threat Posed by Westerners Returning from Syria and Iraq" (Perspective, RADN Corporation, 2014), accessed August 3, 2015, http://www.rand.org/pubs /perspectives/PE130-1.html

JIMÉNEZ FORTEA, Francisco Javier. "De la restricción de derechos a un derecho procesal del enemigo". In MASFERRER, Aniceto. *Estado de Derecho y derechos fundamentales en la lucha contra el terrorismo.* Navarra: Aranzadi, 2011, p. 611-644.

- "La respuesta procesal penal al terrorismo en el marco de la Unión Europea: un ejemplo de cooperación judicial penal y policial". In CALDERÓN CUADRADO, Mº Pía and IGLESIAS BUHIGUES, José Luís. *El*

Espacio Europeo de Libertad, Seguridad y Justicia: Avances y Derechos Fundamentales en Materia Procesal. Navarra: Aranzadi, 2009, p. 63-98.

JONES, Chris. "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, September 2011), accessed May 19 2015, http://www.statewatch.org/analyses/no-145-ecris-epris-ixp.pdf.

KIETZ, Daniela and MAURER, Andreas, "From Schengen to Prüm". (Comments, German Institute for International and Security Affairs, May 2006), accessed November 14, 2014, http://www.swp-berlin.org/fileadmin /contents/products/comments/Com15_06_Ktz_Mrr_Ks.pdf

KINGSTON, Paul. "Personal information and Privacy". In HEFFERNAN, Liz. *Human Rights. A European Perspective.* Portland: The Round Hall Press, 1994.

KOKOTT and SOBOTTA. "The distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law*, 2013, vol. 3, no 4, (222-228), accessed March 19, 2015, http://idpl.oxfordjournals.org/content/3/4/222.full.pdf+html.

LEINIUS, Katharina "An Imbalance between Security and Liberty? An Analysis of Cross-Border Information Exchange and Data Protection in the Context of the EU's Third Pillar since 9/11". (phd diss, University of Twente, 2009), accessed May 20, 2013, http://essay.utwente.nl/60243/1 /bsc_K_Leinius.pdf.

LLORENTE SÁNCHEZ-ARJONA, Mercedes. *Las garantías procesales en el espacio europeo de justicia penal.* Valencia: Tirant lo Blanch, 2014.

- "La cooperación judicial penal en el Tratado de Lisboa". In DE LOS SANTOS MARTÍN OSTOS, José. *El Derecho Procesal en el espacio judicial Europeo: estudios dedicados al catedrático Faustino Gutiérrez-Alviz y Conradi.* Atelier Libros S.A.; Barcelona, 2013, p. 323-343.

LONGO, Francesca. "Justice and Home Affairs as a New Dimension of the European Security Concept". *European Foreign Affairs Review,* 2013, vol. 18, no. 1, p. 29–46.

LÓPEZ GUERRA, Luis María. "Soft law y sus efectos en el ámbito del Derecho Europeo de los Derechos Humanos". *Teoría y derecho. Revista de pensamiento jurídico.* No. 11. Tirant lo Blanch, 2012, p. 151-167.

– "Derechos e integración europea". In UGARTEMENDÍA ECEIZABARRENA, Juan Ignacio and JÁUREGUI BERECIATU, Gurutz. *Derecho Constitucional Europeo*. Valencia: Tirant lo Blanch, 2011, p. 17-40.

LÓPEZ ORTEGA, Juan José. "Prueba y Proceso Equitativo. Aspectos actuales en la jurisprudencia del Tribunal Europeo de Derecho Humanos". *Derechos y Libertades: revista del Instituto Bartolomé de las Casas*. 1993, no I (2), p. 597-628.

LÓPEZ ORTEGA, Juan José. "Los principios constitucionales del proceso penal". *Derecho Procesal Salvadoreño.*San Salvador: Justicia de Pat, 2000, p. 21-178.

