Document title:	Final Report on Systems Review and Approval
Due delivery date:	**31/10/2014**
Nature:	**Deliverable**
Project Title:	**Collaborative Information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime**
Project acronym:	**CAPER**
Instrument:	**Large Scale Collaborative Project**
Thematic Priority:	**FP7-SECURITY-2010-1.2-1**
Grant Agreement:	**261712**

Organisation name of lead contractor for this deliverable: IDT-UAB

Dissemination level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	X

History			
Version	First name & Name	Modifications	Date
1	Antoni Roig	Legal Update and CAPER Regulatory Model v.1	10/06/2014
2	Antoni Roig	Internal and External Supervisors	11/06/2014
3	Antoni Roig	Systems Review and Approval	13/06/2014
4	Jorge González	CAPER Regulatory Model v.2	14/06/2014
5	Antoni Roig	Legal Update	28/06/2014
6	Antoni Roig	CAPER Regulatory Model v.3	29/06/2014
7	Antoni Roig	CAPER Regulatory Model v. 4	30/06/2014
8	Pompeu Casanovas/Antoni Roig	Legal Update/Final version	30/06/2014
9	Antoni Roig	Legal Update July-August 2014	09/09/2014
10	Antoni Roig	Legal Update September-October 2014	10/10/2014
11	Jorge González Conejero	Caper flow figure	18/10/2014
21	Rebeca Varela/Emma Tedoro	Legal Caper Regulatory Model v. 5	21/10/2010

Validation			
	First name & Name	Organisation short name	Visa
Responsible	Antoni Roig	IDT-UAB	X
WP leader	Pompeu Casanovas	IDT-UAB	X
Coordinator	Felipe Melero	S21Sec	X

INDEX

1 INTRODUCTION

1.1 Aim of the deliverable

The aim of D7.7 is to present, complete and prepare the validation of the functioning, affordances and applications of CAPER.

D7.7. has been written in close relation to D7.8, containing the Ethical audit of CAPER. All along the previous Deliverables of WP7 (from D7.1 to D7.6) we have achieved the following milestones:

- An operable definition of "organized crime".

- A description of the state of the art in Privacy by Design (PbD), Data Protection by Design (DPbD) and Security by Design (SbD).

- A conceptual description of the "CAPER Regulatory Model" (CRM), stemming from several related concepts: (i) the pair Interoperability (IT governance) / *Interoperativity* (organizational governance); (ii) Data Governance, (iii) Networked Governance, (iv) and Ethics.

- A description of the legal and ethical framework set after the application of the Treatise of Lisbon (2007) to Security and Data Protection issues.

- A general description of the national Data Protection requirements in France, Germany, Italy, Israel, and Spain.

- A first assessment of some ethical risks, faced within a framework which is broader than the specific challenges which rise in CAPER (CRM).

- A treatment of (i) use of *Social Network Analysis (SNA)* for the purpose of research; (ii) the use of *profiling* for the purpose of research and; (iii) *the storage, access and conservation of multimedia files* for the purpose of research.

- The connection between principles on Freedom, Security and Justice settled by Article 29 (Directive 95/46) Data Protection Working Party in 1997 and several converging formulations recently raised in separate fields: (i) Linked Open Data Principles (T. Berners-Lee, 2006) (ii) Internet Identity Metasystem Layer: Laws of Identity (Kim Cameron, 2005), (iii) Privacy by Design Foundational Principles (Ann Cavoukian, 2006), (iv) Global Privacy Standard (Cavoukian, 2007), (v) LII Standards (Déclaration de Montreal, LAW.GOV Principles, The Hague Principle, 2002-2012).

- The Mid-term Ethical Audit on CAPER System Development and Deployment carried out by the Ethical Committee (Ugo Pagallo, Giovanni Sartor, John Zeleznikow, Danièle Bourcier, Josep Montserrat).

- A Private Impact Assessment (PIA) / Data Protection Impact Assessment (DPIA) that was carried out by WP7 team and presented to technical members and LEAs during the Consortium Meeting organized by Technion in Haifa, Israel, the 30th and 31st January 2013.

- Several assessments (by the Ethical Committee) laid down to give a reply to critical issues:

I. Can LEAs be allowed to use CAPER tools in real investigations before the Project is closed? If this were the case, which conditions would need to be fulfilled? How these prospective investigations could be made accountable?

II. What are the concrete procedures and steps to be taken to prevent false positives? How vulnerability and lack of protection of individuals can be avoided? Which measures will be taken to give citizens the possibility to access and ask for rectification if a personal harm is produced?

III. Which parts, if any, of data protection principles by design (DPbD) could be implemented in CAPER? What it is really meant by "security by design" (SbD) in the CAPER Regulatory Model (CRM)?

IV. And how to embed CRM conceptual scheme into final Recommendations to regulate the use of the platform and secure the protection of data? Is there a link between CRM and SbD? Are ontologies relevant to this link?

- A framework of the legal general concepts (Organized Crime Structure: OCS) based on the literature on organized crime theory and EUROPOL Annual Reviews. This framework was designed to provide a common supranational structure to improve interoperability among the European LEAs involved.

- A ontology, named *European LEAs Interoperability Ontology (ELIO)*, that models OCS, relationships among its concepts, attributes, and all the knowledge directly gathered from LEAs in a planned and commonly shared knowledge acquisition process.

- The theoretical construction of *validity* as a composite indicator which is crucial for the legality of the CAPER Regulatory Model.

As already stated and shown in D7.3, and D7.4, PIA constitutes not only a methodology but also a process. In Europe, security and data protection (the domain of Freedom, Security and Justice) is a hot topic, and an evolving field in which legislation, policies, and principles are dynamically developed. We have taken into account the last contributions by experts and discussions in the EU Parliament (held in May 2014).

With this situation in mind, we have concentrated onto deepening the model, and connecting it with applications and with current discussions in the field of *Ethics and the Semantic Web* (E & SW). We can say that we have been pioneering this connection in several

International Forums and Conferences.[1] The result is that we have set this field as a (relative) independent field of research.

The main question that we intend to answer in D7.7 is this one: Is the CAPER Regulatory Model acceptable within the European Union community on Data Protection?

The core of D7.7 is an attempt to provide a reasonable answer to such a question. Its contents are distributed as follows:

1. Introduction
2. Legal Update
3. Legal CAPER Regulatory Model
4. Internal and External Supervision within CAPER
5. Systems Review and Validation
6. Conclusions

[1] *The Ethical and Legal Aspects of Digital Security. Special Workshop on Digital Security and Data Protection.* Sintelnet and CAPER Projects, CNRS-CERSA, Rue Thénad 10, Paris, November 29th-30th 2013;JURIX JOINT WORKSOP AICOL-2013 V Workshop on Artificial Intelligence and the Complexity of Legal Systems (AICOL) - Follow up IVR-XXVI (Belo Orizonte) Special Workshop on Social Intelligence and the Law (jointly with AICOL http://www.aicol.eu/Artificial Intelligence and Complex Legal Systems), Bologna, December 11th 2013; *IV Simposio de Informática Jurídica Documental y Resolución de Disputas en Línia*, Barcelona , Palau Macaya 4-5 December 2013 http://158.109.228.15/simposio//es/index.html; Crowd intelligence: Foundations, Methods and Practices, SINTELNET Workshop, IEC, Barcelona January 11th, 2014; *Open Data and Data Protection: Problems and Perspectives*, Round Table at *Computers, Privacy & Data Protection (CPDP) Conference* , Brussels, *Les Halles de Schaerbeek* Conference Centre in Brussels, January 22th 2014; *Institutions and Social Coordination in the Intelligent Web*, SINTELNET Workshop, St. Carles de la Ràpita, May 10-12th 2014; Rights and Governance Track, Tutorial and Round Table on Data Protection at 11 *European Semantic Web Conference* (ESWC 14'), Anissaras-Hersonissou, Crete May, 25th-29th, 2014, http://2014.eswc-conferences.org/.

1.2 Corresponding planned work in Annex I

The planned work set in the CAPER DOW was quite general, and included D7.7 as the last Deliverable to check the CAPER Regulatory Model from the legal perspective.

Since D7.1 it is clear why a more specific and detailed CRM substitutes the foreseen Ethical Code. The Final Legal validation has to be performed at the end of the project, once the final version of the platform has been presented by CAPER technical partners, and tested by LEAs. This deliverable is an updated version of D7.7 version 1 delivered in June 2014, due to the extension of the project, and the fact that the platform has being tested during the last three months. Meanwhile, we have been working out the Recommendations, the new PIA for CAPER and the theoretical dimension of the CAPER Regulatory Model that will be presented in D7.8.

In Deliverable D7.6 we specified several tasks to be completed from January 2014 to the end of the project:

1) Monitoring the functioning of the CAPER platform in all the stages of data collection, processing, use and management;

2) monitoring the development of the CAPER use case on drugs, paying a special attention to the connection between the multilingual ontology and the legal interoperability ontology;

3) building a new Data Protection Impact Assessment (or Privacy Impact Assessment) to be developed and applied with the LEAs in their preliminary use of the CAPER tools in real investigations and cases;

4) identifying best practices and CRM Regulatory Protocols (tailor-made) to set an operable set of rules and guidelines for future PIAs, iterative ethical audits and the monitoring of LEA's behaviour;

5) setting a system security plan to differentiate the automatable and non-automatable information processes in the platform, and their involvement with citizens and human rights associations;

6) developing the specific tests and metrics to carry out the final ethical audit;

7) refining validity as a legal composite indicator, and connecting theoretically this kind of tool with its public dimension; that is to say, with the public security space in which the balance between the protection of citizens and their liberty can happen

8) coordinating LEA's needs and practices with the requirements of EUROPOL, and national and EU Data Protection Agencies.

All eight tasks have been faced so far. As we will show later, we have here nurtured the dialogue with LEAs, Data Protection Agencies, and relevant European Union agencies in the field of cooperation in criminal matters, to ensure the correctness and legality of the whole process. This means that we have seen the legal and governance elements of CRM and elaborated in D. 7.8 a broader theory of Ethics and the Semantic Web.

2 LEGAL UPDATE

2.1 Data protection reform: General Principles for the CAPER Regulatory Model

2.1.1. Working Paper 215 Article 29 Data Protection Working Party

Last April the Article 29 Data Protection Working Party adopted an interesting Opinion on surveillance of electronic communications for intelligence and national security purposes[2].

The Article 29 Working Group welcomes the proposal of the European Parliament for a new article 43a of the Data Protection Package, providing for mandatory information to individuals when access to data has been given to a public authority in the last twelve months.

The Working Party considers that the scope of the national security exemption should be clarified in order to give legal certainty regarding the scope of application of EU law. To date, no clear definition of the concept of national security has been adopted by the European legislator, nor is the case law of the European courts conclusive.

The Working Party recommends the quick start of negotiations on an international agreement to grant adequate data protection safeguards to individuals when intelligence activities are carried out. The Working Party also supports the development of a global instrument providing for enforceable, high level privacy and data protection principles.

Surveillance programmes run by the EU Member States will in general not be subject to EU law, following the national security exemption written into the European treaties, as well as – following this decision of the contracting Member States – several EU regulations and directives, including the EU data protection directive 95/46/EC. That does not mean however such programmes are only subject to national law. The analysis of the WP29 shows, that even though EU law in general and the data protection directive in particular do not apply, the

[2] WP 215, Opinion 04/2014 of the Article 29 Data Protection Working Party, on surveillance of electronic communications for intelligence and national security purposes, adopted on 10 April 2014.

data protection principles6 following the European Convention on Human Rights and Council of Europe Convention 108 on the protection of personal data will for the most part still need to be respected by the intelligence services in order to lawfully perform their duties[3].

Under no circumstance surveillance programmes based on the indiscriminate, blanket collection of personal data can meet the requirements of necessity and proportionality set out in these data protection principles.

Also, it should be kept in mind that there is no automatic presumption that the national security argument used by a national authority exists and is valid. This has to be demonstrated.

All conditions for international transfers of personal data set out in directive 95/46/EC need to be respected: this means above all that the recipient ensures an adequate level of protection and that transfers need to be in line with the original purpose for which the data were collected.

None of the instruments available that can be used as an alternative basis to transfer personal data to countries that have not been found adequate (Safe Harbor, Standard Contractual Clauses and BCRs) allow for third country public authorities for the purpose of indiscriminate, massive surveillance to gain access to personal data transferred on the basis of these instruments.

An international agreement providing safeguards could ensure that intelligence services respect fundamental rights.

[3] ECJ, Joined Cases C-293/12 and C-594/12, 8 April 2014 where the Court has held that the retention of traffic data "without any differentiation, limitation or exception" constitutes "a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary" (§§57 jo. 65).

In order to ensure that intelligence services indeed do respect the limits imposed on surveillance programmes, meaningful oversight mechanisms need to be implemented in the laws of all Member States. This should include fully independent checks on data processing operations by an independent body as well as effective enforcement powers. Next to effective and robust parliamentary scrutiny, this could be done by a data protection authority or another suitable independent body, depending on the oversight arrangements adopted by the Member State. If the oversight were to be carried out by another body, the Working Party encourages regular contacts between this body and the national data protection authority to ensure a coherent and consistent application of the data protection principles.

The National Data Protection Regulation*, when applicable, generally provides for a number of exemptions (derogations to one or more principles) for the processing of personal data by intelligence services. These exemptions routinely refer to the basic duties of data controllers and the data subject rights. The limitations may concern restriction to the right to be informed and the right of access by the data subject, which is in general to be exercised through the data protection authority.*

Recommendations

More transparency

The Working Party considers it important that Member States are transparent to the greatest extent possible about their involvement in intelligence data collection and sharing programmes, preferably in public, but if necessary at least with their national parliaments and the competent supervisory authorities. Data protection authorities are recommended to share their expertise at national level in order to restore the balance between national security interests and the fundamental right of respect for the private life of individuals.

