Document title:	**D.7.1 REGULATORY AND ETHICAL FRAMEWORK: CAPER REGULATORY MODEL**
Due delivery date:	**30/06/2012**
Nature:	**Deliverable**
Project Title:	**Collaborative Information, Acquisition, Processing, Exploitation and Reporting for the prevention of organized 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:

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

Proprietary rights statement
This document contains information, which is proprietary to the CAPER consortium. Neither this document, nor the information contained herein, shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except prior written consent of the CAPER consortium.

History			
Version	First name & Name	Modifications	Date
D7.1-01	Pompeu Casanovas	First Version Framework/Networked governance 1. CRM	15/05/2012
D7.1-01vs2	Pompeu Casanovas	Second version Framework/Networked Governance 1. CRM	1/06/2012
D7.1-02	Antoni Roig	Privacy and Data protection Protection Models	
D7.1-03	Esther Morón/MJR-P	Legal Framework (Europe/Spain)	
D7.1-04	M.José Rodríguez-Puerta/EM	Legal Framework (Europe/Spain)	
D7.1-05	Tomàs Gil	LEAs Issues	
D7.1-06	Francesca Gaudino	Legal Framework (EU countries)	
D7.1-07	Marta Poblet/PC	Ethical issues	
D7.1-08		CAPER Regulatory Model	

Validation			
	First name & Name	Organisation short name	Visa
Responsible		IDT UAB	
WP leader	Pompeu Casanovas	IDT UAB	
Coordinator	Marta Poblet		

INDEX

1 THE FRAMEWORK FOR THE CAPER REGULATORY MODEL (CRM)

1.1. AIM OF THE DELIVERABLE

This deliverable aims at offering a general overview of the regulatory and ethical framework of CAPER. These issues are usually presented together in concrete cases and everyday situations, but we'll try to maintain them analytically separated in this Deliverable.

The main targets of the Project are the following (as stated in the Memory and the Project Scope Statement):

- CAPER's objective is to build a common collaborative and information sharing platform for the detection and prevention of organized crime in which the Internet is used (e.g. sale of counterfeit or stolen goods, cyber crime) and which exploits Open Source Intelligence

- CAPER will provide Law Enforcement Agencies (LEA) with a common operational platform for Open Source Intelligence complemented by standards based interfaces sets. It will allow easy integration with legacy systems and future applications.

We will set up a legal and ethical framework that we will term *CAPER regulatory model.* A regulatory model is not only a structured framework, but a generative set of principles, values, and rules which can be shared by all the LEAs and members of the consortium on rights, duties and appropriate behavior. This generative set is twofold: (i) among the members of the consortium, (ii) and regarding the protection of citizens' rights.

Accountability, asymmetrical network governance and responsible data protection are some of the aspects to be pointed out. The CAPER regulatory model will assemble legal boundaries and empowerment capabilities alike, in a three level stake concerning (i) applicable statutes, regulations and judicial rulings, (ii) European and national policies, (iii) and, on top of that, ethical and professional good practices. This regulatory set does not come into a vacuum. The evolutionary context created by criminal threads to the open society must be taken into account, because it sets a bottom-up permanent and dynamic landscape of changing scenarios. The common resilience of governments, companies and citizens are essential to deal with such a landscape, and therefore, the suggested standards will assume that citizens, and not only governments, are entitled to cooperate with police organizations and with the justice to fight organized crime.

This turns to be essential because the normative framework described in the next section does not exhaust all possible options. National law and European Directives hold a democratic legitimation for their enacting and enforcement power stemming from a legitimated authority (parliament, national assembly, judges and magistrates etc..). But to be effective legal norms have to be completed with common policies and political guidelines, and have to be assumed and completed as well across the cooperative behavior of citizens. This is the reason why technological interoperability and legal police actions require common grounds created by social relationships. Fighting organized gangs or illegitimated political violence is a social prerogative of the entire population under the rule of law, Even if professional intervention and expertise are increasingly needed, this is not a matter for police intervention, only, but for citizen cooperation and institutional strengthening.

In this Deliverable we will contend that individuals belong to organizations, and they may behave as individuals, or as community or network members. We will assume as well that there is not a clear divide between "digital" and "real life" behavior, and, accordingly, there is no clear-cut separation between crime and cybercrime. Both of them are backed and shaped into social evolving contexts.

1.2 ORGANIZED CRIME

1.2.1 Organized Crime: A Changing Landscape

K.K. Choo (2008), and Choo and Smith (2009) identify three categories of organized groups that exploit advances in information and communications technologies (ICT) to infringe legal and regulatory controls: (1) traditional organized criminal groups which make use of ICT to enhance their terrestrial criminal activities; (2) organized cybercriminal groups which operate exclusively online; and (3) organized groups of ideologically and politically motivated individuals who make use of ICT to facilitate their criminal conduct.

Global criminals are now sophisticated managers of technology and talent (Goodman, 2011). It is a common place in security studies that the sophistication and high level of knowledge shown by cyberterrorists and criminal networks require more efforts to be put in place by governments, companies and citizens. Terrorist threads or malware expansion have in common the careful and planned using of ICT tools. In the assault to Mahal Palace Hotel in Mumbai (Kuwait), November 2008, the ten men who carried it out were coordinated with their Pakistan based command center using Blackberrys, satellite phones and GM handsets. The command center monitored broadcast news and the internet to provide real-time information and tactical direction. Central networked intelligence and coordinated knowledge are fundamental assets shared with non-terrorist criminal organizations.

"Modern organized crime has abandoned the top heavy structure of dons, capos, and lieutenants made famous in *The Godfather.* Most of today's gangs, along with Al Qaeda and other terrorist groups, are loosely affiliated cooperative networks—and are as likely to recruit website designers and hackers as they are thugs and enforcers. They routinely turn to niche markets for specific expertise. (For instance, Dubai offers the best talent for laundering money.) They are constantly networking to develop sources with the specialized skills they need, much as Hollywood studios scout for talent to cast a given film" (Goodman, 2011: 18).

It is true, as stated by Choo (2010), that despite the synergy between traditional organized crime groups and cyberspace, traditional organized crime groups should not be confused with organized cybercrime groups that operate exclusively online. However, evolutionary approaches to criminal activities in traditional organizations may lead to a better understanding of the deepness of technological impact even on regular and small criminal gangs at a local level. In Julie Ayling´s model, for instance, the external changing environment adds pressure to evolution and leads to a cultural selection of leaders. Those are able to understand the challenges and can move fast towards a selective use of available technology, expanding the original goals and differentiating an inner power structure to increase their dominance over their fellow members (Fig. 1).

"While most street gangs are temporary and disorganized, some have institutionalized, and a number of these show signs of evolving into more serious criminal enterprises, becoming

more networked, technologically savvy and internationalized, less visible, more predatory and sometimes more violent. The boundaries that researchers have drawn between gangs and other types of criminal groups, particularly organized crime, are becoming blurred." (Ayling, 2011:1).