LUENGO ALFONSO, Luis. "Cooperación Policial y Europol". In MINISTERIO DEL INTERIOR. *El espacio Europeo de libertad, seguridad y justicia*. Madrid: Secretaría General Técnica, 2000.

LUIF, Paul. "The Treaty of Prüm: A Reply of Schengen?". (deliverable of the Project within the framework EU-CONSENT "*Wider Europe, Deeper Integration? Constructing Europe Network*", May, 2007), accessed, June 25, 2014, http://www.eu-consent.net/library/deliverables/d38c.pdf

MADSEN, Frank G. *Transnational Organised Crime.* New York: Routledge, 2009.

MARICA, Andreea. *Manual de Europol.* Navarra: Aranzadi, 2014.

MARISCAL, Nicolás. *Más allá de Lisboa: Horizontes europeos.* Técnos: Madrid, 2010.

MARTÍN DIZ, Fernando. "Aspectos recientes de la cooperación judicial y policial hispano-portuguesa; especial consideración del Acuerdo de Évora". *Revista de Estudios Europeos*. 2010, no. 56, p. 95-107.

MARTÍNEZ PÉREZ, Fernando and POZA CISNEROS, María. "El Principio de Disponibilidad: Antecedentes Penales y Convenio de Prüm". In CARMONA RUANO, Miguel; GONZÁLES VEGA, Ignacio U. and MORENO CATENA, Víctor. *Cooperación Judicial Penal en Europa,* Madrid: Dykinson, 2013. P. 417-496.

MCCARTHNEY, Carole I.; WILSON, Tim J. and WILLIAMS, Robin. "Transnational Exchange of Forensic DNA: Viability, Legitimacy, and Acceptability". *European Journal on Criminal and Research.* 2011, vol.17, no. 4, p. 305-322.

MCGHEE, Derek. *Security, Citizenship and Human Rights. Shared Values in Uncertain Times.* Hampshire: Palgrave McMilan, 2010.

MILIONE, Ciro. *El Derecho a la tutela judicial efectiva en la jurisprudencia del tribunal Europeo de Derechos Humanos.* Valencia: Tirant lo blanch, 2015.

MIRANDA ESTRAMPES, Manuel. "La prueba ilícita: la regla de exclusión probatoria y sus excepciones". *Revista Catalana de Seguretat Pública*. May 2010, p. 131-151.

MITSILEGAS Valsamis; MONAR, Jörg and REES, Wyn. *The European Union and Internal Security: Guardian of the People?* Hampshire: Palgrave Macmillan, 2003.

MITSILEGAS, Valsamis. *EU Criminal Law.* Portland: Hart Publishing, 2009.

- MITSILEGAS, Valsamis. "The third wave of third pillar law: which direction for EU criminal justice?" *European Law Review*. 2009, vol. 34, no. 4, p. 523-560.

MOENSSENS, Andre A.; HENDERSON, Carol; E. and PORTWOOD, Sharon G. *Scientific Evidence in Civil and Criminal Cases.* 5th ed. New York: Foundation Press, 2007.

MONTERO AROCA, Juan. *Introducción al Derecho Procesal. Jurisdicción, acción y proceso.* Madrid: Tecnos, 1979.

MONTERO AROCA, Juan; GÓMEZ COLOMER, Juan Luís and BARONA VILAR, Silvia. *Derecho Jurisdiccional I. Parte General.* 20th ed. Valencia: Tirant lo Blanch, 2012.

MORENO CATENA, Víctor. *Fiscalía Europea y Derechos fundamentales.* Valencia, Tirant lo Blanch, 2014, p. 13-14.

- "El cambio de paradigma d el principio de reconocimiento mutuo y sus implicaciones. Perspectivas del Tratado de Lisboa". In CARMONA RUANO, Miguel; GONZÁLEZ VEGA, Ignacio U. and MORENO CATENA, Víctor. *Cooperación Judicial Penal en Europa.* Dykinson: Madrid, 2013, p. 41-78.
- "La garantía de los derechos fundamentales durante la investigación penal". *Cuadernos penales María José Lidón.* 2010, no. 7 p. 13-54.