Maximising public awareness

The Working Party intends to organise a conference in the second half of 2014 bringing together all stakeholders to discuss a possible approach.

Ensure effective oversight on the intelligence services

- Strong internal checks for compliance with the national legal framework in order to ensure accountability and transparency;

- Effective parliamentary scrutiny in line with national parliamentary traditions. National data protection authorities should encourage parliaments already having supervisory powers over the intelligence services to actively carry out these tasks;

- Effective, robust and independent external oversight, performed either by a dedicated body with the involvement of the data protection authorities or by the data protection authority itself, having power to access data and other relevant documentation on a regular basis and on its own initiative (ex officio), as well as an obligation to inspect following complaints. Prior approval of the intelligence services to be supervised must not be required;

Improve the protection on European level

- *Adoption of the data protection reform package*
- *Clarify the scope of the national security exception*

International protection

Adequate safeguards for intelligence data sharing

In the view of the Working Party, secret cooperation agreements between Member States and/or third countries do not meet the standard of the ECtHR for a clear and accessible legal basis.

Negotiate international agreements to grant adequate data protection safeguards4.

[4] See also European Data Protection Officer, Position Paper on The transfer of personal data to third countries and international organisations by EU institutions and bodies, on 14 July, 2014.

The idea of a so-called Umbrella agreement, currently negotiated between the US and the EU, is a step into a right direction. However, such an agreement is likely to have two shortcomings: it will exempt cases concerning national security, at least from an EU perspective, since it is negotiated as an agreement based on EU law only. Its structure suggests that it would only apply to data transferred between public authorities in the US and the EU, not to data collected by private entities. This is also what becomes clear from the report of the EU-US High Level Contact Group (HLCG) on information sharing and privacy and personal data protection 23, which forms the basis for the negotiations on the Umbrella agreement. The Working Party stresses that under the Umbrella agreement, the purpose for the processing of the transferred data should be the same both in the EU and the US. It would not be acceptable if data originating from EU law enforcement could subsequently be used by US intelligence for national security purposes, if such is not also possible in the EU.

Since the Umbrella Agreement will fall short in offering full protection to all citizens, what is needed is an international agreement providing adequate protection against indiscriminate surveillance.

Develop a global instrument protecting privacy and personal data

The Article 29 Data Protection Working Party suggests the adoption of an additional protocol to Article 17 of the UN International Covenant on Civil and Political.

The Working Party supports the initiative taken by the German government and the call from the International Conference of Data Protection and Privacy Commissioners.25,26 Furthermore, the Working Party continues to support the accession of third countries to the Council of Europe's Convention 108.

2.1.2. The right to be forgotten

On a recent Decision [5] the Court of Justice of the European Union had the opportunity to clarify several interesting aspects for the CAPER project related to the territoriality of EU

[5] Case C-131/12, 13 May 2014.

rules, the applicability of EU data protection rules to a search engine and the right to be forgotten.

- EU rules apply to search engine operators, even if the server is located outside Europe, if they have a branch or subsidiary in a Member State
- Search engines are controllers of personal data
- Individuals have the right, under certain conditions, to ask search engines to remove links with personal information about them. This applies when the information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing. A case-by case assessment is required to consider the type information, its sensitivity for the individual's private life and the interest of the public to access that information.

The right to be forgotten is an updated version for the digital age of the current right of access included in the 1995 Data protection Directive[6]. Non-European corporations, when offering services to European consumers, must apply European rules[7]. To make the right more effective, the Commission has proposed reversing the burden of proof: it is the corporation, not the individual who has to prove that the data cannot be deleted because it is relevant and needed. If a court or regulatory authority in the European Union rules that the data must be erased, then individuals have a right to erasure[8].

[6] EU 1995 Data Protection Directive

The data subject's right of access to data

Article 12 : Right of access

Member States shall guarantee every data subject the right to obtain from the controller: (…)

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

[7] Article 3 of the proposed Data Protection Regulation.

[8] Article 17 of the Commission Proposal and of the European Parliament Vote.

Commission Proposal

• Article 17: Right to be forgotten and to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(d) the processing of the data does not comply with this Regulation for other reasons.

2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

European Parliament Vote

• Article 17: Right to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, and to obtain from third parties the erasure of any links to, or copy or replication of that data, where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(a) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;

(d) the data has been unlawfully processed.

1a. The application of paragraph 1 shall be dependent upon the ability of the data controller to verify that the person requesting the erasure is the data subject.

2. Where the controller referred to in paragraph 1 has made the personal data public without a justification based on Article 6(1), it shall take all reasonable steps to have the data erased, including by third parties, without prejudice to Article 77. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties.

The proposed Data Protection Regulation allows data protection authorities to impose fines of up to 2% of annual worldwide turnover where corporations do not respect the right to be forgotten. Some reasons of public interest can justify keeping data and thus limit the right to be forgotten: the right of freedom of speech, public health, and processing data for historical, statistical and scientific purposes.

A search engine will have to delete information when it receives a concrete request from an individual affected. The search engine might conclude that for some reasons like the interest of general public to have access to the information related to public officer or someone who has a public role, the links are maintained. In those cases, the individual has the option to complain to national data protection supervisory authorities or to national courts. The latter will have the ultimate decision on the application of the right to be forgotten.

The Commission now expects a quick adoption of the data protection reform, including the right to be forgotten, and expects engine operators to implement procedures in order to endure individuals can request the deletion of inaccurate, inadequate or irrelevant data.

2.1.3. Fair Trial and special Safeguards for Children in Criminal Proceedings

The European Union proposed in November 2013 a package of five proposals of procedural safeguards to guarantee fair trial rights for all citizens[9]:

- A Directive to strengthen the presumption of innocence and the right to be present at trial in criminal proceedings
- A Directive establishing specific protection to children suspected or accused of a crime, as they are particularly vulnerable during court proceedings[10].
- A Directive on the right to provisional legal aid for citizens suspected or accused of a crime at the early stages of criminal proceedings.
- A Commission Recommendation on procedural safeguards for vulnerable people suspected or accused in criminal proceedings suffering from physical or mental disabilities.
- A Commission Recommendation on the right to legal aid.

On June 2014, the Justice Ministers from the Member States agreed (an informal agreement) for measures that will guarantee special safeguards for children during criminal court proceedings[11]:

"Making the justice system in Europe more child-friendly is a priority for the Commission[12]. As the most vulnerable in society they deserve special protection. I would like to thank Ministers in the Council and especially my colleague Charalambos Athanasiou for their committed work on this file which made it possible to reach such a fast initial agreement," said Vice-President Viviane Reding, the EU's Justice Commissioner. *"This is also about putting the EU Charter of Fundamental Rights into law and action as its states that we must act in the child's best interests. That's exactly what this directive does: putting*

[9] IP/13/1157, MEMO/13/1046, 27/11/2013. http://ec.europa.eu/justice/newsroom/criminal/news/131127_en.htm .
[10] COM/2013/0822 final.
[11] IP/14/636, 06/06/2014.
[12] http://ec.europa.eu/justice/fundamental-rights/rights-child/friendly . EU Agenda for the right of the Child, 15/02/2011, COM(2011) 60 Final, available at http://ec.europa.eu/justice/policies/children/docs/com_2011_60_en.pdf .

children first by guaranteeing better rights for those who are suspected or accused of a crime."

Every year in the EU roughly 1 million children face criminal justice proceedings, representing 12% of the total European population facing criminal justice. The key safeguards that children should benefit from include:

- Children should not be able to waive their right to be assisted by a lawyer
- Children should have the right to a medical examination
- Children should be detained separately from adults
- Children should not have to bear the cost of certain safeguards, even if found guilty
- Being informed of their legal rights
- Being assisted by parents or other adequate people
- Not being questioned in public hearings
- Access to rehabilitation measures

2.1.4. European Parliament support to Data Protection reform

The European Parliament vote in March 2014 has strongly supported the European Commission's data protection reform[13].

"*The message the European Parliament is sending is unequivocal: This reform is a necessity, and now it is irreversible. Europe's directly elected parliamentarians have listened to European citizens and European businesses and, with this vote, have made clear that we need a uniform and strong European data protection law, which will make life easier for business and strengthen the protection of our citizens,*" said Vice-President Viviane Reding, the EU's Justice Commissioner. "*Data Protection is made in Europe. Strong data protection rules must be Europe's trade mark. Following the U.S. data spying scandals, data protection is more than ever a competitive advantage. I want to thank Mr Albrecht and Mr Droutsas for their committed and tireless work on the data protection reform. Today's vote is the strongest signal that it is time to deliver this reform for our citizens and our businesses."*

[13] 12 March 2014: 621 votes in favour, 10 against and 22 abstentions for the Regulation and 371 votes in favour, 276 against and 30 abstentions for the Directive (MEMO/13/923 and MEMO/14/60).

On 4 March 2014 Ministers in the Council discussed the data protection reform, focusing on its territorial scope and on aspects relating to international transfers[14]. The reform should strengthen citizens' rights:

- A right to be forgotten (before-mentioned)
- Easier access to your own data or right to data portability between service providers
- Putting you in control: explicit consent
- Data protection first, not afterthought: "Privacy by design" and "privacy by default" become essential principles in EU data protection rules

2.1.5. European Data Protection Supervisor Opinion on AFSJ, 4 June 2014

An important Opinion on the future development of the area of freedom, security and justice was adopted on June 2014. Some of the main conclusions are:

- *The EU needs to demonstrate that it has learnt the lessons from the last five years, that it cannot adopt measures which, on close examination, interfere with fundamental rights and fail the tests of necessity and proportionality. As the Commission has reiterated many times, the Charter must now be the compass for EU policies and laws (…).*
- *Ways forward to ensuring that privacy and data protection considerations are fully integrated in the development of all new policies and legislation in the area of freedom, security and justice could be:*

. integrating data protection concerns in general impact assessments,

. assessing alternative less intrusive means to achieving policy objectives,

. strengthening data quality and data subject rights and redress,

. evaluating the exchange of information against policy objectives, and

. ensuring international agreements with third countries respect EU individuals' right to data protection.

[14] MEMO/14/144 and SPEECH/14/175.

2.1.6. European Justice and Home Affairs Council 5-6 June 2014 in Luxembourg

Main agenda items for Home Affairs Ministers (5 June):

• Revised EU strategy for combating radicalisation and recruitment to terrorism

• Foreign fighters and returnees from a counter-terrorism perspective

• Future developments in the Home Affairs area

• Task Force for the Mediterranean

Main agenda items for Justice Ministers (5 and 6 June):

• Future developments in the justice area (5 June)

• Reform of EU data protection rules

• Special safeguards for children in criminal proceedings

• European Public Prosecutor's Office

• Cross-border insolvency law

We have already talked about the Right to be forgotten and the special safeguards for children in criminal proceedings. Other items in those agendas are not related to CAPER. We will thus only focus on the revisited EU strategy for combating radicalisation and recruitment to terrorism, future fighters and returnees from a counter-terrorism perspective, future developments in the Home Affairs area and data transfers to third countries and the territorial scope of the data protection regulation.

- Revisited EU strategy for combating radicalisation and recruitment to terrorism

Several proposals were adopted by the Commission in its 15th January 2014 Communication on radicalisation. A collection of approaches and practices to prevent and counter radicalisation developed by the Radicalisation Awareness Network (RAN) was published then by the Commission.

The JHA Council adopts in the 5th June 2014 session the revised strategy for combating Radicalisation and Recruitment to Terrorism.

- Fight against terrorism: Foreign fighters and returnees from a counter-terrorism perspective, in particular with regard to Syria

During the JHA Council in December 2013, four priority areas for the EU action were identified: prevention, information exchange, criminal justice response and cooperation with third countries.

The Commission has set up and supports the Radicalisation Awareness Network (RAN) which supports member States' efforts to prevent violent radicalisation and the recruitment of individuals to terrorism activities.

- Future developments in the Home Affairs area

The Stockholm Programme that guided the Home Affairs policies from 2010 to 2014 is coming to an end in December. The Commission presented its vision of the future agenda for Home Affairs in May 2014. Europe will have to face increasing international mobility, demographic developments, instability in the direct neighbourhood of Europe and challenges due to technology new capabilities. Many of those challenges require strong cooperation between the Member States, the EU institutions, EU agencies and third countries.

- Data transfers to third countries and territorial scope of the data protection regulation.

An agreement has been reached on the Chapter V of the Regulation, the rules that govern data transfers to third countries. In three cases the transfer will be considered legal data transfer:

. When the Commission has found that a third country is "adequate" in terms of data protection, because it has for instance robust data protection legislation or data protection authorities in place.

. When appropriate safeguards exist, like binding corporate rules approved by data protection authorities.

. In clearly defined specific situations which need the transfer like a tax or competition investigation.

- Territorial scope of the data protection regulation.

EU data protection will apply to non-European corporations if they do business on the European Single Market[15].

- Data Retention Directive.

On 8 April the European Court of Justice rendered a judgment by which it invalidated the 2006/24/EC Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive).

The retention is to be performed in order to ensure that the data are available for the purpose of the investigation, detection, and prosecution of serious crime, as defined by each member state in its national law.

The Council held an exchange of views on the consequences of the invalidation of Directive 2006/24/EC.

- EUROPOL.

The Council reached a general approach on the proposal for a regulation on the European Agency for Law Enforcement Cooperation and Training (Europol). This general approach will constitute the basis for negotiations with the European Parliament in order to agree the final text of the regulation.

[15] Article 3 of the Data Protection Regulation.

Apart from the merger, the new draft regulation is mainly aimed at "lisbonising" the current Council decision on Europol, notably including provisions on parliamentary oversight, adapting Europol 's external relations to the new Treaty rules and appointing the European Data Protection Supervisor as the data protection supervisory body for Europol. Moreover, the draft regulation aims at providing Europol with a flexible and modern data management regime and aligning Europol's governance with the general guidelines applicable to agencies.