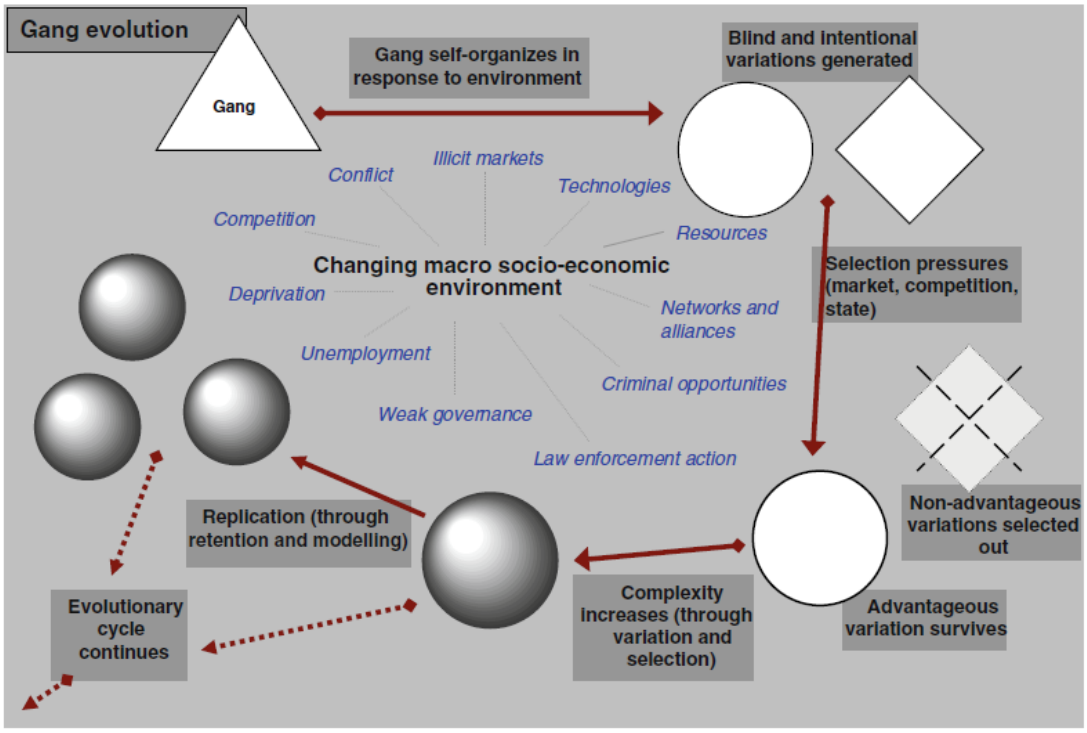

Fig. 1 A gang's simplified evolutionary pathway Source: J. Ayling (2011: 11)

Theft is not the only objective which is targeted in organized crime. Extorsion, industrial espionage and monitoring the traffic flow in order to be alert against defensive counterattacks are objectives as well, targeting business organizations even more than individuals (de Joode, 2011). E.g. The Zeus Trojan gang was eventually arrested in September 2010, after stealing several millions from USA and UK bank accounts. Sophisticated Trojan worms as Zeus may change over fifty times in a single day, depending on the conditions in which they are hosted, and sending automatically information on the general security conditions of the host to remote criminal servers. Calculate risk levels and keeping tuned the programming according to them is not only a common practice among the police and security companies (Gottschalk, 2010). It is also a common practice among cybergangs.

Security companies set the need to display proactive behavior in order to anticipate the opponents´moves. Mel Morris (2010) singles out three flaws in today´s cibersecurity model: (i) The first is a high dependence on prior knowledge of threats in order to mount a defense; (ii) the second is a 'blind spot' to new intrusions that are outside of the model's knowledge base; (iii) finally, the lack of centralized intelligence about new threats means criminals can continue to use the antimalware model against itself and find even more ingenious approaches to evading detection. Morris states that "centralized intelligence is cybercrime's most powerful tool, even in its infancy" (2010: 14).

Twelve years ago, industrial piracy and traditional crime organizations were taking advantage of the internet in a more limited scale, leaning on the black market and on a high hierarchical and tight structure, daily controlled.

“Pirated CDs and DVDs may be found in any Asian city. Data from just one investigation are illustrative of industrial-scale piracy. In August 2000, Malaysian investigators raided a factory, seizing 100 CD stampers, 200 000 counterfeit CDs and 20 PCs, worth an estimated US$ 480 million “ (Grabosky, 2007: 148)

These types of criminal behavior do not disappear and keep going on. But centralized intelligence and networked activities allow a more distributed and resituated targets, according to the pervasive advance of the social web 2.0. Online child pornography (Carr, 2012), prostitution (Cunningham and Kendall, 2011), terrorism and all sorts of extortion and aggressive behavior have been fueled by the expansion of the social web. The Internet is not only a tool, but the condition and natural environment of the organized crime. For what it will follow in this Deliverable, perhaps it is a bit exaggerated to state that “much like Afghanistan before 2001, the World Wide Web has become a sanctuary for terrorists” (McDonald, 2010, 103). But it is nevertheless true that organized crime have updated its structure according to it.

1.2.2 Organized Crime: New Definition

“Organized crime” has been always difficult to define in a precise manner. The concept itself has been dismissed as political and ideological by critical criminology (Van Dijk, 2007). Van Der Heijden (1996) proposed a number of common characteristics to define the concept: *1) Collaboration of more than two people; 2) Commission of serious criminal offences (suspected); 3) Determined by the pursuit of profit and/or power; 4) Each having their own appointed tasks; 5) For a prolonged or indefinite period of time; 6) Using some form of discipline and control; 7) Operating across borders; 8) Using violence or other means suitable for intimidation; 9) Using commercial or businesslike structures; 10) Engaged in money laundering; 11) Exerting influence on politics, the media, public administration, judicial authorities, or economy.*

According to this formula, for any criminal group to be categorized as organized crime it needs to have at least six of the above characteristics, where Items 1, 2, and 3 are obligatory, thus adding three more characteristics.

Leaning on the recent Tayebi and Glässer (2011) revision of Van der Heijden work, for analytical purposes, other flexible notions can be proposed. They focus, e.g., on *co-offending networks*. A “co-ofending network” is simply “a network of offenders who have committed crimes together” (ibid.). Tayebi and Glässer aim at a conceptual foundation for developing advanced computational methods to identify “organized crime structures” from large crime datasets using social network analysis and data mining techniques.

Do notice that this means a slight shift compared to more traditional conceptual approaches. Characterizing the concept is less than developing the appropriate discovery tools to shed new light on criminal networking and related practices. Kaza et al. (2005) similarly proposed a loose definition to concentrate on the topological properties of networks. Deepening on law enforcement databases, and stemming from the successful program COPLINK, they found

that “narcotics networks are small-world with short average path lengths ranging from 4.5-8.5 and have scale-free degree distributions with power law exponents of 0.85 – 1.3.” In addition to that, they found that “utilizing information from multiple jurisdictions provides higher quality leads by reducing average shortest path lengths of the networks” (ibid. 2005, 251).

These proposals are very important for the CAPER Project as well, for they show that Law enforcement agencies and police can greatly benefit from information sharing. Therefore, conceptual approaches to criminal networks have to be related to legal definitions and norms coming from the legal framework, but to be really effective they have to be clung to more precise methodological trends too, aiming at action coordination and data interoperability.

This is what we will show in the next sections, *legal framework* (1.3.) and *regulatory model* (1.4).

1.3 THE LEGAL AND ETHICAL FRAMEWORK

1.3.1 Hard Law and Soft Law

There are three sources of European Union law: primary law, secondary law and supplementary law. The main sources of primary law are the Treatises of the European Union (e.g. it is particularly relevant to CAPER the Treatise of Lisbon, 2007, regarding personal data protection). Secondary sources are legal instruments based on the Treaties: directives, regulations, and decisions. Supplementary sources are international law, general principles of the European Union and decisions coming from the Court of Justice of the EU.

A *directive* is a legislative act of the EU, which requires member states to achieve a particular result without dictating the means of achieving those results. Directives normally leave member states with a certain amount of leeway as to the exact rules to be adopted in the national transposition of the directive. On the contrary, a *regulation* is self-executing, immediately enforceable as law in all members states simultaneously. A *decision* is a legal instrument that has legally binding effects on individuals or member states. They may be taken by the Council of the European Union or, under delegation, by the European Commission.

Similarly, from the national point of view, a *statute* is a formal written enactment of a legislative authority. A *regulation* is a set of norms enacted by a formal authority to develop the content of a legal statute. (e.g. the execution of rights and the allocation of responsibilities). An *administrative action* is a particular body of decisions and rules enacted by a local, regional or national government or agency to implement the content of statutes, regulations or judicial rulings.

All these principles and different types of regulations in level, scope, and jurisdiction constitute an entangled body of applicable law.

One simple way to differentiate its content would be stemming from the *legal value* carried on by the set of regulations. Some of them are binding, while others are simply recommended. In International Law, restorative justice or other social areas in which the binding power of the states can be set apart, it is common to distinguish between *hard law* and *soft law*.