MORENO CATENA, Víctor and CASTILLEJO MANZANARES, Raquel. *La persecución de los delitos en el Convenio de Schengen*. Valencia: Tirant lo Blanch, 1999.

NIETO MARTÍN, Adán. "Modelos de organización del sistema europea de Derecho penal". In ARROYO ZAPATERO, Luis and NIETO MARTÍN, Adán. *El Derecho*

Penal de la Unión Europea. Situación actual y perspectivas de futuro. Universidad de Castilla-La Mancha: Cuenca, 2007, p. 11-28.

O'NEILL, Maria, "The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar", *Journal of Contemporary European Research*, vol. 6, issue 2, 2010, accessed July 15, 2014, http://www.jcer.net/ojs/index.php/jcer/article/view/264/206

OCCHIPINTI, John D. *The Politics of EU Police cooperation. Towards a European FBI?* Colorado, Lynne Rienner Publishers, Inc., 2003.

OUBIÑA BARBOLLA, Sabela. "Cambio de enfoque en la cooperación judicial penal y policial en la UE en relación con la transmisión de datos personales: las nuevas propuestas normativas y la STJUE de 8 de abril de 2014". In COLOMER HERNÁNDEZ, Ignacio and OUBIÑA BARBOLLA, Sabela. *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea".* Navarra: Aranzadi, 2015, p. 71-123.

- "The European Arrest Warrant in Law and Practice". In RUGGERI, Stefano. *Liberty and Security in Europe. A comparative analysis of pre-trial precautionary measures in criminal proceedings.* Göttingen: V&R Unipress gmbh, 2012, p. 47-66.

PARIENTE DE PRADA, Iñaki. "La reforma de la protección de datos en el ámbito europeo". In GOIZUETA VÉRTIZ, Juana; GONZÁLEZ MURUA, Ana Rosa and PARIENTE DE PRADA, Iñaki. *El Espacio de Libertad, Seguridad y Justicia: Schengen y Protección de Datos.* Navarra: Aranzadi, 2013, p. 121-146.

PARKIN, Joanna. "Difficult Road to the Schengen Information System II: the legacy of 'laboratories' and the cost for fundamental rights and the rule of law" (Research, Centre for European Policy Studies, 17 June 2011), accessed September 9, 2013, http://www.ceps.eu/book/schengen-information-system-and-eu-rule-law.

PAULUSSEN, Christophe. "Impunity for international terrorists? Key legal questions and practical considerations", (Research paper. International Centre for Counter-Terrorism, 2012), accessed 21 January, 2015, http://www.icct.nl/download/file/ICCT-Paulussen-Impunity-April-2012.pdf.

PEERS, Steve, "Guide to EU decision-making and justice and home affairs after the Treaty of Lisbon", A Statewatch publication, December 2010, accessed

September 14, 2014. Http://www.statewatch.org/analyses/no-115-lisbon-treaty-decision-making.pdf.

- EU Justice and Home Affairs Law (Third Edition). Oxford University Press: Oxford, 2011.

PÉREZ MARÍN, María Ángeles. *La lucha contra la criminalidad en la Unión Europea.* Barcelona: Atelier, 2013.

PEYROU, Sylvie. "Algunas reflexiones sobre la protección de datos en el ELSJ o la crónica de una esperanza frustrada". In GOIZUETA VÉRTIZ, Juana; GONZÁLEZ MURUA, Ana Rosa and PARIENTE DE PRADA, Iñaki. *El Espacio de Libertad, Seguridad y Justicia: Schengen y Protección de Datos.* Pamplona: Aranzadi, SA., p. 147-164.

PIRIS, Jean-Claude. *The Lisbon Treaty. A Legal and Political Analysis.* Cambridge University Press: New York, 2010.