- Fundamental Rights Agency Annual Report

The Council took note of the annual report of the Fundamental Rights Agency[16].

One interesting item of the report is the Human rights based police training.

A network with relevant actors was build up over 2010–2011 (CEPOL, AEPC, European Council of Police Trade Unions and NGOs). A workshop in 2010 identified the core requirements for turning theory into practice (based on the MIDIS policing-related indications) in formal police training, and has kicked off a process of structured and targeted exchange. It identified thematic areas that are most vital for the police colleges and academies to translate human rights provisions into training. Human rights education and training activities based on existing research work were planned.

In 2013, a Manual is published on Fundamental rights- based police training: a manual for police trainers.

[16] Annual Activity Report 2013 (June 2014), available at http://fra.europa.eu/en/publication/2014/annual-activity-report-2013 .

2.1.7. European Council 26-27 June 2014 in Brussels

One of the interesting discussions held at The European Council was the definition of the strategic guidelines for legislative and operational planning for the coming years within the area of freedom, security and justice[17].

In further developing the area of freedom, security and justice over the next years, it will be crucial to ensure the protection and promotion of fundamental rights, including data protection, whilst addressing security concerns, also in relations with third countries, and to adopt a strong EU General Data Protection framework by 2015.

The National Security exception is now a proportionate limitation of the general data protection framework justified and supervised. This option for a general fulfilment of the data protection, even in the area of freedom, security and justice needs to be present in the CAPER Regulatory Model.

It is essential to guarantee a genuine area of security for European citizens through operational police cooperation and by preventing and combating serious and organised crime, including human trafficking and smuggling, as well as corruption. At the same time, an effective EU counter terrorism policy is needed, whereby all relevant actors work closely together, integrating the internal and external aspects of the fight against terrorism. In this context, the European Council reaffirms the role of the EU Counter Terrorism Coordinator. In its fight against crime and terrorism, the Union should back national authorities by mobilising all instruments of judicial and police cooperation, with a reinforced coordination role for Europol and Eurojust, including through:

- *the review and update of the internal security strategy by mid-2015;*
- *the improvement of cross-border information exchanges, including on criminal records;*
- *the further development of a comprehensive approach to cybersecurity and cybercrime;*
- *the prevention of radicalisation and extremism and action to address the phenomenon of foreign fighters, including through the effective use of existing instruments for EU-wide*

[17] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/143478.pdf .

alerts and the development of instruments such as the EU Passenger Name Record system.

2.1.8. European Council Extraordinary 30 August 2014 in Brussels

The European Council is extremely dismayed by the deterioration of the security and humanitarian situation in Iraq and in Syria as a result of the occupation of parts of their territory by the "Islamic State in Iraq and the Levant (ISIL)".

It calls for the accelerated implementation of the package of EU measures in support of Member States efforts, as agreed by the Council since June 2013, in particular to prevent radicalisation and extremism, share information more effectively- including with relevant third countries, dissuade, detect and disrupt suspicious travel and investigate and prosecute foreign fighters. In this context, the European Council calls on the Council and the European Parliament to finalise work on the EU Passenger Name Record proposal before the end of the year.

The European Council also underlines the need for close cooperation with third countries to develop a coherent approach, including strengthening border and aviation security and counter-terrorism capacity in the region.

The European Council requests the Council to review the effectiveness of the measures and to propose additional action, as required. The European Council will review this matter at its meeting in December[18].

[18] European Council Conclusions, 30 August 2014, Brussels, available at http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/144538.pdf

2.1.9. European Justice and Home Affairs Council 9-10 October 14 in Luxembourg[19]

Justice Ministers are expected to reach a partial general approach on the chapter IV of the draft regulation (controller and processor) setting out a general EU framework for data protection and the related. They also held a debate on the "right to be forgotten" principle following the European Court of Justice Judgment in the Google Spain case[20].

The Council took note and welcomed the results and lessons learnt from the large scale law enforcement operation (Operation Archimedes) which took place between the 15 and 23 September 2014. The operation, which is to be seen as part of the EU policy cycle on serious and international organised crime, targeted organised crime groups and their infrastructures across the European Union (EU), with the cooperation of Eurojust, Frontex and Interpol. The intelligence-led operation saw the participation of law enforcement officers from all 28 EU Member States as well as Australia, Colombia, Norway, Serbia, Switzerland and the USA (ICE and CBP). During the operation, raids and other interventions took place in hundreds of locations including airports, land border-crossing points, ports and specific crime hot spots in towns and cities all of which had featured variously in Europol's Serious and Organised Crime Threat Assessment (SOCTA), criminal intelligence reports from EU member states and third countries and analytical products drawn from Europol's criminal databases. Some preliminary results are:

– 1 146 individuals arrested

– nearly 600 kg cocaine seized and 200 kg of heroin seized

– 1.8 tonnes of cannabis seized

– 200 potential victims saved from trafficking, of which 30 children.

[19] The next meeting of the Justice and Home Affairs Council under the Italian Presidency will take place on 4 and 5 December 2014, in Brussels.

[20] ECJ, Decisión C-131/12, on 13 May 2014, Google Spain SL, Google Inc. *v.* Agencia Española de Protección de Datos, Mario Costeja González.

The Court of Justice of the European Union will have a key role in implementing the Area of Freedom, Security and Justice Post-Lisbon. The European Union Council will explain it in three conferences in November 2014, April 2015 and September 2015[21].

2.2. Some aspects to be considered before building up the Legal CAPER Regulatory Model

We will follow the risk and solutions structure of a Privacy Impact Assessment (PIA) to describe the CAPER Regulatory Model (CRM). According to Wright and Raab, a PIA should include sixteen steps[22]:

1. Determine whether a PIA (or SIA) is necessary (threshold analysis).
2. Identify the PIA (or SIA) team and set the team's terms of reference, resources and time frame.
3. Prepare a PIA (or SIA) plan.
4. Determine the budget for the PIA (or SIA).
5. Describe the proposed project to be assessed.
6. Identify stakeholders.
7. Analyse the information flows and other impacts.
8. Consult with stakeholders.
9. Determine whether the project complies with legislation.
10. Identify risks and possible solutions.
11. Formulate recommendations.
12. Prepare and publish the report, e.g., on the organisation's website.
13. Implement the recommendations.
14. Ensure a third-party review and/or audit of the PIA (or SIA).
15. Update the PIA (or SIA) if there are changes in the project.
16. Embed privacy awareness throughout the organisation and ensure accountability.

[21] http://www.luiss.edu/sites/www.luiss.it/files/The_role_of_the_CJEU_ok3_REV.pdf .
[22] Wright, D., Raab, C.D. (2012), Constructing a surveillance impact assessment, *Computer Law & Security Review*, 28, 613-626.

However, the CAPER Regulatory Model (CRM) not only identifies the impacts of the project on data protection (like a PIA), but also addresses other kinds of impacts: legal and ethical. Another difference with PIA is that surveillance increasingly targets groups and populations, and not only concrete individuals. Indeed, PIA will also have to include Group Data Protection in the near future in order to become an efficient way of imposing safeguards.

3. LEGAL CAPER REGULATORY MODEL

3.1. Risk mitigation strategy

This section of the document contains the final recommendations from the point of view of the legal constraints that hard law instruments pose to the CAPER platform. In the **current** legislation we can find, as the two relevant legislative instruments: the *Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data* and the *Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*. The first one sets the **general** framework for the protection of personal data as it is nowadays, whereas the second one regulates, in a more **specific** manner, the processing of personal data in the field of police work in criminal issues.

Within the current process of **reform** of the Data Protection strategy of the UE we can find the Proposal for a *Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data* defined as the **General** Data Protection Strategy, as well as the *Proposal for a Directive 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*, again for the **specific** domain of police work in criminal matters.

The legal provisions contained in these four texts have been used to define a risk mitigation strategy that is explained in this section and represented in the tables that can be found at the end on paragraph 3 of this deliverable. In order to better explain the recommendations references to the flow of data within the Caper system, represented in the figure below will be made.

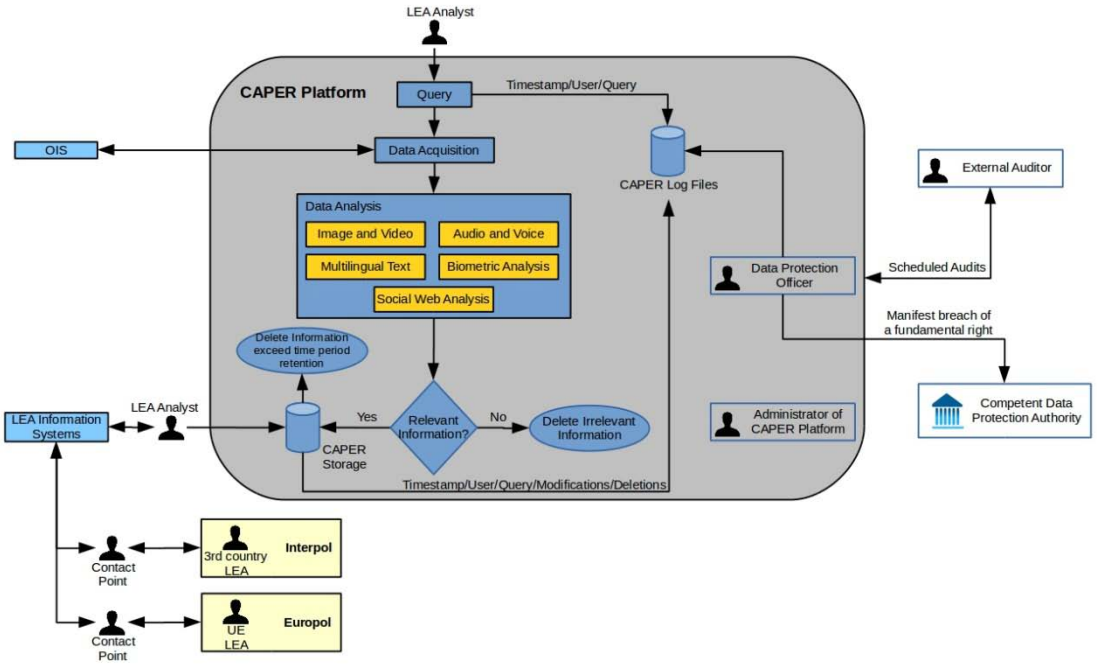


Figure: CAPER data flow

The general principles of the current Data Protection Directive are, firstly, applicable to the phase in which personal data are collected and stored. In relation to the principle of purpose and data minimization and to the duration of the retention period of personal data, the Data Protection Directive stipulates that personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" and they must be "kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed". The data protection principles expressed in this rules are therefore legally binding when capturing and storing personal data.

The regulation does not impose a concrete time period; nevertheless the Article 29th Working Party does not envisage a basis for a retention period beyond 6 months[23]. However, the retention of personal data and the corresponding retention period must always be justified (with concrete and relevant arguments) and reduced to a minimum, to improve transparency,

[23] Opinion 1/2008 on data protection issues related to search engines adopted on 4 April 2008.

to ensure fair processing, and to guarantee proportionality with the purpose that justifies such retention.

The regulation of the Data Protection at Eurojust and Europol can also provide crucial principles:

Article 21 Eurojust Council Decision:

Time limits for the storage of personal data

1. Personal data processed by Eurojust shall be stored by Eurojust for only as long as is necessary for the achievement of its objectives.

2. The personal data referred to in Article 14(1) which have been processed by Eurojust may not be stored beyond:

(a) the date on which prosecution is barred under the statute of limitations of all the Member States concerned by the investigation and prosecutions;

(b) the date on which the judicial decision of the last of the Member States concerned by the investigation or prosecutions which justified coordination by Eurojust became final;

(c) the date on which Eurojust and the Member States concerned mutually established or agreed that it was no longer necessary for Eurojust to coordinate the investigation and prosecutions.

3. (a) Observance of the storage periods referred to in paragraph 2 shall be reviewed constantly by appropriate automated processing. Nevertheless, a review of the need to store the data shall be carried out every three years after they were entered.

(b) When one of the storage deadlines referred to in paragraph 2 has expired, Eurojust shall review the need to store the data longer in order to enable it to achieve its objectives and it may decide by way of derogation to store those data until the following review.

(c) Where data has been stored by way of derogation pursuant to point (b) a review of the need to store those data shall take place every three years.

4. Where a file exists containing non-automated and unstructured data, once the deadline for storage of the last item of automated data from the file has elapsed all the documents in the file shall be returned to the authority which supplied them and any copies shall be destroyed.

5. Where Eurojust has coordinated an investigation or prosecutions, the national members concerned shall inform Eurojust and the other Member States concerned of all the judicial decisions relating to the case which have become final in order, inter alia, that paragraph 2(b) may be applied.

Article 20 of Council Decision of 6 April 2009, establishing the European Police Office (Europol) (2009/371/JHA).

Time limits for the storage and deletion of data

1. Europol shall hold data in data files only for as long as is necessary for the performance of its tasks. The need for continued storage shall be reviewed no later than three years after the input of data. Review of data stored in the Europol Information System and their deletion shall be carried out by the inputting unit. Review of data stored in other Europol data files and their deletion shall be carried out by Europol. Europol shall automatically inform the Member States three months in advance of the expiry of the time limits for reviewing the storage of data.

2. During the review, the units referred to in the third and fourth sentences of paragraph 1 may decide on the continued storage of data until the following review which shall take place after another period of three years if that is still necessary for the performance of Europol's tasks. If no decision is taken on the continued storage of data, those data shall be deleted automatically.