Hard law refers to legally binding obligations, either in the national or international arena, under regulations that can lead to adjudication court processes. Soft law, on the contrary, is not mandatory and leaves room to dialogue, negotiations and common decisions. "International actors choose softer forms of legalized governance when those forms offer superior institutional solutions. […]. The realm of soft law begins once legally arrangements are weakened along one or more of the dimensions of obligation, precision, and delegation. This softening can occur in varying degrees along each dimension and in different combinations across dimensions. We use the shorthand term *soft law* to distinguish this broad class of deviations from hard law – and, at the other extreme, from purely political arrangements in which legalization is largely absent. But bear in mind that soft law comes in many varieties: the choice between hard law and soft law is not a binary one" (Abbot and Snidal, 2000: 421-422).

Soft and hard law are not discrete categories, but they are placed on a *continuum* which allows the coordination of different powers and authorities to produce what it is sometimes called, *global law*, regulations across borders among citizens, organizations and the different states (Karlsson-Vinkhuyzen and Vihma, 2009). Figure 2 describes such a continuum, from hard to soft law, and from policies and political decisions to ethics. We have ordered also in Table 1 the different regulatory instruments currently available to produce this institutional strengthening.

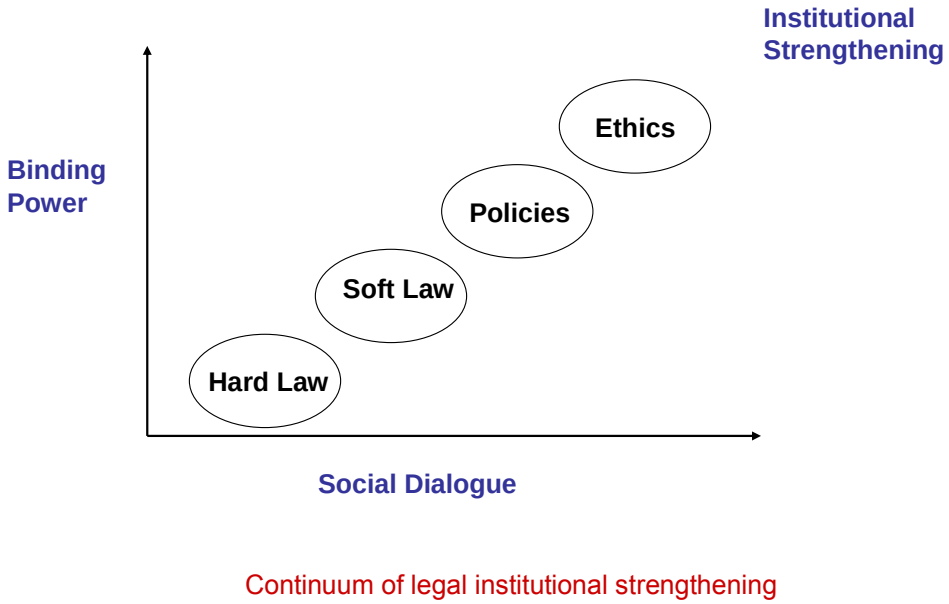

Fig. 2: Regulatory scale

Regulation	Norms	Hard law	International level	Treaties
				International custom
				Principles of international law
			European level	Treaties
				Directives
				Regulations
			National level	Law
				Regulations
			Regional level	Law
				Regulations
			Local level	Rules
		Soft Law	International level	Declarations
				Programs
			European level	Declarations
				Recommendations
				Standards
			National level	Codes
				Recommendations
				Standards
				Reports
			Regional level	Codes
				Standards
				Guides
			Local level	
	Protocols, rules, non binding technical instructions	International domain	Private	
			Public	
		European domain	Private	Codes of conduct
			Public	Communications, White Books, Codes of Conduct
		National domain	Private	White Books, Codes of Conduct
			Public	
		Regional domain	Private	
			Public	White Books
		Local domain	Private	
			Public	Protocols

Table 1. Table of regulatory instruments. Source: P. Casanovas et al. (2010)

Do notice that we deal with three different kinds of power: (i) binding power of the national sovereign states which form the European Union; (ii) binding power of the European union as a whole; (iii) binding power of the international community. It is a common place that the latter one lacks of real enforcement means; and that the EU leans on economic and political sanctions. This is the old discussion about the sovereignty of the states, which has been maintained nevertheless through the EU legal forms. In sensitive areas like policing and security, this fact has to be taken into account.

1.3.2 EU Regulations on Data Protection

Lawyers and jurists have been harvesting data protection and security and personal data for the last forty years in the European Union. This is a well-trodden path, one of the most valued legal buildings of the EU. However the upcoming of Web 2.0, ubiquitous computing, the storage and processing of data in the cloud, and the presence of an increasingly number of web services forced a complete revision of the EU policies and regulations. Starting November 2010, In December 2011 and January 2012 the Commission ended up two years of preparatory works and presented its proposals.

"The stakes are high, because the Commission intends to replace nothing less than the entire EU data protection edifice. This herculean task shall be carried out by two instruments released simultaneously: the *General Data Protection Regulation*[1], intended to replace the EU *Data Protection Directive 95/46/EC3*[2] and the *Police and Criminal Justice Data Protection Directive*[3] intended to replace the Framework Decision 2008/977/JHA.5[4] The latter has a short history and its replacement is perhaps more of a semantic rather than of substantial value. The replacement of the Directive, however, is an important and far-reaching development; once finalized, the new instrument is expected to affect the way Europeans work and live together" (de Hert and Papakonstantinou, 2012: 130-31).

There are economic reasons as well. Maria Giannakaki (2012) reports that according to the European Network and Information Security Agency (ENISA), the worldwide forecast for cloud services in 2013 amounts to USD 44.2bn, with the European Market expected to go from € 971 in 2008 to € 6005 in 2013. Gartner projects the worldwide cloud revenues to reach $68.3 billion for 2010 (a 16.6 percent increase from 2009), and forecasts revenues to surpass $148 billion by 2014 (Srivastava et al. 2011).

[1] "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (General Data Protection Regulation).
[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 pp.0031e0050.
[3] "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of intervention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data" (Police and Criminal Justice Data Protection Directive).
[4] Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters.

The new Directve and Regulations constitute a complex and nuanced set of instruments, (yet, awaiting for approval). The analysis of these documents is the purpose of the present Deliverable. We are not going deeply into them now. However, for the sake of understanding and introducing the legal vocabulary, we will offer a short summary of their content. In what follows we will lean on direct reading and on the preliminary critical analysis carried out by Hon, Millard and Walden (2011), Van Eecke, Craig and Halpert (2012) and, especially, de Hert and Papakonstantinou (2012). We borrow from the latter the following summary:

I. The Lisbon Treaty (2007) formally turned the *right to data protection* into a separate fundamental right, distinct from the *right to privacy* (art. 16 TFEU).
II. The wording of the Draft Regulation repeats that of the Directive: "*personal data* means any information relating to a data subject".
III. The release of a Regulation, rather than a new Directive, to replace the EU Data Protection Directive maintains the distinction between *general* and *commercial data* processing, on the one hand, and *security* and *related personal data* processing, on the other.
IV. The Directive's distinction between *common* and "*special categories of*" (sensitive) personal data is maintained in the draft Regulation (adding "genetic data", "biometric data", and "data concerning health").
V. It is also maintained the traditional scheme of personal data processing, whereby a single entity ("data controller") decides to process the personal information of "data subjects" and it proceeds to execute such processing either at its own premises and with its own means, or by contracting it to third parties ("data processors").
VI. Data controllers retain their central role as to the processing of personal data, but they may come in various types and formats. For instance, Web 2.0 service providers only provide the platform upon which personal data processing is performed and it is not always evident that they are themselves involved in such processing. The same applies to cloud computing.
VII. The *Fair Information Principles* of the Directive are maintained in the text of the draft Regulation (for instance, the *fair and lawful processing of personal information*, the *data quality principle*, the *purpose specification principle*, the *transparency principle*, the clarification *of data minimization principle*.
VIII. Both the *principle of transparency* and thus of *accountability* that are introduced here constitute substantial reinforcement of the individual rights protection.
IX. The *principle of accountability* would place upon data controllers the burden of implementing within their organizations specific measures in order to ensure that data protection requirements are met.
X. The draft Regulation allows "*further processing*" for a purpose that "is not compatible with the one for which the personal data have been collected". The processing of personal information for purposes unforeseeable at the time of data collection, to which evidently no consent has been given by the individuals concerned, undermines the principle of purpose specification.
XI. The Commission substantially reinforced the *individual consent* requirement in its draft Regulation. Its definition has been enhanced by means of requiring *"explicit" consent* in order to "avoid confusing parallelism with 'unambiguous' consent".
XII. The Regulation updates the Directive's *individual rights* (Art. 11-20 of the Regulation) and introduces the *right to be forgotten* (Art. 17 of the Regulation). The draft Regulation has added a data controller obligation to transparency and to establishment of appropriate procedures that will assist data subjects.
XIII. The *right to system interoperability* "data portability" (Art. 18 of the Regulation), as is the case with the right to be forgotten, is an internet-specific right. In particular, it

grants individuals the right to obtain a copy of their profiles uploaded onto internet platforms in a suitable format for further processing and use by themselves, and for such profile not to contain technical or other impediments to it being subsequently uploaded onto the internet platform of another service provider (essentially, a competitor to the former).