PRAINSACK, Barbara and TOOM, Victor, "Performing the Union: The Prüm Decision and the European dream" in *Studies in History and Philosophy of Biological and Biomedical Sciences,* 2013, 44(1), accessed April 7 2014, http://www.sciencedirect.com/science/article/pii/S1369848612001033. 71-79.

REBOLLO DELGADO, Lucrecio. *Vida privada y protección de datos en la Unión Europea.* Madrid: Dykinson S.L., 2008.

RECUERO, Paz. "La protección de datos y Schengen: Una visión desde la experiencia española". In GOIZUETA VÉRTIZ, Juana; GONZÁLEZ MURUA, Ana Rosa and PARIENTE DE PRADA, Iñaki. *El Espacio de Libertad, Seguridad y Justicia: Schengen y Protección de Datos.* Pamplona: Aranzadi, SA., 2013, p. 197-216

REINARES, Fernando and RESA, Carlos. "Transnational organized crime as an increasing threat to the national security of democratic regimes: assessing political impacts and evaluating state responses". In NORTH ATLANTIC TREATY ORGANISATION, 1997, accessed February 1, 2015, http://www.nato.int/acad/fellow/97-99/reinares.pdf.

RENARD, Thomas. "Partners in crime? The EU, its strategic partners and international organised crime." (Working Paper, European Strategic Partnership Observatory, May 2014), http://fride.org/publication/1191/partners-in-crime?-the-eu,-its-strategic-partners-and-international-organised-crime.

ROBINSON, Neil; DISLEY, Emma; POTOGLOU, Dimitris et al. "Feasibility Study for a European Cybercrime Centre" (Final report, February 2012), accessed 1 June, 2015, http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre_en.pdf.

RUGGERI, Stefano. "La transmisión de datos personales en cooperación judicial penal y policial en la UE. La perspectiva italiana". In COLOMER HERNÁNDEZ, Ignacio and OUBIÑA BARBOLLA, Sabela. *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea".* Navarra: Aranzadi, 2015, p. 277-300.

RUIZ DE GARIBAY, Daniel. "Coordination Practice in the Parliamentary Control of Justice and Home Affairs Agencies: The Case of Europol". In CRUM, Ben and FOSSUM, John Erik. *Practices of interparliamentary coordination in international politics.* Colchester: ECPR Press, 2013, p. 87-104.

SANTOLAYA, Pablo. "El derecho a la vida privada y familiar". In GARCÍA ROCA, Javier and SANTOYALA, Pablo. *La Europa de los Derechos. EL Convenio Europeo de Derechos Humanos*. 3rd ed. Madrid: Centro de Estudios Políticos y Constitucionales, 2014, p. 429-449.

- "Limitación de la aplicación de las restricciones de derechos. Art. 18 CEDH". In GARCÍA ROCA, Javier and SANTOYALA, Pablo. *La Europa de los Derechos. EL Convenio Europeo de Derechos Humanos.* 3rd ed. Madrid: Centro de Estudios Políticos y Constitucionales, 2014, p. 657-667.

SANTOS VARA, Juan. "Las consecuencias de la integración de Europol en el Derecho de la Unión Europea (comentario a la Decision del Consejo 2009/371/JAI, de 6 de abril de 2009)". *Revista General de Derecho Europeo.* 2010(20), p. 1-24.

SCHATTENBERG, Bernd. "Schengen Information System: Privacy and Legal Protection". In SCHERMERS, Henry G.; FLINTERMAN, Cees; KELLERMANN, Alfred E. et al. *Free Movement of Persons in Europe*, Dordrecht: Martinus Nijhoff, 1993.

SOLETO MUÑOZ, Helena. "DNA data in criminal procedure in the European fundamental rights context." *Recent Advances in DNA and Gene Sequences*. 2014, no. 8(2), p. 91-97.

- La identificación del imputado: Rueda, fotos, ADN… De los métodos basados en la percepción a la prueba científica. Valencia: Tirant lo blanch, 2009.
- "Parámetros europeos de limitación de Derechos Fundamentales en el uso de datos de ADN en el proceso penal", article submitted for publication.