3. Where a Member State deletes from its national data files data communicated to Europol which are stored in other Europol data files, it shall inform Europol accordingly. In such cases, Europol shall delete the data unless it has further interest in them, based on intelligence that is more extensive than that possessed by the communicating Member State. Europol shall inform the Member State concerned of the continued storage of such data.

4. Such data shall not be deleted if this would damage the interests of a data subject who requires protection. In such cases, the data shall be used only with the consent of the data subject.

The principle of accountability set out in the proposal for a reform of the data protection framework, and defined by the Article 29 Working Party in the Opinion 3/2010 adopted on

the 13th of July 2010, requires technical solutions, such as Caper, to implement mechanisms that make it possible to verify who has access to the data and to ensure that only those users that need to have access (principle of necessity) are allowed to enter the data sets. Moreover these principles demand to keep a register of what data have been used, when and by whom. These legal requests are met with the recommendation of the establishment of a file log that registers all the activity by the different users, the queries, the results, timestamps, modifications and deletions of data that occur within the Caper platform. In order for this technical solution to work it is also necessary to set up a rigid access control to the platform. Explicit and detailed provisions with a list of profiles and concrete powers should be adopted. At the same time specific information on every user and the correlative profile should be kept in the log file and made available for the relevant supervisors.

Once it has been registered, that information needs to be available to the internal data protection supervisor (DPO) in order to make effective the principle of liability set out in Chapter VIII of the Proposal for a *Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data* and the Chapter VIII of the *Proposal for a Directive 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.*

In the same line of argumentation, the external supervisory authority should regularly check the use of the data collected and stored in the Caper platform. The recommendation is to perform an audit once a year. At the same time the DPO should be in contact regularly with the external supervisor and notify the competent authority in case of violation of the data protection legal requirements. The roles, within the Caper platform, of the internal, external and competent supervisors will be explained in section 4 of this document.

A critical issue that needs to be addressed in the definition of potential risks to personal data within Caper is that of the relationship between the data obtained and stored in Caper and the LEAs own information system. By its own nature the actions taken in the Caper

platform will deal with data of potentially vulnerable people like victims, witnesses and people whose data have been preemptively stored based on factual indications (possible criminals). This could be considered indiscriminate data storing not tolerated by the European Court of Human Rights[24]. When dealing with this kind o data LEAs generally need to take a step-by-step approach: access can only be permitted initially to only a few restrictive data, such as name, or date of birth and, if the search reveals a hit, further information could be provided later. The data once marked by the human expert as to maintain the label (victim, witness or possible criminal) and the step-by-step procedure. When data of victims or witness are interlinked with other personal data, particular supervision needs to be provided to assure that the status of the person concerned is not negatively influenced by the linking: a witness in an organised crime case and a person in a list to be refused entry to a country.

This scenario is not the one provided by the Caper platform as the distinction between suspects and non-suspects (vulnerable people) is not a direct issue for CAPER. Nonetheless, we remind this discussion in order to facilitate the LEA's processing of the data collected and stored in CAPER. Relevant data should be used only by authorized investigators. Criminal analysis and CAPER results must be clearly and carefully distinguished. No distinction between suspects and non-suspects should be automatically done by CAPER tools.

Once the data has been considered relevant by the human analyst it should be transferred to the LEAs information system where the data protection procedures set by the relevant authority and, independent from Caper, apply. If the data is deemed not relevant it should be erased. The information will be kept only on the log file for the purposes of supervision by the DPO and the external supervisor in the annual audits.

One element that needs to be specifically considerer due to the nature of the activities related to the Caper platform is that of the transfer of data or data exchange between different end users, in this case, LEAs. Regarding this point two scenarios need to be distinguished. The first one is that related to the data collected and stored in the Caper platform, that is, the access that a different user from the same LEAs, or even a user from a different LEA can

[24] *S. and Marper v. The United Kingdom*, Application nos. 30562/04 and 30566, Judgment of 4 December 2008..

have, to the results of a concrete query stored by the platform. The principle of purpose stated before applies one more time therefore the recommendation needs to be that only in case that, due to a concrete investigation, another user, with the same privileges, needs to have access to the same data, that access can be allowed. No access should be granted to allow general searches on that data when the purpose is not specifically stated.

The second scenario instead refers to the transfer of data originated in Caper, after it has been treated by the human analyst, transferred to that LEA information system (see Fig.) and therefore cross referred with other information, even with data originated form closed sources legally obtained by the LEA. In those cases it is clear that data cannot be transferred trough the Caper platform and that the LEA should refer to the applicant framework for police cooperation such as Europol or Interpol (see Fig.)

Finally the right of access needs to be considered. Information, access, rectification and deletion rights could be partially accepted in some cases without jeopardizing the investigations. LEAs should have the first decision on this issue because they know the possible risks of a disclosure of information better than anyone. The reasons of the decision of denying access and other rights should be preserved and ready for a double-check examination by the DPO or the competent authority, even a court in certain cases. If someone exercises the right to access, it is enough to notify the applicant that some checking has been carried out, without any information which could reveal whether or not the applicant is known. Nonetheless, the reasons for denying access to some people should be internally preserved in case a Judge asks for them. In the Judgment of 25 November 2010 in Case 277/10AJ, K v. Eurojust, the General Court of the European Union evaluated very positively the fact that Eurojust provided the individual with information that no personal data on him had been processed.

Perhaps the Eurojust legal framework could here help:

Article 19 Right of access to personal data

1. Every individual shall be entitled to have access to personal data concerning him processed by Eurojust under the conditions laid down in this Article.

2. Any individual wishing to exercise his right to have access to data concerning him which are stored at Eurojust, or to have them checked in accordance with Article 20, may make a request to that effect free of charge in the Member State of his choice, to the authority appointed for that purpose in that Member State, and that authority shall refer it to Eurojust without delay.

3. The right of any individual to have access to personal data concerning him or to have them checked shall be exercised in accordance with the laws and procedures of the Member State in which the individual has made his request. If, however, Eurojust can ascertain which authority in a State transmitted the data in question, that authority may require that the right of access be exercised in accordance with the rules of the law of that Member State.

4. Access to personal data shall be denied if:

(a) such access may jeopardise one of Eurojust's activities;

(b) such access may jeopardise any national investigation which Eurojust is assisting;

(c) such access may jeopardise the rights and freedoms of third parties.

5. The decision to grant this right of access shall take due account of the status, with regard to the data stored by Eurojust, of those individuals submitting the request.

6. The national members concerned by the request shall deal with it and reach a decision on Eurojust's behalf. The request shall be dealt with in full within three months of receipt. Where the members are not in agreement, they shall refer the matter to the College, which shall take its decision on the request by a two-thirds majority.

7. If access is denied or if no personal data concerning the applicant are processed by Eurojust, the latter shall notify the applicant that it has carried out checks, without giving any information which could reveal whether or not the applicant is known.

8. If the applicant is not satisfied with the reply given to his request, he may appeal against that decision before the joint supervisory body. The joint supervisory body shall examine whether or not the decision taken by Eurojust is in conformity with this Decision.

9. The competent law enforcement authorities of the Member States shall be consulted by Eurojust before a decision is taken. They shall subsequently be notified of its contents through the national members concerned.

3.2. CAPER regulatory model tables

3.2.2. CAPER Data Collection and Storage

Item 1 CAPER Data Collection and Storage			
Current legal basis	**Reform** of the legal basis (Proposal for the reform of data protection)	Risk	Recommendation
General: NO **Specific**: NO	**General**: Art.22.2.c; Art.33 **Specific**: NO	No concrete Data Protection Impact Assessment done by the LEAs	• Every LEA should perform a concrete Data Protection Impact Assessment according to the general framework offered by the CAPER Regulatory Model.
General: Art.6.b **Specific**: Art.3.1	**General**: Art.5.b.c; General Provisions (13) **Specific**: Art.4.b.c	CAPER Data used for ordinary criminal investigations	• Data collected and stored by CAPER must only be used for fighting organized crime • The storage of data collected by CAPER should be implemented in a separate repository. No contact with ordinary criminal data bases should be allowed.
General: Art.15 **Specific**: Art.7	**General**: General Provisions (13); Art.20 **Specific**: Art.9	Labelling from CAPER Data considered as an evidence	• No automated classification of suspects, victims and witnesses can be inferred from CAPER results. • Caper does not label individuals or groups as suspects, victims and witnesses. This labelling is performed by a human analyst. Lately, an information management process should determine how the data is transferred to the LEAs

			Information Systems (see Fig). • No automatic decision should substitute the police analysis by human experts.
General: Art.6.c **Specific**: Art.4.2; Art.5	**General**: Art.17.b **Specific**: Art.4.d	CAPER Data unlimited storage	• Time retention periods should be linked with the relevancy of the data, "no reason for storing irrelevant data or data that has become irrelevant" should be the rule. • Data not relevant/needed in any investigation should be erased. • There should be an automated tool detecting the end of the retention period and informing the competent LEA or controller so that they can take action if the data is still relevant /needed.
General: Art.17 **Specific**: Art.22	**General**: Art.22; Art.30 **Specific**: Art.24	CAPER Data queries and results not available for monitoring and auditing	• The CAPER data management system deletes all the results when the search is already finished. All queries and results should be kept, in a log file (see Fig.) ,available for the control by the internal and external CAPER data supervisors
General: NO **Specific**: NO	**General**: Art.22.3; Art.26 **Specific**: Art.18.3	CAPER tool use never audited	• Regular audits of the CAPER system should be performed by the external CAPER supervisor.

3.2.3. CAPER Data Management

Item 2 CAPER Data management			
Current legal basis	**Reform** of the legal basis (Proposal for the reform of data protection)	Risk	Recommendation
General:Art.17 **Specific**: Art.22	**General**:Art.22; Art.30 **Specific**: Art.24	Unauthorized access	• Explicit and detailed provisions with a list of detailed profiles and specific powers should be adopted. • Specific information on every user and the correlative profile should be kept in the log file and made available for the relevant supervisors. • Access to CAPER database should be granted for the purpose of prevention, detection or investigation of organised crime. • Any other request of access for other purposes should be rejected. • Non-authorised LEAs and administrative bodies of the authorised LEAs should not have access to data collected and stored by CAPER.
General: Art.17 **Specific**: Art.22	**General**: Art.22; Art.30 **Specific**: Art.24	Unauthorized use and modification	• The use of system integrity tools should enable detection and reporting of changes applied on servers. In case of such an event the system should be able to notify specific users such as the creator of the query which results have been modified. • Regular audits of the CAPER system should be performed by

			the external supervisor. The competent authority should be informed of the results, if necessary according to national legislation, including the plans for enforcing recommendations.
General: Art.6.d **Specific**: Art.4.2	**General**: Art.5.d **Specific**: Art.16	CAPER Data not properly erased	• A specific procedure for the secure deletion of personal data within CAPER.

3.2.4. CAPER Data Reuse and Transfer

Item 3 CAPER Data Reuse and transfer			
Current legal basis	**Reform** of the legal basis (Proposal for the reform of data protection)	Risk	Recommendation
General: Art.25 **Specific**: Art.11	**General**: Art.40; Art.41: Art.42 **Specific**: Art.33; Art.34; Art.35	Transfer of data obtained trough CAPER	• In cases when data related to a criminal investigation which is not OSINT-based, needs to be transfer to another LEA it should be done trough the existing institutional channels and not trough the CAPER platform.
General: Art.15 **Specific**: Art.7	**General**: General Provisions (13); Art.20 **Specific**: Art.9	CAPER Data transferred to existing internal databases	• No automated classification of suspects, victims and witnesses can be inferred from CAPER results. • Caper does not label individuals or groups as suspects, victims and witnesses. This labelling is performed by a human analyst. Lately, an information

			management process should determine how the data is transferred to the LEAs Information Systems (see Fig). • Data should be transferred to already existing databases subject to their own Data Protection regulations.

3.2.5. CAPER Data Access Right

Item 4 CAPER Data Access Right			
Current Legal Basis	**Reform** of the legal basis (Proposal for the reform of data protection)	Risk	Recommendation
General: Art.12 **Specific**: Art.17.2	**General**: Art.15 **Specific**: Art.12	CAPER tool procedure and data results never available	• Individuals should have the possibility to contact the internal or external supervisor to support them in exercising their access right.
General: Art.13 **Specific**: Art.17.2	**General**: Art.21 **Specific**: 13	Access requests always denied	• The reasons to deny access should be clear and defined. Access can be denied when the access may jeopardise the fulfilment of the LEA tasks, or the rights and freedoms of third parties.
General: Art.28 **Specific**: Art.25	**General**: Art.46; Art.51; Art.52 **Specific**:	Denial of access never monitored	• The alleged to deny access should be open to external supervision. The external supervisory authority should have the possibility to access the

	Art.25		documents justifying the refusal. A short time-span of three months (for instance) to reply to an access should be implemented.

4. INTERNAL AND EXTERNAL SUPERVISION WITHIN CAPER

In order to ensure that the use of the Caper platform fulfils all the legal requirements set out in the previous sections of this document the recommendation is, in line with the European Data Protection regulation reform proposal, the establishment of a control system in two phases: internal and external.

4.1. Internal Supervisor

The figure of the Data Protection Officer (DPO) is well known in the field of Justice and Security in Europe, as all European Agencies dealing with the processing of personal data in criminal matter have such a role within their organizational structure. We will examine both the Data protection Officer at Eurojust and at Europol in order to extract the main features- appointment, requirements, role, and powers- and recommend the appointment of such a figure in the context of the Caper platform. The proposal for a *Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data* dictated the obligation of appointing such a figure in some cases.

Article 35
Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

   (a) the processing is carried out by a public authority or body; or

   (b) the processing is carried out by an enterprise employing 250 persons or more; or

   (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

Since by its own nature Caper envisages controllers and processors that fall within the letters a) and c) in case the proposal enters into force the appointment of a DPO will be mandatory, thus reinforcing the justification of such a recommendation.