XIV. *Member State Data Protection Authorities* (DPAs) are intended to constitute "the main instrument of data protection enforcement" within their respective jurisdictions (Art. 45-46 of the Regulation) This means that DPAs are responsible for warranting effective implementation of their respective national data protection acts within their jurisdiction. There are several means to achieve this: investigative powers, powers of intervention and the power to engage in legal proceedings.

XV. The Regulation make a generalized use of "personal data breach notifications" (Art. 31-32).

XVI. The role of 'soft law' is enhanced with *Data Protection Impact Assessments* (Art. 33 of the Regulation) The Commission Communication prior to the release of the draft Regulation set that, in order to enhance data controllers' responsibility, it would be examined whether "an obligation for data controllers to carry out a data protection impact assessment in specific cases" should be included. These situations could include, inter alia, processing of sensitive data or "when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance"..

This summary primarily refers to the Regulation. It entails a reinforcement of the protection of individual rights. However, this has to be balanced with the member states duty to protect national citizens. Therefore, as stated by the Commission:

"Article 16 TFEU requires the legislator to lay down rules relating to the protection of individuals with regard to the processing of personal data also in the areas of judicial co-operation in criminal matters and police cooperation, covering both cross-border and domestic processing of personal data. This will allow protecting the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, *ensuring at the same time the exchange of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties*" (PD, Explanatory Memorandum, p. 3).

The twofold objective of preventing terrorism and transnational crime while protecting human rights and applying personal data guaranties explains why the Commission chose the Directive form (and not the Regulation form) for cases involving national security. This is a sensitive issue regarding sovereignty. For each EU state there are different constitutional and organic norms that must be applied. Therefore, on one hand, normative and legal harmonization is at stake. But, on the other hand, transnational relationships among security administrations (police and the judiciary) are crucial to comply with the spirit of new Directive.

From the legal point of view, the proposed new *Police and Criminal Justice Data Protection Directive* is rooted in the balancing of the *principle of subsidiarity* (the objectives envisaged cannot be achieved sufficiently by Member States, but can rather, by reason of the scale or effects of the proposed action, be better achieved by the Union); and the *principle of proportionality*, that requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives.

These two principles, taken together, pave the Directive way and the interpretation of the rules to be followed to tailoring the new data protection body.

The whereas 7 (*considerandum*) of the intended Directive states:

"Ensuring a consistent and high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial co-operation in criminal matters and police cooperation. To that aim, the level of protection of the rights and freedoms 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 must be equivalent in all Member States. Effective protection of personal data throughout the Union requires strengthening the rights of data subjects and the obligations of those who process personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States."

n. 19:
"For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to retain and process personal data, collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context to develop an understanding of criminal phenomena and trends, to gather intelligence about organised criminal networks, and to make links between different offences detected."

And, most interestingly, n. 38:

"*The protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organisational measures be taken to ensure that the requirements of the Directive are met. In order to ensure compliance with the provisions adopted pursuant to this Directive, the controller should adopt policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default*."

This leads directly to art. 19 and the concept of *data protection by design* and *by default*:

"1. Member States shall provide that, having regard to the state of the art and the cost of implementation, the controller shall implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject.
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data which are necessary for the purposes of the processing are processed."

There is room, then, to regulating the relationships between *controller*[5], *processor*[6] and *independent supervisory authority*[7] and to allocate responsibilities, but art 19 (and those referred to the exchange of data) shows that the EU Commission understands the technological difficulties of storage, interoperability, design and processing of the file content, which is supposed to be *structured*[8]. In other words, without following good practices and technical protocols from the accumulated experience, and creating new soft law instruments the twofold goal of protection at the individual level (personal data protection) and at the collective level (national and European security) would not be attainable. The new regulation is not only aiming at the Web 2.0, the Social Web, but to Web 3.0, the Web of Data as well.

We are not going further now into the details of the proposed text. Our goal will be instead to set up a suitable form of a regulatory model that may contain the guidelines to implement the content of the data protection and security body into the CAPER platform. We will call it the CAPER Regulatory Model (CRM), and we will show in the next section that this is a form of what it is known as *Networked Governance*, and one of the first steps of a new concept of *Security by Design*.

1.4 SECURITY BY DESIGN: THE CAPER REGULATORY MODEL (CRM)

1.4.1 Privacy by Design and Ubiquitous Computing

Let's deepen a bit more on privacy, first. *Principles of fair information practices* (FIPs) after the Alan Westin tradition can be summarized as follows (Langheinrich, 2001):

1. Openness and transparency: There should be no secret record keeping. This includes both the publication of the existence of such collections, as well as their contents.
2. Individual participation: The subject of a record should be able to see and correct the record.
3. **Collection limitation:** Data collection should be proportional and not excessive compared to the purpose of the collection.
4. Data quality: Data should be relevant to the purposes for which they are collected and should be kept up to date.
5. Use limitation: Data should only be used for their specific purpose by authorized personnel.
6. Reasonable security: Adequate security safeguards should be put in place, according to the sensitivity of the data collected.

[5] Art. 3.6: 'controller' means the competent public authority which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law.
[6] Art. 3.7: 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
[7] Art. 3.15: 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 39.
[8] Art. 3.5 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

7. Accountability: Record keepers must be accountable for compliance with the other principles.

These Principles went into the *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, where the EU limited data transfers to non-EU countries only to those with "an adequate level of privacy protection" (art. 25.1), and stated for the first time the principle of "explicit consent" (art. 7).

Langheinrich (2001) was one of the first works to put in place some fundamental questions on privacy and ubiquitous computing: What differences in our lives will an ubiquitous environment make, and how can we extrapolate from these changes on how future privacy codes must be implemented and used, given the existing ones?

In May 2005, Kim Cameron, Chief Identity Architect of Microsof, worked out with a community of experts and eventually launched and blogged what she would call the "7 Laws of Identity" (http://www.identityblog.com/stories/2004/12/09/thelaws.html).Their main purpose are conscious and clear:

"The Internet was built without a way to know who and what you are connecting to" – Cameron stated. "This limits what we can do with it and exposes us to growing dangers. If we do nothing, we will face rapidly proliferating episodes of theft and deception that will cumulatively erode public trust in the Internet.

This paper is about how we can prevent the loss of trust and go forward to give Internet users a deep sense of safety, privacy, and certainty about whom they are relating to in cyberspace. Nothing could be more essential if Web-based services and applications are to continue to move beyond "cyber publication" and encompass all kinds of interaction and services. Our approach has been to develop a formal understanding of the dynamics causing digital identity systems to succeed or fail in various contexts, expressed as the Laws of Identity. Taken together, these laws define a unifying identity metasystem that can offer the Internet the identity layer it so obviously requires." [9]

This *Internet Identity Metasystem Layer* attracted a lot of attention. In a way, Cameron was advocating for a new kind of regulation, less concerned with the structural power of the states or even the effective power of big companies, and more focused on the practical facility of the end user himself. In addition, the reason for this shift was not to be found on the failure of the legal power of the states, but on the nature of the new digital environment for human behavior and action. As we will state later on, Cameron was thinking in architectural terms, rather than in legal or ethical ones. Here are the seven "laws":

1, User Control and Consent: Technical identity systems must only reveal information identifying a user with the user's consent.
2. Minimal Disclosure for a Constrained Use: The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

[9] "We need a *unifying identity metasystem* that can protect applications from the internal complexities of specific implementations and allow digital identity to become loosely coupled. This metasystem is in effect a system of systems that exposes a unified interface much like a device driver or network socket does. That allows one-offs to evolve towards standardized technologies that work within a metasystem framework without requiring the whole world to agree a priori." Cameron, 2005, ibid.