SOLETO MUÑOZ, Helena and ALCOCEBA GIL, Juan. "Protección de datos y transferencia de perfiles de ADN". In CABEZUDO BAJO, María José. *Las bases de datos policiales de ADN ¿Son una herramienta realmente eficaz en la lucha contra la criminalidad grave nacional y transfronteriza?* Madrid: Dykinson, S.L., 2013, p. 325-344.

SOLETO MUÑOZ, Helena and FIODOROVA, Anna. "DNA and Law Enforcement in the European Union: Tools and Human Rights Protection". *Ultrecht Law Review.* January 2014, vol. 10, issue 1, p. 149-162.

STORBECK, Jürgen. "La cooperación policial europea". In MONTERO, Julián; ROMERO, Francisco and VALIENTE, Elena. *¿Hacía una Policía Europea?* Madrid: Fundación Policía Española, 2002, p. 155-169.

TOPFER, Eric. "Searching for Needles in an ever expanding haystack: Cross-border DNA data exchange in the wake of the Prüm Treaty". *Statewatch Journal,* 2008, vol 18, no 3, accessed may 3, 2014, http://www.statewatch.org /news/2008/dec/eu-dna-statewatch-article.pdf.

VACAS FERNÁNDEZ, Félix. *El terrorismo como crimen internacional. Definición, naturaleza y consecuencias jurídicas internacionales para las personas.* Valencia: Tirant lo Blanch, 2011.

VALLÉS CAUSADA, Luís M. "Usos delictivos no comunicativos de la telefonía móvil: una excepción a la protección del artículo 18.3 CE?". In PÉREZ GIL, Julio. *El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar y probar el delito*. Madrid: La Ley, 2012, p. 219-240.

- *La Policía judicial en la obtención de inteligencia sobre comunicaciones electrónicas para el proceso penal*. (PHd diss., National Distance Education University, 2012), accessed March 20, 2015, http://e-spacio.uned.es/fez/eserv/tesisuned:Derecho-Lmvalles/Documento.pdf.

VERMEULEN, Gert; VANDER BEKEN, Tom; VAN PUYENBROECK, Laurens et al. *Availability of law enforcement information in the European Union. Between mutual recognition and equivalent right of access.* Antwerp: Maklu Publisher, 2005.

VERVAELE, John A. E. "Medidas de investigación de carácter proactivo y uso de información de inteligencia en el proceso penal." In PÉREZ GIL, Julio. *El proceso penal en la sociedad de la* información. Madrid: La Ley, 2012, p. 27-85.

VILABOY LOIS, Lotario. "El sistema jurisdiccional comunitario". In MARIÑO, Fernando M.; MORENO CATENA, Víctor and MOREIRO, Carlos. *Derecho procesal comunitario.* Valencia: Tirant lo Blanch, 2001, p. 15-50.

VLASSIS, Dimitri. "The Global situation of transnational organized crime, the decision of the international community to develop an international convention and the negotiation process". *Resource Material Series*. 2002, no. 59, p. 475-494.

VON BOGDANY, Armin; CRUZ VILLALÓN, Pedro and HUBER, Peter. *El Derecho Constitucional en el espacio jurídico europeo.* Valencia: Tirant lo Blanch, 2013, p. 93.

WALKER, Neil. "In Search of the Area of Freedom, security and Justice: A Constitutional Odyssey". In WALKER, Neil. *Europe's Area of Freedom, security and Justice*. Oxford University Press: Oxford, 2004, p. 3-37.

WARREN Samuel, BRANDEIS, "The Right to Privacy", *Harward Law Review*, 1890, vol.4 no. 5, http://groups.csail.mit.edu/mac/classes/6.805/articles /privacy/Privacy_brand_warr2.html

WILLIAMS, Robin. "Making Forensic DNA Databases: Global Themes and Local Variations". In CABEZUDO BAJO, María José. *Las bases de datos policiales de ADN ¿Son una herramienta realmente eficaz en la lucha contra la criminalidad grave nacional y transfronteriza?* Madrid: Dykinson, S.L., 2013, p. 359-374.