We will next examine the figure of the DPO in the context of Eurojust and Europol.

4.1.1. Data Protection Officer (DPO) at Eurojust

According to Article 17 of Council Decision of 28 February 2002, those are the Eurojust DPO tasks[25]:

Article 17

Data Protection Officer

1. Eurojust shall have a specially appointed Data Protection Officer, who shall be a member of the staff. Within that framework, he shall be under the direct authority of the College. In the performance of the duties referred to in this Article, he shall take instructions from no-one.

2. The Data Protection Officer shall in particular have the following tasks:

(a) ensuring, in an independent manner, lawfulness and compliance with the provisions of this Decision concerning the processing of personal data;

(b) ensuring that a written record of the transmission and receipt, for the purposes of Article 19(3) in particular, of personal data is kept in accordance with the provisions to

be laid down in the rules of procedure, under the security conditions laid down in Article 22;

(c) ensuring that data subjects are informed of their rights under this Decision at their request.

[25] Council Decision of 28 February 2002, setting up Eurojust with a view to reinforcing the fight against serious crime, available at http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejdecision/Eurojust%20Decision%20%28Council%20Decision%202002-187-JHA%29/Eurojust-Council-Decision-2002-187-JHA-EN.pdf .

3. *In the performance of his tasks, the Officer shall have access to all the data processed by Eurojust and to all Eurojust premises.*
4. *When he finds that in his view processing has not complied with this Decision, the Officer shall:*

(a) inform the College, which shall acknowledge receipt of the information;

(b) refer the matter to the joint supervisory body if the College has not resolved the non-compliance of the processing within a reasonable time.

The key aspects of the institution are:

- The DPO is a member of the staff. In CAPER, the DPO should then be appointed by the data controller.
- He shall be under a direct authority of a concrete institution. In the performance of his duties, he should follow instructions from no one.
- He should ensure, in an independent manner, the compliance with the legal framework. In CAPER, he should ensure the compliance with the CAPER Regulatory Model.
- He should ensure that a written record of transmission and receipt of personal data is kept, according to the rules of procedure and under security conditions. In CAPER, he should ensure that the file log is kept.
- He should ensure that data subjects are informed of their rights at their request. In CAPER, individuals should have the possibility to contact the internal supervisor to support them in exercising their access right.
- To support these tasks, the DPO shall have access to all the data processed by Eurojust. In CAPER, he should have access to the file log.
- When he finds that the processing does not comply with the Council Decision, he shall inform the College and refer the matter to the joint Supervisory body. In CAPER, whenever he finds that the processing does not comply with the CAPER Regulatory Model, he should inform the data controller in order to correct the situation and, in case of manifest breach of a fundamental right notify the competent data protection authority.

4.1.2. Data Protection Officer (DPO) at Europol

Article 28 of the Europol Council Decision

Data Protection Officer

1. The Management Board shall appoint, on the proposal of the Director, a Data Protection Officer who shall be a member of the staff. In the performance of his or her duties, he or she shall act independently.

2. The Data Protection Officer shall in particular have the following tasks:

(a) ensuring, in an independent manner, lawfulness and compliance with the provisions of this Decision concerning the processing of personal data, including the processing of personal data relating to Europol staff;

(b) ensuring that a written record of the transmission and receipt of personal data is kept in accordance with this Decision;

(c) ensuring that data subjects are informed of their rights under this Decision at their request;

(d) cooperating with Europol staff responsible for procedures, training and advice on data processing;

(e) cooperating with the Joint Supervisory Body;

(f) preparing an annual report and communicating that report to the Management Board and to the Joint Supervisory Body.

3. In the performance of his or her tasks, the Data Protection Officer shall have access to all the data processed by Europol and to all Europol premises.

This experiences are reflected as well in articles 30 and following of the *Proposal for a Directive 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*

that envisages the procedure for the designation of a DPO, the position of the DPO and the main task assigned to him/her.

SECTION 3
DATA PROTECTION OFFICER

Article 30

Designation of the data protection officer

1. Member States shall provide that the controller or the processor designates a data protection officer.

2. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 32.

3. The data protection officer may be designated for several entities, taking account of the organisational structure of the competent authority.

Article 31

Position of the data protection officer

1. Member States shall provide that the controller or the processor ensures that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. The controller or processor shall ensure that the data protection officer is provided with the means to perform duties and tasks referred to under Article 32 effectively and independently, and does not receive any instructions as regards the exercise of the function.

Article 32

Tasks of the data protection officer

Member States shall provide that the controller or the processor entrusts the data protection officer at least with the following tasks:

(a) to inform and advise the controller or the processor of their obligations in accordance with the provisions adopted pursuant to this Directive and to document this activity and the responses received;

(b) to monitor the implementation and application of the policies in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations and the related audits;

(c) to monitor the implementation and application of the provisions adopted pursuant to this Directive, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under the provisions adopted pursuant to this Directive;

(d) to ensure that the documentation referred to in Article 23 is maintained;

(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 28 and 29;

(f) to monitor the application for prior consultation to the supervisory authority, if required pursuant to Article 26;

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on his own initiative;

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on the data protection officer's own initiative.

4.2. External Supervisor

The internal control in not enough in a case where there are risks to the protection of personal data of citizens. This idea is clear also in the case of the European Agencies in the field of criminal matters, and therefore they are monitored by a Joint Supervisory Body. We will therefore examine the Joint Supervisory Body role at Eurojust and at Europol. What is

relevant is to define its role in order to identify the key elements that an external supervisor must follow.

4.2.1. Joint Supervisory Body at Eurojust

According to article 23 of the Eurojust Council Decision:

(…) *7. The Joint Supervisory Body shall examine appeals submitted to it in accordance with Article 19(8) and Article 20(2) and carry out controls in accordance with paragraph 1, first subparagraph, of this Article. If the Joint Supervisory Body considers that a decision taken by Eurojust or the processing of data by it is not compatible with this Decision, the matter shall be referred to Eurojust, which shall accept the decision of the Joint Supervisory Body.*

8. Decisions of the Joint Supervisory Body shall be final and binding on Eurojust.

9. The persons appointed by the Member States in accordance with paragraph 1, third subparagraph, presided over by the chairman of the Joint Supervisory Body, shall adopt internal rules of procedure which, for the purpose of the examination of appeals, lay down objective criteria for the appointment of the Body's members.

10. Secretariat costs shall be borne by the Eurojust budget.

The secretariat of the Joint Supervisory Body shall enjoy independence in the discharge of its function within the Eurojust secretariat.

11. The members of the Joint Supervisory Body shall be subject to the obligation of confidentiality laid down in Article 25.

12. The Joint Supervisory Body shall submit an annual report to the Council.

The decisions of the Joint Supervisory Body of Eurojust contain very valuable indications in regard of some of the key issues in data protection such as the right of access. For instance, regarding the appeal filed on behalf of Mr T, some interesting considerations were made:

- The decision of Eurojust related to the request of Mr T of 11 January 2011 concerning access to any personal data on him processed by Eurojust, deletion of

such data, undertaking not to further process any data on him and notification on the same subject to any relevant third party.

- The decision of Eurojust, as communicated to the applicant by the DPO of Eurojust, was worded as follows:
- In accordance with Article 19.7 of the Eurojust Decision, I hereby notify you that checks have been carried out, but I am unable to give any information which could reveal whether or not your client is known.

The key arguments held in the Decision are:

However, as the JSB already stated in its decision of 26 April 2007 in the S case, a systematic application of Article 19.7 without further examination of the specific details of the individual cases might lead in practice to a systematic denial of the rights of the individuals. As already stated in the S decision, the Joint Supervisory Body of Eurojust considers that in all cases where an individual seeks access to personal data concerning him processed by Eurojust, including those cases where there are no data processed, the College of Eurojust shall decide whether in the specific case the disclosure of the data or of the non-existence of data concerning the applicant processed by Eurojust may contravene any interests of Eurojust or of one of the Member States. If this is not the case, Eurojust shall reveal to the individual the requested data or inform him that in fact there are no data concerning him.

The decision of the JSB in the S case has been recently confirmed by the European Court of Justice in the case T - 277/10 AJ, K v Eurojust.

(…) In the specific case, the JSB welcomes the fact that the College of Eurojust considered the request of Mr T at its plenary meeting of 17 February 2011 and that a thorough discussion took place regarding all aspects of the specific case at stake, as stated in the written observations provided by Mr Williams on the 31 March 2011. It is regrettably however that the decision of Eurojust does not seem to take account of the interests at stake in this case or of the impact for the data subject of the mere provision of a standard answer. Neither the reply of Eurojust to the data subject nor the written observations submitted to the JSB contain any consideration as to how the disclosure of the data or of the non - existence of

data concerning the applicant processed by Eurojust may contravene any interests of Eurojust or of one of the Member States.

The Decision is thus:

In the light of the specific circumstances and complexity of the case as well as of the big interest at stake for the data subject, who has been de facto enied the possibility to exercise his rights, as guaranteed by articles 19 and 20 of the Eurojust Decision, by the provision of the standard answer by Eurojust, and, in the absence of any evidence that Eurojust could suffer any harm by providing the individual a clear and unambiguous answer, the JSB decides, in accordance with Article 23.7 of the Eurojust Decision, to refer the matter to Eurojust for reconsideration.

Eurojust is required, in line with Article 23.8 of the Eurojust Decision, to provide Mr T a clear and unambiguous answer as to the fact that no personal data on him are processed by Eurojust and to clarify that, therefore, there is no object for the exercise of any other of the rights invoked by the individual.

Two case-related appeals were received by the Eurojust Joint Supervisory Board in 2013. The second one received on the 25th June deals with some relevant issues for our project. Following to the Applicants' request of 10 April to access personal data processed by Eurojust relating to them, a decision of Eurojust stated:

In accordance with Article 19(7) of the Eurojust Decision, I hereby notify you that the necessary checks have been carried out, but I am unable to give you any information which could reveal whether or not your clients are known to Eurojust.

The Joint Supervisory Board concluded in November 2013 that:

That the JSB is of the opinion, that Eurojust correctly redacted certain parts of the content by removing the names of the other persons mentioned in the documents for the purpose of protecting their right to privacy. The JSB notes that according to Article 19(1) of the Eurojust. Decision an individual is entitled to have access to data concerning him processed

by Eurojust[..]. Therefore, the applicants were entitled to receive any data concerning them individually".

In the light of the specific circumstances and the fact that the applicant was provided with full access to information concerning him, processed by Eurojust, that by redacting the names of other persons Eurojust protected their right to privacy, the JSB decides, in accordance with Article 23.7 of the Eurojust Decision, that in the present appeal case Eurojust correctly applied the provisions of the Eurojust Decision.

4.2.2. Joint Supervisory Body at Europol

Article 34 of the Europol Council Decision:

Joint Supervisory Body

1. An independent Joint Supervisory Body shall be set up to review, in accordance with this Decision, the activities of Europol in order to ensure that the rights of the individual are not violated by the storage, processing and use of the data held by Europol. In addition, the Joint Supervisory Body shall monitor the permissibility of the transmission of data originating from Europol. The Joint Supervisory Body shall be composed of a maximum of two members or representatives, where appropriate assisted by alternates, of each of the independent national supervisory bodies, having the necessary abilities and appointed for five years by each Member State. Each delegation shall be entitled to one vote. The Joint Supervisory Body shall choose a chairman from among its members. In the performance of their duties, the members of the Joint Supervisory Body shall not receive instructions from any other body.

2. Europol shall assist the Joint Supervisory Body in the performance of the latter's tasks. In doing so, it shall in particular:

(a) supply the information the Joint Supervisory Body requests and give it access to all documents and paper files as well as to the data stored in its data files;

(b) allow the Joint Supervisory Body free access at all times to all its premises;

(c) implement the Joint Supervisory Body's decisions on appeals.

3. The Joint Supervisory Body shall be competent to examine questions relating to implementation and interpretation in connection with Europol's activities as regards the processing and use of personal data, to examine questions relating to checks carried out independently by the national supervisory bodies of the Member States or relating to the exercise of the right of access, and to draw up harmonised proposals for common solutions to existing problems.

4. If the Joint Supervisory Body identifies any violations of the provisions of this Decision in the storage, processing or use of personal data, it shall make any complaints it deems necessary to the Director and shall request him to reply within a specified time limit. The Director shall keep the Management Board informed of the entire procedure. If it is not satisfied with the response given by the Director to its request, the Joint Supervisory Body shall refer the matter to the Management Board.

5. For the fulfilment of its tasks and to contribute to the improvement of consistency in the application of the rules and procedures for data processing, the Joint Supervisory Body shall cooperate as necessary with other supervisory authorities.

An interesting Report on data processing in Europol's Information System contains guidelines for Europol National Units[26]. The Recommendations are:

i) Criteria should be developed for assessing whether data to be inputted into the EIS relate to crimes for which Europol is competent and comply with the provisions on which data may be inputted into the EIS.

ii) These criteria should also include the criteria already agreed upon between Europol and the JSB in respect of processing data on minors, persons related to trafficking in human beings and persons who are member of an organisation which is considered to be a criminal organisation in only some Member States.

iii) Europol and the Heads of the ENUs should develop these rules as soon as possible. The JSB needs to be involved in this process.

[26] Report 12/61, on the conditions for Europol National Units in relation to data processing in Europol's Information System, available at http://europoljsb.consilium.europa.eu/media/257488/12-61%20rev%2007%20final%20report%20survey%20national%20units.pdf , 23/07/2013.

iv) On national level procedures should be developed ensuring that the inputting authority is informed when proceedings are dropped or the person involved is acquitted.

v) The national data protection authorities, the JSB and Europol should closely monitor the proper implementation of these rules in the procedures and data processing in the Member States.