3. Justifiable Parties: Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
4. Directed Identity: A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.
5. Pluralism of Operators and Technologies: A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.
6. Human Integration: The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine ommunication mechanisms offering protection against identity attacks.
7. Consistent Experience Across Contexts: The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

In 2006, Ann Cavoukian, a well known expert in privacy issues and Ontario Information and Privacy Commissioner, was stroked by the similarity of these principles with FIPs, and she engaged herself into a systematic comparison between the two sets of principles.

The results are shown in the "Privacy-Embedded Laws of Identity" (Table 2), below, in which Cavoukian figures out a "universal identity metasystem"

The 7 Laws of Identity	The 7 Privacy-Embedded Laws of Identity
Law 1: **User Control and Consent**	**Law 1:** **Personal Control and Consent**
Technical identity systems	Technical identity systems must only reveal information identifying a user with the user's consent. Personal control is fundamental to privacy, as is freedom of choice. Consent is pivotal to both.
Law 2: **Minimal Disclosure for a Constrained Use**	**Law 2:** **Minimal Disclosure for Limited Use: Data Minimization**
The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution.	The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution. It is also the most privacy protective solution**.**
Law 3: **Justifiable Parties**	**Law 3:** **Justifiable Parties: "Need to Know" Access**
Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.	Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship. This is consistent with placing limitations on the disclosure of personal information, and only allowing access on a "need-to-know" basis.

Law 4: **Directed Identity**	**Law 4:** **Directed Identity: Protection and Accountability**
A universal identity metasystem must support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.	A universal identity metasystem must be capable of supporting a range of identifiers with varying degrees of observability and privacy. Unidirectional identifiers are used by the user exclusively for the other party, and support an individual's right to minimize data linkage across different sites. This is consistent with privacy principles that place limitations on the use and disclosure of one's personal information. At the same time, users must also be able make use of omnidirectional identifiers provided by public entities in order to confirm who they are dealing with online and, thereby ensure that that their personal information is being disclosed appropriately. To further promote openness and accountability in business practices, other types of identifiers may be necessary to allow for appropriate oversight through the creation of audit trials.
Law 5: **Pluralism of Operators and Technologies**	**Law 5:** **Pluralism of Operators and Technologies: Minimizing surveillance**
A universal identity solution must utilize and enable the interoperation of multiple identity technologies run by multiple identity providers	The interoperability of different identity technologies and their providers must be enabled by a universal identity metasystem. Both the interoperability segregation of identity technologies may offer users more choices and control over the means of identification across different contexts. In turn, this may minimize unwanted tracking and profiling of personal information obtained through surveillance of visits across various sites.
Law 6: **Human Integration**	**Law 6:** **Human Integration: Understanding is Key**
The identity metasystem must define the human user to be a component of the distributed system, integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks**.**	Users must figure prominently in any system, integrated through clear human-machine communications, offering strong protection against identity attacks. This will advance user control, but only if users truly understand. Thus, plain language in all communications used to interface with individuals is key to understanding. Trust is predicated on such understanding.
Law 7: **Consistent Experiences Across Contexts**	**Law 7:** **Consistent Experiences Across Contexts: Enhanced User Empowerment and Control**

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.	The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies. We return full circle to the concept of individual empowerment and informed consent. Clear interfaces, controls and options that enhance an individual's ability to exercise control across multiple contexts in a reliable, consistent manner will serve to enhance the principle of informed consent**.**

Table 2: Mapping of the Privacy-Embedded Laws of Identity. Source: Cavoukian (2006).

These principles can be combined with the privacy by design principles (PBDP) for the Internet. The new Directive encompasses, as a matter of fact, the result on the main discussions on this issue that followed to Cameron´s serious warning.

Cavoukian formulates PBDP along with the idea of *privacy by default* (PBDF) in 7 new laws suitable for audit matters to helping to built up this embedded identity protection as follows:

The 7 Foundational Principles of privacy by Design	**Explanation**
1. ***Proactive*** not Reactive; ***Preventative*** not Remedial	The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred − it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.
2. Privacy as the ***Default***	We can all be certain of one thing − the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy − it is built into the system, by default.
3. Privacy ***Embedded*** into Design	Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality**.**
4. **Full** Functionality – Positive-Sum, not Zero-Sum	Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-

	sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.
5. **End-to-End** Security – Lifecycle Protection	Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.
6. **Visibility and Transparency**	Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike. Remember, trust but verify!
7. **Respect for** User Privacy	Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric!

Table 3: The 7 Foundational Principles of Privacy by Design. Source: Cavoukian (2010).

The notions of privacy by design and by default were eventually incorporated into the EU Document *Digital Agenda for Europe* (2010)[10], which is the immediate precedent for the new regulations being put on place.

Two main Conferences have been already held in 2012 to discuss what we may term as the late consequences of the "privacy by design turn": (i) in USA, the IEEE Symposium on Security & Privacy (San Francisco, May 20-23) http://www.ieee-security.org/TC/SP2012/); (ii) in Europe, the 5th edition of the international conference Computers, Privacy and Data Protection (CPDP) 2012 "European Data Protection: Coming of Age", took place from 25 till 27 January 2012, http://www.cpdpconferences.org/cpdp2012.html#top, at Vrije Universiteit, Brussels.

[10] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Agenda for Europe, Brussels, 26.8.2010, COM(2010) 245 final/2,

The final formulation of the integration of the Fair Information Practice principles (FIPs), the 7 Identity Laws, and the Privacy by Design Foundational Principles, is shown in Table 4.

Privacy by Design **Foundational Principles**	***Fair Information Practice*** **Principle (GPS)**	**Extended Principles**
1. Proactive not Reactive; Preventative not Remedial		Demonstrable commitment to set and enforce high privacy standards. Evidence that methods to **recognize** poor privacy designs, to **anticipate** poor privacy practices and outcomes, and to correct the negative impacts proactively are established
2. Privacy as the Default	3. Purpose Specification 4. Collection Limitation, Data Minimization 5. Use, Retention and Disclosure Limitation	Privacy as the default starting point for designing and operating information technologies and systems represents the maximum personal privacy that one can have. That is, privacy becomes the prevailing condition - without the data subject ever having to ask for it - no action required.
3. Privacy Embedded into Design		Systemic program or methodology in place to ensure that privacy is thoroughly integrated into operations. It should be standards-based and amenable to review and validation All privacy threats and risks should be identified and mitigated to the fullest extent possible in a documented action plan.
4. Full Functionality – Positive-Sum, not Zero-Sum		All legitimate non-privacy interests and objectives are identified early, desired functions articulated, agreed metrics applied, and unnecessary trade-offs rejected in favour of achieving multi-functional solutions
5. End-to-End Security – Lifecycle Protection	7. Security	
6. Visibility and Transparency	2. Accountability 8. Openness 10. Compliance	
7. Respect for User Privacy	1. Consent 6. Accuracy 9. Access	

Table 4: The Mapping of FIPs into the Privacy by Design Foundational Principles. Source: Cavoukian (2010).

1.4.2 From Privacy by Design, back to Security by Design

This formulation deserved a great deal of comments and discussions, with a big impact on regulations and on the field. However, it is worthwhile noticing that the original statement of the "seven laws" by first discussants, coming mainly from the computer science field, has been recently increasingly leaned over the ethical and legal field. Cameron´s statements intended to be a technical formulation for an identity layer[11], a set of architectural notions: "the set of objective dynamics defining a digital identity metasystem capable of being widely enough accepted that it can serve as a backplane for distributed computing on an Internet scale". On the contrary, Cavoukian´s principles are normative, a golden standard proposal, a set of guidelines to be understood as a schema for evaluative and audit purposes aiming both at guide law, and ethical judgments.