YON, Hasan. "Police liaisons as builders of transnational security cooperation". In AYDINLI Ersel. *Emerging Transnational (In)Security Governance: A Statist-transnationalist approach*. Routledge. New York, 2010, p. 124-142.

ZILLER, Jaques. "Le traité de Prüm. Une vraie-fausse cooperation renforcée dans l'Espace de sécurité de liberté et de justice". (Working Paper, LAW No. 2006/32, European University Institute, 2006), accessed October 2, 2013, http://cadmus.eui.eu/handle/1814/6401.

2. Official documents

ASSOCIATION OF CHIEF POLICE OFFICER OF ENGLAND, WALES & NORTHERN IRELAND. "Guidelines for the use of the Schengen Information System II to locate people for judicial purposes", version 7, 2010, accessed January 16, 2013, http://www.acpo.police.uk/documents/criminaljustice/2008 /200810CJUSIS01.pdf.

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD. "Computers at Risk: Safe Computing in the Information Age", *The National Academies Press,* 1991, accessed January 21, 2015, http://www.nap.edu/openbook. php?Record_id=1581.

COUNCIL OF EUROPE. *Organised crime in Europe: the threat of cybercrime.* Strasbourg: Council of Europe Publishing, 2005.

- "Cross Border Cooperation in the Combating of Organised Crime" (Organised crime – Best Practice Survey nº 5, Strasbourg, January 2003), accessed, October 16, 2013 http://www.coe.int/t/dghl /cooperation/ economiccrime/organisedcrime/BestPractice5E.pdf.
- "Report on the Organised Crime Situation in Council of Europe Member States – 1999", p. 25, accessed May 16, 2015, http://www.coe.int/t/dghl /cooperation/economiccrime/organisedcrime/Report1999E.pdf.

EU FINANCIAL INTELLIGENCE UNITS' PLATFORM. "Report on Confidentiality and Data Protection in the Activity of FIUs", April 2008, accessed August 1, 2015, http://ec.europa.eu/internal_market/company/docs/financial-crime/fiu-report-confidentiality_en.pdf.

EUROPEAN AGENCY FOR THE OPERATIONAL MANAGEMENT OF LARGE-SCALE IT SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE. "SIS II – 2013 Statistics" (Report, June 2014), accessed July 16, 2014, http://www.eulisa.europa.eu/Pages/SIS-II-statistics.aspx

EUROPEAN ASSOCIATION FOR THE DEFENSE OF HUMAN RIGHTS AND EUROPEAN DIGITAL RIGHTS. "Report on Privacy and Personal Data Protection in the European Union", December 2009, accessed October 13, 2014, http://www.ldh-france.org/IMG/pdf/legislation_Europeenne.pdf

EUROPEAN COMMISSION. "Special Eurobarometer 432. "Europeans' attitude towards security", April 2015, accessed July 10, 2015, http://ec.europa.eu/public_opinion/archives/ebs/ebs_432_sum_en.pdf