In the Fifth Activity Report of the Joint Supervisory Body at Europol for the period 2008-2012, some interesting information is available[27]:

In the period covered by this report, the committee handled five appeals. Of the five decisions taken by the committee, one concluded that Europol's decision was in compliance with the legal basis; and three concluded that Europol's decision was not in compliance with the legal basis. In these three cases, Europol revised its decision in line with the decision of the committee. In one case, Europol reconsidered its decision during the appeals procedure; in view of the outcome, the appeals procedure was stopped.

One recent Appeal can illustrate how the access right has build up[28]: The case illustrated relates to a request for access from a Spanish Citizen to Europol based on Article 19 of the Europol Convention. On 29 March 2010, Europol decided on the request of Mr. A:

In accordance with the procedure stipulated in the Council Decision of 6 April 2009 establishing the European Police Office (Europol,) I would like to inform you that following your request checks of Europol files have been made. Following Article 30 of the Europol Council Decision, I would like to inform you that no data concerning you are processed at Europol to which you would be entitled to have access to in accordance with Article 30 of the Europol Council Decision.

The facts are:

[27] Activity Report of the Joint Supervisory Body at Europol (2008-2012), 09/04/2013.
[28] JSB Europol, Appeals Committee, Appeal of Mr. A, no. 10/02, 14/03/2012.

Mr. A. stated that he is in preventive custody and that criminal proceedings against him are before the Audiencia Nacional de Madrid (National High Court). In those proceedings, there is a report of the Spanish police dated, 4 December 2007 in which an official mentions that following consultation of Europol, the French police have two records on him. This information is, according to Mr. A ., false.

In its observations of 20 July 2010, Europol explained that it consulted the Spanish national competent authority. That authority informed Europol that, "regarding the access request of the data subject, the requested information must not be provided to this individual, neither in a positive, nor in a negative way". According to Europol, the consulted Spanish authorities furthermore stated that since this was an "organised crime" investigation, the Spanish law for Personal Data Protection is not applied with reference to an exemption in that law (Article 2.2 sub c) that the law is not applied to files established for the investigation of terrorism and other forms of serious organised criminality.

In view of the comments made by the competent Spanish authorities, Europol took the decision not to communicate any information to Mr. A. by applying the following two exemptions contained in Article 30(5) of the Europol Council Decision: i) to enable Decision on the appeal of Mr. A. Europol to fulfil its tasks properly and ii) to protect security and public order in the Member State or to prevent crime.

In additional provided information of 8 August 2011, Europol explained that after consulting the relevant Member State and asking whether they have any objection to the communication of data, and following scrutiny of the information received, Europol carefully considered whether the operational and legal arguments of the Member State justified the application of one or more of the exemptions as listed under Article 30(5) of the Europol Council Decision.

The key arguments on the case are:

The first reason presented is the gravity of the charges against the appellant. The appellant is believed to be involved in serious crimes. The Appeals Committee notes that the gravity of charges against a person are as such not a justified reason for refusing communications. Furthermore, when a person is formally charged by judicial authorities, he/she is informed

about the content of the accusations. Since the appellant is already charged and detained for many years, he will be aware of the content of the charges, including the facts he is suspected of having committed. The mere statement that the appellant is suspected of being a member of a criminal group is, in combination with the charges brought against him, too abstract a reason and, as such, insufficient to justify the refusal of the right of access.

The second reason presented is the ongoing investigations. Whether informing an individual suspected of being involved in crime that data on him/her are processed and - when data are processed - to communicate those data, will effectively undermine

Decision on the appeal of Mr. A. investigations, is dependent on various factors such as the data processed and specific elements of the investigation. This may include: the different investigation phases – from initial suspicion till further investigations while the suspect is already charged and detained; the investigation strategies; the information position of the police authorities; gathering intelligence; information gathering methods used; and which involved police authorities. If it is deemed necessary to protect these investigation aspects by refusing the communication of data to a data subject who is object of these investigations, it is necessary to determine whether the communication can effectively undermine the investigation. The type of data, the investigation phase, and the specific situation of a data subject, will play a relevant role in this. When a person is suspected and investigated he might not be aware of this police-interest and this may be an important aspect in determining whether any communication could effectively undermine the investigation. If a person is already arrested, and detained for a long period, he is aware of the police interest and of the grounds for his arrest and detainment. In this situation, communication of data concerning the data subject's arrest and the object of suspicion cannot be determined as effectively undermining the interests of the investigation.

The third reason presented is that the case against Mr. A. is sub judice and that until there is a formal court hearing, the judicial authorities may ask police authorities to carry out any investigations. The effectiveness of such investigations could be endangered by any communication to the appellant whether data concerning him are processed by Europol. The Appeals Committee notes that the mere fact that a case is sub judice is not an aspect that is protected by one of the exemptions of Article 30(5) (a and b). This could only be different if

new investigations to the appellant are foreseeable and that it can be determined that the effectiveness of these investigations could be undermined. In the observations and additional comments from Europol, taking into account the specific situations of Mr. A., no such indications are given.

The Decision is then:

Based on the considerations of the Appeals Committee on the operational reasons to refuse access as presented by Europol and the results of the investigation at Europol on 26 July 2010, and after careful evaluation of the available information, the Appeals Committee concludes that Europol's reasons for refusing access in this case, whether considered separately or combined, cannot justify the refusal to communicate to Mr. A. whether any data concerning him are processed and if so, to communicate this data to him, based on the exemptions referred to in Article 30(5) of the Europol Council Decision.

(…) *In accordance with the provisions in Article 32(3) of the Europol Council Decision, the Appeals Committee decides that Europol should have communicated to Mr. A. that Europol processes data stating the suspicion of his involvement with drugs trafficking, being facts for which Mr A. is presently charged and detained.*

The idea of an external supervisory authority is also foreseen in the proposal for the reform of the data protection legislation in the European Union. To be more precise is contained in Chapter VI of the *Proposal for a Directive 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.*

5. SYSTEMS REVIEW AND VALIDATION

5.1. New Recommendations after CAPER tool version 4 release June 2014

The CAPER tool version 4, released just before the June 2014 CAPER Workshop at San Sebastian, included new capabilities. None of them was relevant for the CAPER Regulatory Model except one that needs a new and *ad hoc* regulation.

Version 4 of the platform includes in fact a link to already existing LEAs information systems. This means that CAPER queries can be launched to data coming from police databases. The implementation of this functionality raises concerns due to the fact that, as explained in the risk mitigation strategy, in section 3 we have clearly distinguish between data obtained and stored in CAPER and data contained in LEAs information systems (see Fig.). The Caper Regulatory Model has been defined in relation to open source information, in other words, is data obtained in sources that are generally open. And it has been defined in relation to the Caper platform architecture. There is, therefore a problem, when data previously collected by the LEAs under a different framework is treated by the platform. This should not be the case, and if this functionality is used, complementary safeguards should be defined, only for those situations. Some possibility will be to implement measures such as the ones envisaged in Article 26 of the *Rules of procedure on the processing and protection of personal data at Eurojust* (text adopted unanimously by the college of Eurojust during the meeting of 21 October 2004 and approved by the council on 24 February 2005) (2005/c 68/01).

Automated case management system

1. Eurojust shall put in place an automated case management system integrating a filing system, that shall be used by the National Members when dealing with case-related activities and which shall include the temporary work files and index as defined in Article 16 of the

Eurojust Decision. This system shall include functionalities such as case management, description of the workflow, cross-references of information and security.

2. The case management system shall be approved by the College after having consulted the Data Protection Officer, the Joint Supervisory Body and the relevant Eurojust staff and shall take full account of the requirements of Article 22 and any other relevant provisions of the Eurojust Decision.

3. The case management system shall enable National Members to identify the purpose and specific objectives for which a temporary work file is opened, within the framework of the tasks mentioned in Articles 5, 6 and 7 of the Eurojust Decision.

5.2. Paris CAPER Workshop November 2013

In our first Workshop (programme in Annex1) with experts in the field of Data Protection coming from European agencies such as Eurojust and Europol, and national ones such as the Spanish National Data Protection Agency (AEPD), our goal was to present not only our concrete Legal recommendations for CAPER, but also envisioned Ethical concerns and solutions. This option forced to include a big number of speakers, with heterogeneous backgrounds.

The results of the Workshop were very interesting and gave us some crucial feedback as well as important indications of data protection and ethical risks and recommendations for CAPER on several aspects such as:

a) From the Purpose perspective:

- Caper should be used only for organised crime.
- Multipurpose and preventive search are new risks: Intelligence units work more and more on networks, not on individuals.
- Data minimisation/ principle of purpose? With Big Data and data mining, these principles are at risk.

b) From the Storage perspective:

- The Caper repository should not be linked to other databases.
- Access should be limited to the human experts.
- Non-relevant data should be erased whereas relevant should be data sent to already existing databases.

c) From the Data information Management perspective:

- Data is not analyzed by a criminal human expert within CAPER.
- The indication of labels such as suspects, victims, witnesses cannot be utomatically inferred from CAPER.
- Analyzed data should be labelled and sent to other databases

Nonetheless, it was clear that a new meeting was needed in order to address in a more concrete way the risk scenarios and ad hoc solutions that could occur within the Caper platform. Thus a second Workshop was organised, in May 2014.

5.3. Barcelona CAPER Workshop May 2014

The Barcelona CAPER Workshop on Data Protection and Security Issues: the CAPER Model, on 16th May 2014, was an opportunity to check whether the CAPER Regulatory Model could be acceptable for National Data Protection Agencies and Eurojust and Europol Data Protection Officers (programme in Annex 2). This was the second time the legal and ethical work done during the project was to such experts, after the November 2013 Paris Workshop.

Key aspects discussed:

Within the CAPER platform there is not anonymisation. This raised some concern in the Paris Workshop, because usually anonymisation is the preferred Data Protection Enhanced Technology for lawyers and Data Protection Agencies and Officers. In the Barcelona Workshop, on the contrary, the focus was set on the discussion on procedural safeguards like file logs, access permits and privileges, and internal and external supervision frameworks.

Some problems were still to be solved:

a) CAPER tool should not erase CAPER data results after a query, but keep them in the file log and made available for the internal and external supervisors (see below chapter 5.1.1).

b) CAPER Data is supposed to be only "filtered" Raw Data, but indeed CAPER e-discovery capabilities give the tool an analyst-like expertise (see below chapter 5.1.2).

5.3.1. CAPER query and results log for internal and external supervision.

Data Protection experts suggested the need for a query and results automatic saving capability, in order to have logs and data always available. This suggestion was made to the engineers. Their first reaction was to consider CAPER tool as a prototype. This is true, according to the Project, but we insisted in giving the prototype this capability. Obviously, the concrete Data Protection internal and external supervisors will be appointed afterwards by each data controller.

This is a concrete application of the data protection by default and data protection by design principles. Ann Cavoukian's concept of "Privacy by Design" (PbD) was first developed in the 90s (Cavoukian, 2009). At that time, the regulatory approach was dominant. PbD tries to capture the notion of embedding privacy into the technology itself. We should thus settle privacy in the application by default. Moreover, if we combine PET and privacy

preserving procedures, we could obtain a general privacy protective architecture. In fact, one of the most common difficulties of the generalization of PET is that they are usually built as "privacy packs": we have to add them to an already running application, or as an external limit to it. As a result, there is an added cost and sometimes even some incompatibilities. Obviously, these problems don't favour the promotion of PET. Perhaps these are the reasons why, despite 15 years of research in PET, we still do not find PET in the markets. PbD is a principle for fuelling PET. Without a general rule in favour of PbD, no general implementation of PET will take place. The privacy-preserving technology is there, waiting for its opportunity to proof its worthy benefits. What we need now is a political option for privacy in a democracy society.

But we do not only need in this case traditional PET: cryptography, anonymizers, and access and identity management. What is rather suggested is a procedural PET, a necessary log saving for audits. To understand exactly the role of the concrete procedural PET here suggested, we need to describe the evolution of traditional PET.

In 1995, in a paper of the Information and Privacy Commissioner of Ontario (IPC) with the Netherlands Data Protection Authority, the term "PET" was coined (IPC, 1995). At this time, PET were tools for the exclusive use of individuals, like e-mail and file encryption, anonymizers and password managers (Cavoukian, 2009). We call these tools "traditional PET" in this book. The Internet Standards Organization (ISO) has at least achieved consensus on four components of privacy –and of traditional PET-:

- Anonymity ensures that a subject may use a resource or service without disclosing user identity.
- Pseudonymity ensures that a user may use a resource or service without disclosing identity, but can still be accountable for that use.
- Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
- Unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that we use the resource or service.

General Privacy Enhancing technologies, like anonymity, pseudonymity, and access management are useful for surfing Internet. But an access control management and a proper processing of data are not the whole problem. We shouldn't however abandon anonymity and access control. For instance, some authors update access control with a semantic web framework; others adapt interesting cryptographic solutions to Facebook. Another interesting access control technique is to develop a method that allows Social Network users to easily filter unwanted messages, according to content based criteria. The task of semantically categorizing short texts is not trivial. The authors propose to combine two main phases: text representation and machine learning-based classification. This approach uses an empirical knowledge acquisition, like Machine Learning, that can lead to a great accuracy depending on the data corpus. The problem is that users don't usually know which privacy policy is better for them. So the next step is to use data mining to infer the best privacy preferences to suggest to SN users. This filter is like a smart and active privacy policy.

All these access control techniques can be worthy. They should not be considered as an isolated tool, but rather as a combined tool. Other PET can also focus on transparency, automatic compliance assurance functions and proactive communications techniques on risks. Discussions on how traditional PET and this new wage of privacy-preserving tools will cooperate are still not conclusive.