"Contextual identity choices" —browsing, personal, professional, community, credit card, citizen— are, in their original formula, ways to make computable at the data ("thing") level all the different contextual aspects that can shift language meaning from one to another environment. It is a way to codify user's interrelated interfaces within changing scenarios.

This formula seems to be like the complementary side of the Web of Data, launched more or les at the same time by Tim Berners-Lee and the W3C (2006). To sum up, we reproduce the 2009 reformulation of the three Berners-Lee "simple" rules of the Linked Open Data approach[12]:

1. All kinds of conceptual things, they have names now that start with HTTP.
2. I get important information back. I will get back some data in a standard format which is kind of useful data that somebody might like to know about that thing, about that event.
3. I get back that information it's not just got somebody's height and weight and when they were born, it's got relationships. And when it has relationships, whenever it expresses a relationship then the other thing that it's related to is given one of those names that starts with HTTP.

In both approaches, architectural (Cameron/Cavoukian) or relational (Berners-Lee/W3C), user *empowerment* is the key concept. However, empowerment in both formulations means to gaining control not only over its own data but over the environment in which data can be versed, gathered, aggregated and eventually reused.

Therefore, control over the data to be linked and reused becomes crucial. Trust and security are the two sides of the same token. And, sometimes, as Pagallo (2012) is suggesting, they might be incompatible. "Instead of letting people determine autonomously levels of access and control over personal data, depending on personal choices and circumstances, the use of self-enforcement technologies seems incompatible with a basic tenet of the democratic rule of law—autonomy." Limits of the privacy-by-design approach (at least as plotted by Kavoukian), have to be taken into account.

[11] "This investigation has led to a set of ideas called the "Laws of Identity". We chose the word "laws" in the scientific sense of *hypotheses about the world – resulting from observation – which can be tested and are thus disprovable*. The reader should bear in mind that we specifically did not want to denote legal or moral precepts, nor embark on a discussion of the "philosophy of identity". Cameron, ibid. 4/11/2005.

[12] http://www.ted.com/talks/tim_berners_lee_on_the_next_web.html *TED Talk,* 2009

One of the most insightful challenges has been formulated by Stuart S. Shapiro (2010: 29), asking from the ACM: *if privacy by design is still a ways off, and security by design still leaves something to be desired, how do we get there from here?* Shapiro advocates for the emergence of expertise able to gather both kinds of knowledge in an integrated framework. "*Security by design and privacy by design can be achieved only by design*. We need a firmer grasp of the obvious." (ibid.)

Let´s come back to cloud computing to restate this point. According to the NIST standards the cloud model is composed of five essential characteristics, three service models, and four deployment models (Srivasta, 2011; also Reddy and Reddy, 2011; Shaikh and Sasikumar, 2012). The five essential characteristics are: On-demand self-service, broad network access, resource pooling, rapid elasticity, measured service.

The service models are as follows:

• Software as a Service (SaaS): Use provider's applications over a network for example, Google Docs.
• Platform as a Service (PaaS): Deploy customer-created applications to a cloud for example, Microsoft Azure.
• Infrastructure as a Service (IaaS): Rent processing, storage, network capacity and other fundamental computing resources (for example Salesforce.com)

The deployment models, which can be either internally or externally implemented, are summarized in the NIST presentation as follows:

• Private cloud—Enterprise owned or leased
• Community cloud—Shared infrastructure for specific community sharing common interests
• Public cloud—Sold to the public, mega-scale infrastructure
• Hybrid cloud—Composition of two or more clouds

Cloud computing possesses several advantages over regular one (elasticity, scalability, multi-tenancy, ease of use, reduced cost…). It is especially prone to web services, because the cloud can consider as cloud services either infrastructures, platforms, or software (Shaikh and Sasikumar, 2012). However, it is more sensitive to external attacks. Table 5 summarizes the issues at stake:

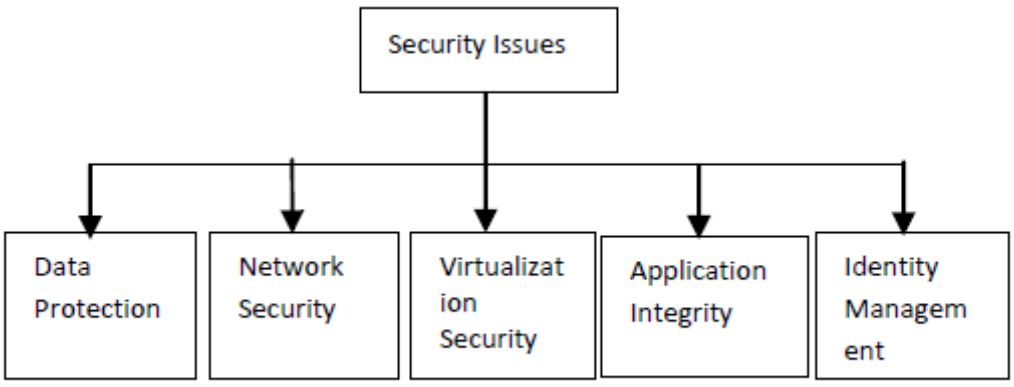

Table 5: Classification of Security Issues. Source: Shaikh and Sasikumar, 2012.

Srivasta et al. (2011) have recently elaborated as follows the risks of public and private clouds as the new computational framework to be operated in the web:

Threats	Public Cloud	Private Cloud
Abuse and Nefarious Use of Cloud Computing	✓	×
Insecure Interfaces and APIs	✓	✓
Malicious Insiders	✓	×
Shared Technology Issues	✓	✓
Data Loss or Leakage	✓	×
Account or Service Hijacking	✓	×
Unknown Risk Profile	✓	×

Table 6. Threads affecting public and private clouds. Source: Srivasta et al. (2011)

This is an interesting approach, because threads into the cloud *only* can be tackled by means of a conscious policy making ruling. It is not automatic; some decisions have to be taken to protect the cloud at every computation level. According to Srivasta et al. (2011) at least it should address all the issues of the Gartner Seven Security Risks of Cloud Computing:

- *Privileged User Access* (accountability of the provider)
- *Regulatory Compliance* (hird party audits and exhibit due care for regulatory concerns)
- *Data Location* (location independence)
- *Data Segregation (*encryption schemes)
- *Recovery* (In event of a disaster data must be Recoverable)
- *Investigative Support*
- *Long Term Viability (*Acquisition and mergers at the service provider)
- *Non-proprietary technologies* (Open Virtualization Format)
- *Data management* (describe the exact data management policies adopted by the service provider).
- *Application security* (periodic application of security tests)
- *Security model of cloud provider interface* (*Secure APIs:* security model of the interfaces)
- *Provider HR Policy* (to investigate the HR Policy of the Provider)
- *Secure data deletion* (securely wipe persistent data in accordance with industry standard guidelines like the NIST Special Publication 800-88: Guidelines for Media Sanitization)
- *Defense in Depth* (2-factor authentication should be used where possible)
- *Information from Provider* (The provider must disclose appropriate logs)

If the target of “co-offending networks” that we proposed as a redefinition of “organized crime” (Section 1.2.2.) is accepted, then security issues can be redefined as well according to this main purpose of harmonizing data protection and collective security. CAPER offers a way to address such a purpose, by means of what we well define as a “regulatory model”.

1.4.3 Police Interoperability, Networked Governance, and Data Governance

Police and technology have not always had an easy relationship. Technology is sometimes perceived only as an instrumental way to conduct investigations, and not as a key for coordination and more efficient institutional performance. A recent empirical study carried out by Bart Custers in the Netherlands (2012) shows the existence of legal, organizational and technology obstacles in policing (Fig. 3).