- Report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. "2014 Report on the Application of the EU Charter of Fundamental Right", 8 May 2015, COM(2015) 191 final.
- Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. "The European Agenda on Security", 28 April 2015, COM(2015) 185 final.
- "Summary Report of Expert Meeting on EPRIS, 19.04.2012", accessed June 3, 2014, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=6238&no=1
- Communication to the European Parliament and the Council. "Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)", 7 December 2012, COM(2012) 735 final.
- Report to the European Parliament and the Council. "Implementation of Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and crossborder crime (the 'Prüm Decision')", 7 December 2012, COM(2012) 732 final.
- Communication to the Council and the European Parliament "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre", 28 March 2012, COM(2012) 140 final.
- Commission Staff Working Paper. "Commission Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments", 6 June 2011, SEC (2011) 567 final.
- Staff working paper "Operation of the Council Framework Decision 2006/960/JHA of 18 December 2006 (Swedish Initiative")", 13 May 2011, SEC(2011) 593 final.
- Staff working paper "Operational Guidance on taking account of Fundamental Rights in Commission Impact Assesment", 6 May 2011, SEC(2011) 567 final.
- Report to the European Parliament and the Council. "based on Article 8 of the Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in th field of tracing and identification of proceeds from, or other property related to, crime, 12 April, 2011, COM(2011) 176 final.
- Communication to the European Parliament and the Council. "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", 22 November, 2010, COM(2010) 673 final.
- Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. "A

comprehensive approach on personal data protection in the European Union", 4 November, 2010, COM(2010) 609 final.

- Communication "On the global approach to transfers of Passenger Name Record (PNR) data to third countries", 21 September 2010, COM(2010) 492 final.
- Communication to the European Parliament and the Council. "Overview of information management in the area of Freedom, security and Justice", 20 July 2010, COM(2010)385 final.
- Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. "Delivering an area of Freedom, security and Justice for Europe's citizens. Action Plan Implementing the Stockholm Programme", 20 April 2010, COM(2010) 171 final.
- Communitacion to the European Parliament and the Council. "Proceeds of organised crime: ensuring that "Crime does not pay", 20 November 2008, COM(2008) 766, final.
- Communication to the Council and the European Parliament. "The Hague Programme: Ten priorities for the next five years The Partnership for European renewal in the field of Freedom, security and Justice", 10 May 2005, COM(2005)184 final.
- Communication to the Council and the European Parliament. "Towards enhancing access to information by law enforcement agencies", 16 June 2004, COM(2004) 429 final.
- Communication to the European Parliament and the Council. "Enhancing police and customs co-operation in the European Union", 18 of May 2004, COM(2004) 376 final.

EUROPEAN COURT OF AUDITS. "Lessons from the European Commission's development of the second generation Schengen Information System (SIS II)" (Special Report, 2013), accessed July 16, 2014, http://www.eca.europa.eu/Lists/ecadocuments/SR14_03/SR14_03_EN.pdf.

EUROPEAN DATA PROTECTION SUPERVISOR. "The European Data Protection Supervisor Strategy 2015-2019", accessed September 30, 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-02-26_Strategy_2015_2019_EN.pdf

- "Europe's big opportunity. EDPS recommendations on the EU's options for data protection reform" (Opinion 3/2015), accessed, September 4, 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/D

ocuments/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_EN.pdf.

- "Executive summary EDPS Opinion of 7 March 2012 on the data protection reform package", OJ, C 192, 30.6.2012, p. 8.
- "Opinion of the European Data Protection Supervisor 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" OJ C 181, 22.6.2011, p. 24-30.

EUROPEAN MONITORING CENTER FOR DRUGS AND DRUG ADDICTION, EUROPOL. "Cocaine: A European Union Perspective in the global context", 2010, accessed, June 7, 2015, https://www.google.es/#q=analytical+work+file+Cola.

EUROPEAN PARLIAMENT. Committee on Civil Liberties, Justice and Home Affairs. "Amendments 48-329 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, accessed September 6, 2015, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/am/1058/1058388/1058388en.pdf

- "Report on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD))", accessed September 4, 2015, http://www.europarl.europa.eu/sides/getDoc.do?type= REPORT&reference=A7-2013-0403&language=EN
- "Report on the initiative by the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (6566/2007 – C6-0079/2007 – 2007/0804(CNS))", p. 6, accessed June20, 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2007-0207+0+DOC+XML+V0//EN&language=hr.