5.3.2. CAPER analysis

CAPER uses Video, Audio, Text and Social Network (FOAF, Friend of a Friend) analytics to select the relevant data that is sent to the human expert analyst. This is a first superficial analysis that does not conclude whether someone has a role in a crime: suspect, victim, third party or non-suspect. Those kinds of tools are what have been called e-Analysis projects, and CAPER is not one of them. This distinction is relevant, because e-Analyst-like Projects are far more challenging for data protection and other individual rights like innocence presumption. A Eurojust-like Case Management System would then be needed, for the subsequent databases were the data are stored already labelled.

Nonetheless, it is clear that CAPER will reduce the amount of information received by the human expert and therefore in some way "anticipates" the decision. It reduces the options and

leads to the decision. In e-Discovery, for instance, when the lawyer uses a tool that selects the relevant information to be analysed, this is also called predictive code: links with other statistically information, that are CAPER main capabilities, allow quicker labelling, but do not substitute human labelling: suspect, non-suspect, victim, third party are not CAPER labels. Indeed, CAPER links different information, like a search engine.

When the police will eventually use an ultimate version of the Caper tool, they would collect data that will go directly to the experts for a criminal analysis. No LEA investigator, without the relevant privileges to use the tool should have access to the data before the criminal analyses, by the expert, takes place. As a result, no distinction between suspects and non-suspects should be done by the CAPER tool. This is important, because we avoid distinguishing between suspects and non-suspects, victims and third parties. All this criminal labelling is done afterwards, when the data are included in already existing LEAs information systems.

The only management of data done by the technological tool is:

- Erase non-relevant data.
- Send relevant data to already existing LEAs information systems.

Data collected with CAPER should go to a database with restricted access (CAPER Storage see Fig.). Explicit and detailed users and levels of privileges to access should be adopted. Analysts will determine whether this data is relevant or irrelevant. Irrelevant data should be erased, not stored in any database except in the file log accessible only to the internal supervisor for the purposes of control.

5.4. New suggestions from Agencies after Barcelona CAPER Workshop May 2014

After sending the CAPER Regulatory Model to experts from the national agencies and Europol and Eurojust Data Protection Officers we obtained more feedback from the representative of the Spanish Data Protection Agency.

(…) Nevertheless, I would like to add some considerations. [1] The first has to do with retention periods. Indeed you reflect in your table the risks of continued data storage but, in my view, it could be useful to add to the recommended controls the need of having automated tools detecting the end of the conservation period is going to be reached and asking for positive action if the LEA or controller in charge wants to keep the data.

[2] Although it could be considered that is included in the "Post-CAPER Data reused in other cases" point, I would like to draw your attention on whether it would be advisable to speak of the risks of CAPER data reaching bodies outside de LEA community, for instance, intelligence services or other non-authorised LEAs or even administrative bodies

[3] Besides, in spite of the general risks you have identified, I would strongly recommend the inclusion in your model of a thorough Privacy Impact Assessment be carried out by any LEA wanting to benefit from the CAPER project.

Concerning the first recommendation, the tool detecting the end of the conservation period is going to be implemeted and will notify the need for positive action [1], it has been included in Item 1 of the CAPER Regulatory Model tables: Data Collection and Storage.

There should be an automated tool detecting the end of the conservation period is going to be reached and asking for positive action if the LEA or controller in charge wants to keep the data.

The second recommendation concerning non-authorised access to CAPER Data [2] has been included in Item 3: CAPER Data Reuse and Transfer of the CAPER Regulatory tables as follows:

Non-authorised LEAs and intelligence services or administrative bodies of authorised LEA should not have access to CAPER data.

The third recommendation concerning the need of a concrete Privacy Impact Assessment for every LEA according to the general framework of the CAPER Regulatory Model [3] was included in Item 1: Data collection and storage:

6. CONCLUSIONS

Big Data and statistics allow mass surveillance of behaviours (CHAU, WANG, YUE, CHEN (eds.), 2012) .The increasing capabilities of new IT tools are modifying the trade off between security and privacy. The use of data mining for security purposes is not new. In 2002, the Defence Advanced Research Projects (DARPA) of the United States Department of Defence established the Information Awareness Office (IAO) whose seal has a Latin inscription, Sciencia est Potencia, knowledge is power. One of IAO programs, The Total Information Awareness (TIA) program, pretended to identify, track and predict terrorist behaviour. An adverse media reaction and a distrust of the Director of IAO, Admiral John Poindexter, were crucial to the Congress elimination of funding to TIA program in September 2013. However, TIA didn't really cease to exist, and the NSA has been enhancing the same system for its Terrorist Surveillance Program (in depth, LEE, 2013).

Those new programs collect as much information as possible just in case data could be relevant in the future. With statistics, no expert can assure anymore that a data is irrelevant and confirm thus that it can be deleted without losing information. Every data might be statistically relevant in the future; consequently this is enough to eventually consider it relevant now. Surveillance Data Mining populates and enhances current networks of individuals, places, dates and institutions. In information theory and computer science it is usually known as individualisation. In fact, people are not only isolated items or subjects, but rather nodes of a collective structure, a network. Networks can be interconnected to build up a concrete social network. This communitarian perspective is even more present in preventive search and in classification. Classification based on statistics has a crucial effect on security sciences: security is becoming risk management and risk simulation. Risk is increasingly reckoned and security is a practical field for probabilistic knowledge. Big data revolution and mass surveillance give classification the power to re-identify. Statistics transforms identification in a second level classification: a group reduced to a unique member. Classification is absorbing identification, and this has important consequences. One relevant for lawyers is that data protection regulations are mainly focussed on preserving

identification. As a result, data protection acts simply do not protect citizens against this statistical emergent capability of creating personal data from apparently irrelevant and unrelated raw data. Legal experts are more and more aware of this limitation, and the restrictive perspective on profiling can also be understood as the last opportunity to maintain current data protection regulations non-adapted to big data.

Should counterterrorism Intelligence and police units that fight against organised crime have access to statistics? Yes, of course, it is a non-sense to ban data mining or, let's say it in the legal way, "profiling", in the fight against terror and organised crime. But TIA-like policies go beyond this: no legal restriction should now limit an intensive use of IT tools that is fully justified by efficiency. Should we thus collect everything, just because everything might be relevant some day?

Setting statistics directly at the core of the security–privacy balancing can be, however, a dangerous solution. On the first hand, traditional risk management was based on the human expert knowledge of a criminal analyst. We are now assisting to a starting field: risk as a statistical deviance compared with average behaviour. If a tool can classify behaviour it can offer a risk evaluation. So statistics are opening the possibility of e-criminal analysis. Statistics are enhancing the predictive capabilities of the Intelligence counterterrorism and the police investigation in general. But, in the security field, statistics do not generate automatic security: 100% effectiveness. Human expertise of criminal analysts should not be undermined. Human analysts should check and enhance the statistical labelling.

Another risk comes from the Social sciences themselves. Big data and statistics allow social behaviour computation, and then feed classification and prediction. But not all Social Sciences are predictive or even behavioural sciences. At least this is not the case now for the legal field. Some social models are obviously discussed, but all the capabilities statistics offer are not properly understood. As a result, statistical criminal labelling, without expert validation, is not trustworthy. Statistics certainly do have the capacity to detect links and patterns humans, even experts, cannot even imagine. But automatically inferring from a statistical correlation a ready-to-use social rule or model is less than clear. Social Scientists,

the same way we said before for criminal experts, will have to check whether these results are relevant or they are only false positives. Mistakes will increasingly appear and legal appeals will cost considerable amounts of money.

Human experts and social scientists' participation is crucial, as said before. Nonetheless, it is not the only requirement for a data protection-preserving security. The alternatives for achieving this balancing are threefold: enhancing the legal framework, allowing universal open access or reinforcing data control. The first possibility could be a new big data-adapted legal framework (WRIGHT, FRIEDEWALD, GUTWIRTH, LANGHEINRICH, MORDINI, BELLANOVA, DE HERT, WADHWA and BIGO, 2010). On the other hand, a universal transparency and an open access to all the data are supposed to avoid some institutions to take advantage of them. In this sense, a resistance to the surveillance is even considered (FERNBACK, 2013). Another strategy would consist in the payment to the data controller for its data to limit the temptation of collecting everything (LANIER, 2013). In CAPER, the first option is implemented in a concrete situation.

CAPER’s general framework includes not only Law, but according to Privacy Impact Assessments (PIA) general procedures, risks to be preserved and ad hoc measures. As a result, procedural safeguards allow due respect of the Legal Principles, for instance the principles of purpose or accountability. This is a key point now, when Data Protection Authorities (DPA) postulate Data Protection by Design (DPbD), Data Protection Enhancing Technologies (DPET) as the ultimate legal arsenal. Those crucial principles, without a concrete implementation in a regulatory model, would only be general good willingness.

We are fully aware of the limits of the CAPER Regulatory Model. But the alternative does not exist. If we only trust PET, as a technological solution are we really preserving data protection? Do we have any way to check it? This is a key point, not only for security, but in general when we audit a tool. Computer scientists start to use Information theory and statistics to classify the wide variety of existing data protection metrics. For example to measure the anonymity of a communications network some apparently different entropy criteria are proposed (REBOLLO-MONEDERO, PARRA, DIAZ and FORNE, 2012): Shannon's entropy,

Hartley's entropy and min-entropy. In statistical disclosure control, the measurement of data protection is done using t-closeness, mutual information and k-anonymity and l-diversity. Some authors consider that there is a general framework these concrete proposals all belong. Data protection measurement could be an attacker's estimation error (REBOLLO-MONEDERO, PARRA, DIAZ and FORNE, 2012). For Statistical Disclosure Control situations, t-closeness would be the worst case, mutual information the average case and k-anonymity and l-diversity the best case. For Anonymous communication Systems, min-entropy would be the worst case, Shannon's entropy the average case and Hartley's entropy the best case.

Is that useful in the security field? For sure it is, but not in the short-term. Perhaps, only some concrete capabilities of a tool can be audited, in a well-known and defined use case. The audit of the information workflow will perhaps give the opportunity to reckon the attacker's estimation error. If we want to know whether a PET is really protecting personal data, we need to complement the data protection compliance with some information metrics. Personal data will never be protected at 100% and forever. It is an arms race field like cryptography whether attackers and safeguards are constantly updating their capabilities. But we need a metrics to confirm the need for a new version of the current PET or a new PET. This cannot be done in a theoretical way. There is a need for concrete measurements for concrete PET or fields. The best way, in our opinion, is to embed in concrete PETS data protection but also measured safeguards. The concrete PETS should be accurately selected to cover different subfields and offer general data protection metrics as a result. No need to build up new data protection seals or institutions but rather to improve the existing ones with a metrics for some subfields. The Prise project's European Privacy Seal is a valuable tool that only needs to be complemented with computer science and information theory[29].

Concerning the CAPER tool, only the compliance of the concrete recommendations will be checked. An internal and external supervisor should also have the opportunity to decide whether the data protection embedded procedures of the Caper regulatory model have been respected or not in a concrete case. Accountability is there crucial, in the sense that there is an

[29] https://www.european-privacy-seal.eu/ .

obligation to provide good arguments for one's judgments (ERIKSEN, 2011). This is a crucial idea for the so called Surveillance Impact Assessments (SIA) (WRIGHT, RAAB, 2012): a Regulatory Model or a SIA can help an organisation to gain public's trust and confidence, built on transparency. Institutions plan to give citizens a role in crowdsourcing urban surveillance, and consequently trust will become crucial.

7. ANNEXES/REFERENCES

7.1. REFERENCES

Casanovas, P. (2012), A Note on Validity in Law and Regulatory Systems (position Paper), Quaderns de filosofia i ciència,42, 2012, pp. 29-40.

Bäcker, M., Hornung, G. (2012), Data processing by police and criminal justice authorities in Europe - The influence of the Commission' draft on the national police laws and laws of criminal procedure, ComputerLaw & Security Review, 28, 627-633.

Cavoukian, A. (2009), Privacy by Design...Take the challenge, Information and Privacy Commissioner of Ontario, Canada (www.ipc.on.ca).

Chau, M. ,Wang, G.A., Yue, W.T, Chen. H. (Eds., 2012)), Intelligence and Security Informatics, Pacific AsiaWorkshop, PAISI 2012, Kuala Lumpur, Malaysia, May 29, 2012, Proceedings, LNCS 7299.

Cumbley, R., Church, P. (2013), IS "Big Data" creepy?, Computer law & security review, 29, 601-609.

Dragu, T. (2011), Is There a Trade-off between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism, The American Political Science Review, 105 , 64-78.

Eriksen, E.O. (2011) Governance between expertise and democracy: the case of European Security, Journal of European Public Policy, 18:8, 1169-1189.

Fan, M.D. (March 2012), Panopticism for Police: Structural Reform Bargaining and Police Regulation by Data-Driven Surveillance, Washington Law Review, 87, 1, 93-138.

Fernback, J. (2013), Sousveillance: Communities of resistance to the surveillance environment, Telematics and Informatics, 30, 11-21.

Finn, R.L., Wright, D. (2012), Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications, Computer Law & Security Review, 28, 184-194.

Floridi, L. (2013). The ethics of information. Oxford: Oxford University Press.

Floridi, L. (2014), Open Data, Data Protection, and Group Privacy, Philos. Technol., 27:1–3

Hildebrandt, M. (2013), Balance or Trade-off? Online Security Technologies and Fundamental Rights, Philosophy & Technology, december 2013, Volume 26, Issue 4, pp 357-379.

Lanier, J. (2013), Who owns the Future?, Simon & Shuster.

Lee, N. (2013), Counterterrorism and Cybersecurity. Total Information Awareness, Springer.

Maras, M.H. (2012), The social consequences of a mass surveillance measure: What happens when we become the "others"?, International Journal of Law, Crime and Justice, 40, 65-81.

Monathan, T., Mokos, J.T. (2013), Crowdsourcing urban surveillance: the development of homeland security markets for environmental sensor networks, Geoforum, 49, 279-288.