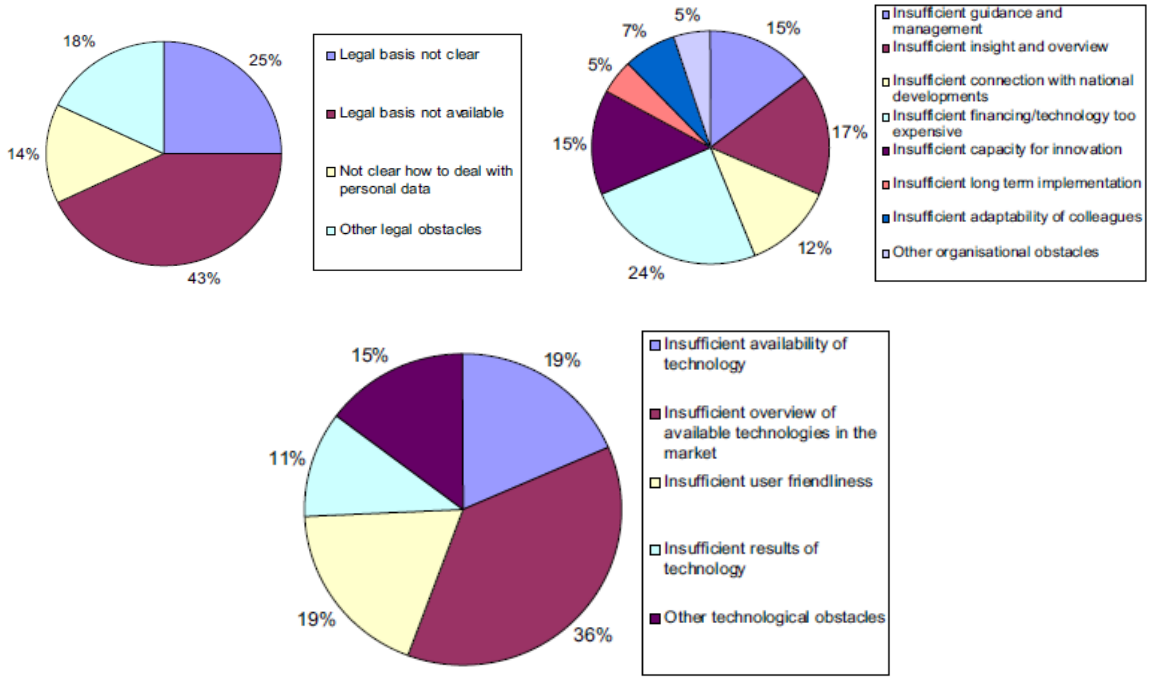

Fig. 3. Legal, organizational and technological obstacles. Source: Bart Custers (2012: 66)

Overall wiretapping, fingerprints, GPS/position tracking devices, camera surveillance and DNA were the most often used technologies by respondents to the survey. (Custers, ibid.). However, the challenge for technology to be effectively used lies on the way these results, as data, can be linked, shared and reused along the nodes of a police network.

Bennell et al.(2012) express clearly some doubts about “computerized crime linkage systems”. Brief, according to the authors, the possibility to build such systems is based in some non-checked or non-proved assumptions.

"These assumptions are that (a) data contained in the systems can be coded reliably, (b) data contained in the systems are sufficiently accurate to draw meaningful inferences, (c) violent serial offenders exhibit consistent but distinctive patterns of behavior across their crimes that will enable the linking process, and (d) analysts possess the ability to identify such patterns and link crimes accordingly." (ibid. 623).

Human, legal, and organizational obstacles should be taken into account and carefully described. However, we think that mature technologies can tackle this kind of problems with a minimum of reliability. The condition would be to comply with the policy making principles embedded into the toolkit. In other words, police interconnectivity and system interoperability should be treated as a form of *governance*, and more precisely, as a form of *networked data governance*. Let's flesh out these notions before coming back to the CAPER model.

We will put at work together three notions: (i) *interoperability*, (ii) *networked governance*; (iii) and *data governance*.

(i) Paul de Hert and Serge Gurwitth (2006: 33) pointed out the narrow definition of interoperability supported by the EU Commission in The *Communication from the Commission to the Council and the European Parliament on improved effectiveness enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs* (2005) [13]. The *Communication* defines 'interoperability' as the "ability of IT systems and of the business processes they support to exchange". This seems to trim the notion to a technical issue, avoiding its political and legal implications. On the contrary, de Hert and Gurwith argue that interoperability is a complex issue involving several layers and dimensions. Regarding interoperability of police databases, they recover three guidelines already stated by the criminologist H. Herold in1977:

(1) Sharing should only be possible for law enforcement purposes;
(2) The receiving party can only 'get' the information when he or she uses it for the purposes that have initially led to its gathering by the sending party;
(3) The general principle of efficiency in state administration practice.

"Interoperability of systems enables interoperability of organizations. Systems interoperability is concerned with the ability of two or more systems or components to exchange information and to use the information that has been exchanged. Organizational interoperability is concerned with the ability of two or more units to provide services to and accept services from other units, and to use the services so exchanged to enable them to operate effectively together .Semantic interoperability is part of the interoperability challenge for networked organizations. Inter-organizational information systems only work when they communicate with other systems and interact with people". (Gottschalck, 2009)

(ii) Governance is a widely used concept in political science and management studies *Network governance* refers to the relational structure which allows the emergence of an ordered regulation among networks of organizations (companies, administrations,

[13] Commission of the European Communities Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM (2005) 597 final, Brussels, 24 November 2005.

governments…). Rhodes (2007: 1244) refers broadly to "policy networks" in the public domain. "The term 'policy network' refers to sets of formal and informal institutional linkages between governmental and other actors structured around shared interests in public policymaking and implementation". Those are the elements that compound them (ibid. 1245; for a strong criticism facing the EU powers and functioning, cfr. Coen and Thatcher, 2008[14]):

(a) Any organization is *dependent* upon other organizations for *resources*.
(b) In order to achieve their *goals*, the organizations have to exchange resources.
(c) Although decision-making within the organization is constrained by other organizations, the *dominant coalition* retains some discretion. The *appreciative system* of the dominant coalition influences which relationships are seen as a problem and which resources will be sought.
(d) The dominant coalition employs *strategies* within known *rules of the game* to regulate the *process of exchange*.
(e) Variations in the degree of *discretion* are a product of the goals and the relative power potential of interacting organizations. This relative power potential is a product of the resources of each organization, of the rules of the game and of the process of exchange between organizations.

When technology comes into play, governance acquires a dimension of e-governance or, more precisley, *IT governance*.

"*Public-sector IT Governance* has not yet been defined in a widely accepted fashion in scholarly research. However, on a general plain, (public) *governance* has been defined "as regimes of laws, administrative rules, judicial rulings, and practices that constrain, prescribe, and enable government activity, where such activity is broadly defined as the production and delivery of publicly supported goods and services. When transposing this broad definition of governance to public-sector governance of IT, one could define IT governance as "regimes of IT-related standards, agreements, methods, rules, and practices that constrain, prescribe, and enable the implementation and use of ICTs to support government activity." (Scholl et al, 2011, 343)

In a most quoted recent article, Provan and Kennis (2012, 229) assume impliciltly that complex networks have a legal, organizational and a technological side. "By network functioning, we refer to the process by which certain network conditions lead to various network-level outcomes". (...) "We define the term ''network'' narrowly. Our focus is on groups of three or more legally autonomous organizations that work together to achieve not only their own goals but also a collective goal. Such networks may be self-initiated, by network members themselves, or may be mandated or contracted, as is often the case in the public sector. When defined in this way, as multilateral collectivities, networks can become extremely complex entities that require explanations that go well beyond the dyadic approaches that have been traditionally discussed in the organization theory and strategic management literatures" (ibid. 231).

[14] "The new networks have been given a wide range of tasks and broad membership, but enjoy few formal powers or resources. They are highly dependent on the European Commission and ace rivals for the task of co-ordinating European regulators. Thus institutional terms the spread of network governance has in fact been limited." (ibid.