- Directorate General for Internal Policies "Developing an EU Internal Security Strategy, fighting terrorism and organized crime" (Study, 2011), accessed August 13, 2015, http://www.europarl.europa.eu/document/activities/cont/201206/20120627ATT47777/20120627ATT47777EN.pdf

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE. "Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data", accessed September 4, 2015, http://fra.europa.eu/sites/default/files/fra-2014-fundamental-rights-considerations-pnr-data-en.pdf.

- "Handbook on European Data Protection Law", 2014, accessed October 30, 2014, http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law.
- "Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package", October 2012, accessed September 3, 2015, http://fra.europa.eu/en/opinion/2012/fra-opinion-proposed-eu-data-protection-reform-package.

EUROPOL. "EU Terrorism Situation and Trend Report 2015", accessed August 10, 2015, https://www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015.

- "The Internet Organised Crime Threat Assessment (IOCTA) 2015", accessed October 9, 2015, https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.
- "TE-SAT 2014 - European Union Terrorism Situation and Trend Report 2014", accessed August 10, 2015, https://www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014.
- "Operation Archimedes infographics", September 2014, accessed July 6 2015, https://www.europol.europa.eu/content/operation-archimedes-infographics "EU Serious Organised Crime Threat Assessment (SOCTA 2013)", accessed September 30, 2013, https://www.europol.europa.eu/content/eu-serious-and-organised-crime-threat-assessment-socta.
- "Worldwide Operation against Cybercrime", May 2014, accessed July 6, 2015, https://www.europol.europa.eu/content/worldwide-operation-against-cybercriminals
- "OCTA 2011: EU Organised Crime Threat Assessment", accessed September 26, 2013, https://www.europol.europa.eu/content/publication/octa-2011-eu-organised-crime-threat-assesment-1465

– "OCTA 2009: EU Serious Organised Crime Threat Assessment", accessed September 30, 2013, https://www.europol.europa.eu/content /publication/octa-2009-eu-organised-crime-threat-assessment-1463

JOINT SUPERVISORY AUTHORITY OF SCHENGEN. "Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 99 alerts in the Schengen Information System" 2007, accessed January 14, 2013, http://schengen.consilium.europa.eu/media/135672/07-02%20draft%20report%20article%2099.en08.pdf.

INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT. "Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments", 2010, accessed 12 September, 2015, http://ec.europa.eu/dgs/home-affairs/doc_centre/police/docs /icmpd_study_lea_infoex.pdf.

INTERPOL. "Annual Report 2014", accessed May 17, 2015, http://www.interpol.int /News-and-media/Publications.

HOUSE OF LORDS. European Union Committee Report. "Schengen Information System II (SIS II)" (Report with Evidence, 2007), accessed January 18, 2013, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldeucom/49/49.pdf

– "Prüm: an effective weapon against terrorism and crime?" (Report with Evidence, May 2007), accessed July 13, 2014, http://www.statewatch.org /news/2007/may/eu-hol-prum-report.pdf.

SCHENGEN JOINT SUPERVISORY AUTHORITY. "Eight Activity Report – December 2005 – December 2008", accessed January 16, 2013, http://schengen .consilium.europa.eu/media/135384/8th%20schengen%20act.report%202005-08.en.pdf.

SIS SUPERVISION COORDINATION GROUP. "A Guide for Exercising the Right of Access", October 2014 (updated October 2015), accessed November 3, 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite /shared/Documents/Cooperation/Large_IT_systems/SIS/15-1012_SIS_II _GUIDE_OF_ACCESS _UPDATED_2015_EN.pdf

THE LISBON NETWORK. "The Right to a Fair Trial: Analysis of the Condemnations of the Portuguese State due to the Violation of Article 6 of the European Convention on Human Rights", Council of Europe, 2008, accessed October

30, 2014, http://www.coe.int/t/dghl/cooperation/lisbonnetwork/Themis/ECHR/Paper4_en.asp.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. "Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes: Research Report (Vienna, October 2011)", accessed September 20, 2013, www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

– "The Globalization of Crime. A Transnational Organized Crime Threat Assesment. 2010", accessed September 27, 2013, https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.