Pagallo, U. (2013), Online Security and the Protection of Civil Rights: A Legal Overview, Philosophy & Technology, December 2013, Volume 26, Issue 4, pp 381-395.

Pavone, V., Degli Esposi, S., Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security, Public Understanding of Science, 21 (5) 556-572.

Peissl, W. (2009), Privacy and Security - a Way to Manage the Dilemma, N. Pohlmarm. H. Reimer. and V. Schneider (Editors): Securing Electronic Business Processes. Vieweg , 187-196.

Rebollo-Monedero, D., Parra, J., DIAZ, C. and Muñoz, J. (2012), On the measurement of privacy as an attacker's estimation error, International journal of information security, also available at http://hdl.handle.net/2117/18044

Schermer, B.W. (2011), The limits of privacy in automated profiling and data mining, Computer Law and Security Review, 27, 45-52.

Taddeo, M. (Dec 2013), Cyber Security and Individual Rights, Striking the Right Balance, Philosophy & Technology, Volume 26, Issue 4, pp 353-356.

Xhelili, B. Crowne, E. (2012), Privacy & Terrorism Review. Where Have We Come In 10 Years?, Journal of International Commercial Law and Technology, Vol. 7, Issue 2, 121-135.

Wright, D. (2012), The State of the Art in Privacy Impact Assessment, Computer law & Security Review, 28, 54-61.

Wright, D., Friedewald, M., Gutwirth, S., Lengheinrich, M. Mordini, E., Bellanova, R., De Hert, P. Wadhwa, K., BIGO D. (2010), Sorting out smart surveillance, Computer Law & Security Review, 26, 343-354.

Wright, D., Raab, C.D. (2012), Constructing a surveillance impact assessment, Computer Law & Security Review, 28, 613-626.

7.2. ANNEXES.

Annex 1. CAPER Worshop in Paris, 29th and 30th of November 2013, with the Spanish Data Protection Agency, Eurojust and Europol experts. Final Programme:

The Ethical and Legal Aspects of Digital Security

SPECIAL WORKSHOP ON

Digital Security and Data Protection

Final Programme

29th November

14.30-14.40	**Michel Borgetto**, Director of CERSA: *Welcome and Opening*
14.40-15.00	**Danièle Bourcier, Pompeu Casanovas**: *Welcome and Timetable. Goals of the Workshop.*
15.00-15.30	**Danièle Bourcier, Primavera de Filippi**: *Distributed on line architectures: disrupting the balance between security and privacy*
15.30-16.00	**Luciano Floridi**: *Paternalisms and Rights in Security Contexts*
16.00-16.30	**Giovanni Sartor**: *A framework for balancing competing legal values*
16.30-17.00	*Break*
17.00-17.30	**John Zeleznikow**: *Trust and Security in Online Dispute Resolution*
17.30-18.00	**Christian Fluhr**: *From text to structured information, application for personal information extraction*
18.00-18.30	**Aldo Gangemi**: *Ontologies vs. Machine Reading On the Semantic Web: The Misery and Nobility Rights*
18.30-19.00	*Apéritif-champagne at CERSA*
19.30	*Dinner at Restaurant* **La Petite Périgourdine**

30th November

08.00-08.30 **Emilio Aced**: *Elements for Adequate Data Protection in the 21st century*

08.30-09.00 **Joaquin Bayo**: *The specificities of data protection in the field of criminal justice and police*

09.00-09.30 **Daniel Drewer**: *The experience of Europol in Security and Data Protection*

09.30-10.00 **Diana Alonso**: *The experience of Eurojust in Security and Data protection*

10.00-10.30 *Break*

10.30-10.50 **Pompeu Casanovas**: *Semantic Web Regulatory Models: Social Intelligence and Ethical Impact Assessments*

10.50-11.10 **Antoni Roig**: *Privacy and Ethical requirements for EU CAPER Project*

11.30-11.50 **Rebeca Varela Figueroa**: *Seeking interoperability: a conceptual scheme for the fight against organized crime in Europe*

11.50-12.20 **Ugo Pagallo**: *Circumnavigating the Cape Horn of Legal Science: Notes on Social Intelligence and the CAPER Project, Between Ethics and the Law*

12.20-13.00 **Ugo Pagallo, Pompeu Casanovas**: *Final Discussion, summary of conclusions, and future work*

Participants

Emilio Aced (eaced@agpd.es), Spanish Data Protection Agency (Agencia Española de Protección de Datos)
Geraldine Aïdan (geraldineaidan@hotmail.fr), Université Paris I Panthéon-Sorbonne
Diana Alonso Blas (dalonsoblas@eurojust.europa.eu), Eurojust
Joaquin Bayo-Delgado (J.bayo@poderjudicial.es), former Assistant Supervisor of the European Data Protection Supervisor
Danièle Bourcier (daniele.bourcier@cersa.cnrs.fr), Centre d'Études et de Recherches de Sciences Administratives et Politiques
Pompeu Casanovas (pompeu.casanovas@uab.cat), Institute of Law and Technology (IDT), Universitat Autònoma de Barcelona
Cyril Debard (cyril.debard@gendarmerie.interieur.gouv.fr), Gendarmerie Nationale
Daniel Drewer (daniel.drewer@europol.europa.eu), Europol
Luciano Floridi (luciano.floridi@oii.ox.ac.uk), Oxford University
Christian Fluhr (christian.fluhr@gmail.com), GEOL Semantics
Aldo Gangemi (aldo.gangemi@cnr.it), LIPN - Laboratoire d'Informatique de Paris-Nord
Guillaume Piolle (guillaume.piolle@supelec.fr), Supélec
Ugo Pagallo (ugo.pagallo@unito.it), Center for Transnational Legal Studies
Valentina Presutti (valentina.presutti@cnr.it), LIPN - Laboratoire d'Informatique de Paris-Nord
Antoni Roig (Antoni.roig@uab.cat), Institute of Law and Technology (IDT), Universitat Autònoma de Barcelona
Giovanni Sartor (giovanni.sartor@iue.it), European University Institute
Rebeca Varela Figueroa (Rebeca.varela@uab.cat), Institute of Law and Technology (IDT), Universitat Autònoma de Barcelona
John Zeleznikow (john.zeleznikow@vu.edu.au), Victoria University, Melbourne

Practical information

Venue

CERSA
10 Rue Thénard, 75005 Paris
Tel: +33 142345880
Website: http://www.cersa.cnrs.fr

Hotel

Best Western Trianon Rive Gauche
1 bis et 3 Rue de Vaugirard, 75006 Paris
Tel: +33 143298810 — Fax: +33 143291598

Restaurant

La Petite Périgordine
39 Rue des Écoles, 75005 Paris
Tel: + 33 143263335

Organizers:

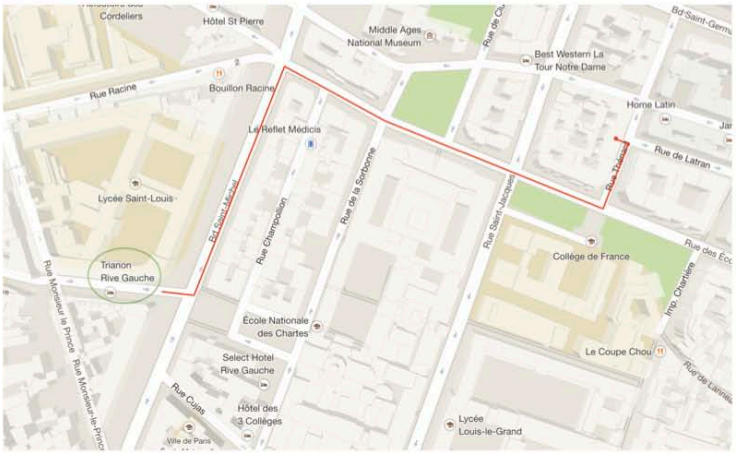
CERSA–CNR (Paris, France) and **IDT–UAB** (Barcelona, Spain)

Projects:

CAPER – Collaborative information Acquisition, Processing, Exploitation and Reporting for the Prevention of Organized Crime (http://www.fp7-caper.eu/fr.html)

SINTELNET – The European Network for Social Intelligence (http://www.sintelnet.eu/)

Route from the hotel to the venue:



Annex 2. CAPER Worshop in Barcelona, 16th May 2014, with the Spanish Data Protection Agency, Eurojust and Europol experts. Final Programme:

Data Protection and Security Issues: the CAPER model.

Barcelona, 16th May 2014-05-11

IEC

Final Programme

15th May 2014

20.30. Dinner at ATN Restaurant

16th May 2014

09.30-10.00. Pompeu Casanovas. *The Caper Regulatory Model.*

10.00-10.30. Jorge González-Conejero, Rebeca Varela, Emma Teodoro; IDT-UAB. *Organized Crime Structure modelling for European Law Enforcement Agencies.*

10.30-11.00. Antoni Roig. ***Legal and Procedural Safeguards of CAPER Surveillance Regulatory Framework***

11.00- 11-30 Coffee Break

11.30-12.30. Felipe Melero, Project Coordinator-S21Sec; Juan Arraiza Technical Project Coordinator-Vicomtech. *The Caper platform.*

12.30-13.00. Emilio Aced. Recommendations for the Caper Data Protection Strategy.

13.00.13.30. Diana Alonso. Recommendations for the Caper Data Protection Strategy.

13.30-14.00. Sonia Sousa Pereira. Recommendations for the Caper Data Protection Strategy.

Lunch at: L'Antic Forn

Participants

Aced, Emilio	Spanish Data Protection Agency
Arraiza, Juan	Vicomtech
Alonso, Diana	Data Protection Officer Eurojust
Casanovas, Pompeu	IDT-UAB
González-Conejero, Jorge	IDT-UAB
Melero, Felipe	S21sec.com
Roig, Antoni	IDT-UAB
Sousa Pereira, Sonia	Data Protection Office Europol
Teodoro, Emma	IDT-UAB
Varela Figueroa, Rebeca	IDT-UAB

Annex 3. Discussion with the Spanish Data Protection Agency, Eurojust and Europol representatives, at the Barcelona Workshop, 16th May 2014:

CAPER

Data Protection and Security Issues: the CAPER model
Barcelona, 16th May 2014
IEC

Legal and Procedural Safeguards for CAPER: a Surveillance Regulatory Framework

1

CAPER

1. CAPER RISKS

- CAPER enhances accuracy of retrieved information and reduces time of search. IT improvement that reinforces preventive search and data mining profiling. It does not classify according to criminal labelling. Pre- (criminal) analysing process.
- RISK1: used for ordinary police investigations
- RISK2: CAPER data considered police analysed data or suitable for automatic decisions
- RISK3: storage of irrelevant data of non-guilty people, third parties, victims.

Workshop on Digital Security and Data Protection 2

CAPER

1. CAPER RISKS -2

- RISK 4 Data storage in Networks. Not based on individual cases. Permanent labelling, guilty presumption of third parties and victims?
- Risk 5: General deny of access
- Risk 6: Difficult or almost impossible judicial audit of proportionality and due process of law
- Risk 7: Transfer of CAPER raw data shift into relevant data.

3

CAPER

2. Legal and procedural Safeguards

- RISK1: used for ordinary police investigations
  - Only for terrorism and organised crime in a separate repository
  - CAPER data directly sent to human criminal expert, not used by investigators

4

CAPER

- RISK2: CAPER data considered police analysed data or suitable for automatic decisions
  - CAPER data will have no labelling. Only human experts can do it, afterwards
  - Access limited to the human expert
  - Erase non-relevant data, Relevant data sent to already existing Databases

5

CAPER

- RISK3: storage of irrelevant data of non-guilty people, third parties, victims
  - CAPER = Row data, not analysed by criminal human expert. Suspects, victims, witnesses cannot be automatically inferred from CAPER. Analysed data = labelled and in other databases

6

CAPER

- RISK 4 Data storage in Networks. Not based on individual cases. Permanent labelling, guilty presumption of third parties and victims?
  - After CAPER: only mentioned in CAPER Regulatory Framework as recommendation: There should be a clear difference between the processing of personal data of convicted perpetrators and of victims and third parties. More, this should be a priority in databases created for preventive purposes or the prosecution of future crime. So, additional protection is required when the data of "non-suspects" is processed (WP 201 art. 29 DPWG).

7

CAPER

- Risk 5: General deny of access
  - Some information, access, rectification and delete rights could be partially accepted in some cases without jeopardizing the investigations. work.
  - LEA should have the first decision on it because they know the possible risks of a disclosure of information better than anyone.
  - Data should be preserved in case a DPS or a Court want to check the reasons of a deny of access after the investigation has finished. This could happen during a periodic audit of a DPS or if one citizen wants to confirm LEA have proceeded properly, fulfilling the CAPER Surveillance Regulatory Framework

8

CAPER

- Risk 5: General deny of access
  - Some information, access, rectification and delete rights could be partially accepted in some cases without jeopardizing the investigations. work.
  - LEA should have the first decision on it because they know the possible risks of a disclosure of information better than anyone.
  - Data should be preserved in case a DPS or a Court want to check the reasons of a deny of access after the investigation has finished. This could happen during a periodic audit of a DPS or if one citizen wants to confirm LEA have proceeded properly, fulfilling the CAPER Surveillance Regulatory Framework

8

CAPER

- Risk 6: Difficult or almost impossible judicial audit of proportionality and due process of law
  - Authorisations, audit track
  - Internal supervisor (DPO-like institution)
  - External supervisor: national DPA, ad hoc Eurojust and Europol-like Joint Supervisory Body or European Supervisor

9

CAPER

- Risk 7: Transfer of CAPER raw data shift into relevant data.

  - CAPER data will not be transferred to other countries. If transferred, they will be labelled as raw data, with clear indication that they are pre-analysing data

10