What they propose is to combine the network analytical and governance perspectives. Therefore, according to the latter, the network itself is considered to be the units of analysis; and according to the former, networks are a set of actors or nodes, with relationships between these nodes. Table 7 shows the structural patterns they identify from the two integrated perspectives:

Governance Forms	Trust	Number of Participants	Goal Consensus	Need for Network - Level Competencies
Shared governance	High density	Few	High	Law
Lead organization	Low density, highly centralized	Moderate number	Moderately low	Moderate
Network administrative organization	Moderate density, NAO monitored by members	Moderate to many	Moderately high	High

Table 7. Key Predictors of Effectiveness of Network Governance Forms. Source: Provan and Keniis, 2012: 237)

They conclude that "Network Administrative Organizations network governance will be most effective for achieving network-level outcomes when trust is moderately to widely shared among network participants (moderate density trust), when there are a moderate number to many network participants, when network-level goal consensus is moderately high, and when need for network-level competencies is high". (ibid. 247).

This is the case for all the CAPER LEAs. However, to complete the broad picture, another kind of governance dimension is required. We will refer to it as *data governance.*

(iii) *Data Governance* is a quite recent notion, not developed yet in the public domain. It comes from the field of *corporate governance*, regarding the kind and level of decisions to be taken regarding data. According to Otto (2011), there is broad consensus among researchers that Data Governance must find answers to three questions:

- What decisions, with regard to corporate data, need to be made on an enterprise wide level?
- Which roles are involved in the decision-making process?
- How are the roles involved in the decision-making process?

Otto draws the relationship of fundamental concepts of Data Governance as follows (Fig. 4):

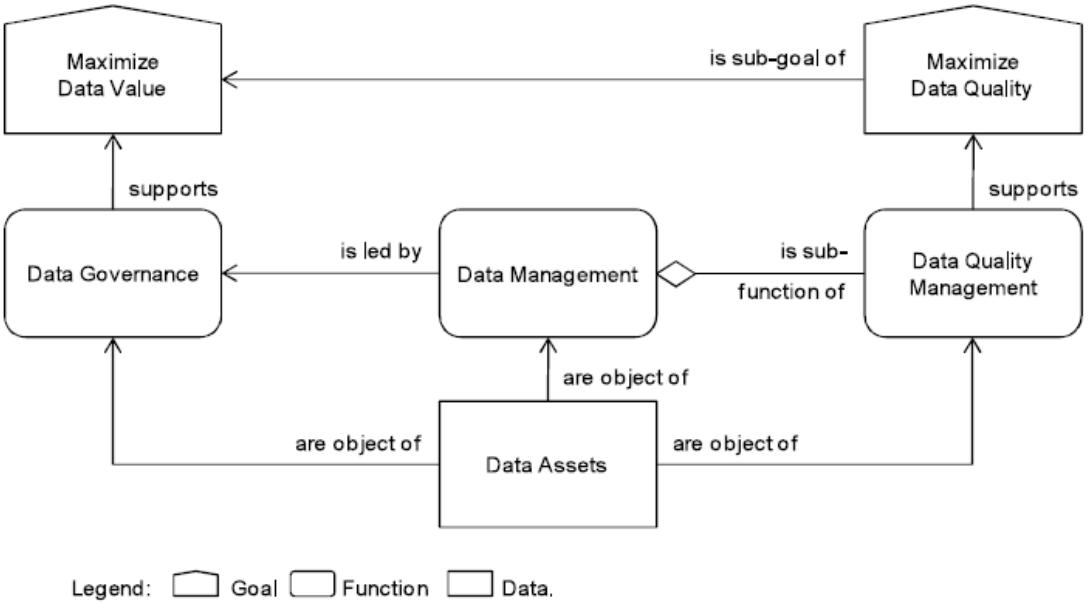

Fig. 4 Fundamental Concepts of Data Governance. Source: Otto (2011: 242)

For a company, it is clear that the goals are to maximize the value of their assets, and those are the main guidelines for data government. Khatri and Brown (2010) align data governance domains, domain decisions, and potential roles of accountability in the way it is showed in Table 8. They start identifying five structured and related domains: (i) data principles, (ii) data quality, (iii) metadata, (iv) data access, and (v) data lifecycle.

There is no equivalent table for data governance for public organizations such the police, but this is a quite precise framework to be implemented to regulate data eliciting, storing and sharing in public databases as well. In this case, as we will describe in the next sect, rule compliance and the setting of a regulatory model can help to the proper monitoring of both the information flow between LEAs and the rights of citizens (privacy and data protection).

The conception of CAPER architecture as a service facilitates the regulatory issues as a type of networked governance, mainly centred in data processing and storing, and showing the following features: asymmetric between the stakeholders, multi-layered (syntactic, semantic and processing levels), hybrid (covering different types of roles and functions) and addressed to different kinds of relationships [(Government-to-Citizens (G2C), Government-to-Business(G2B),Government-to-Government(G2G)].

Data Governance Domains	Domain Decisions	Potential Roles or Locus of Accountability
Data Principles • Clarifying the role of data as an asset	• What are the uses of data for the business? • What are the mechanisms for communicating business uses of data on an ongoing basis? • What are the desirable behaviors for employing data as assets? • How are opportunities for sharing and reuse of data identified? • How does the regulatory environment influence the business uses of data?	• Data owner/trustee • Data custodian • Data steward • Data producer/supplier • Data consumer • Enterprise Data Committee/ Council
Data Quality • Establishing the requirements of intended use of data	• What are the standards for data quality with respect to accuracy, timeliness, completeness and credibility? • What is the program for establishing and communicating data quality? • How will data quality as well as the associated program be evaluated?	• Data owner • Subject matter expert • Data quality manager • Data quality analyst
Metadata • Establishing the semantics or "content" of data so that it is interpretable by the users	• What is the program for documenting the semantics of data? • How will data be consistently defined and modeled so that it is interpretable? • What is the plan to keep different types of metadata up-to-date?	• Enterprise data architect • Enterprise data modeler • Data modeling engineer • Data architect • Enterprise Architecture Committee
Data Access • Specifying access requirements of data	• What is the business value of data? • How will risk assessment be conducted on an ongoing basis? • How will assessment results be integrated with the overall compliance monitoring efforts? • What are data access standards and procedures? • What is the program for periodic monitoring and audit for compliance? • How is security awareness and education disseminated? • What is the program for backup and recovery?	• Data owner • Data beneficiary • Chief information security officer • Data security officer • Technical security analyst • Enterprise Architecture Development Committee
Data Lifecycle • Determining the definition, production, retention and retirement of data	• How is data inventoried? • What is the program for data definition, production, retention, and retirement for different types of data? • How do the compliance issues related to legislation affect data retention and archiving?	• Enterprise data architect • Information chain manager

Table 8. Framework for data decision domain. Source: Khatri and Brown (2010).

1.4.4 The CAPER Regulatory Model (CRM)

As stated in CAPER Deliverable WP2 *Architecture Modeling* :

“SOA [Service Oriented Architecture] architecture is a software architecture where every component is designed as a service. (...) This way, it is possible to develop applications/functionalities composed by interoperable Services. CAPER is supposed to be constituted from a bunch of different applications that together will build an application capable of performing unstructured data analysis from different media sources.”

Furthermore, CAPER Technical Report *Visualisation & Data Mining Tools For Visual Analytics Framework Report* (WP6), after listening to LEAs requirements *for Visual Analytics Workflow Management Support,* aims at "making our way of processing this data transparent for an analytic discourse". Three goals are envisaged:

"a) Implementing a framework that realises the task of connecting multiple data sources with multiple visualisation techniques via a standardised data interface and includes support for data-mining components.

b) Enabling a quick and robust import of data types from disparate data sources in order to improve the ability of different LEAs to work collaboratively.

c) Supporting pattern discovery, documentation and reuse, thus progressively increasing detection capabilities "

The CAPER approach has four major components: (i) Data harvesting (knowledge acquisition: data gathering), (ii) Analysis (content processing), (iii) Semantic Storage and Retrieval, and (iv) Access Control.

Figures 5 and 6 plot the intended architecture. We have signaled on them the three conflicting areas in which rights and duties have to be harmonized trough a single regulatory model. They regard access and data gathering; data processing; and data storing and retrieval.

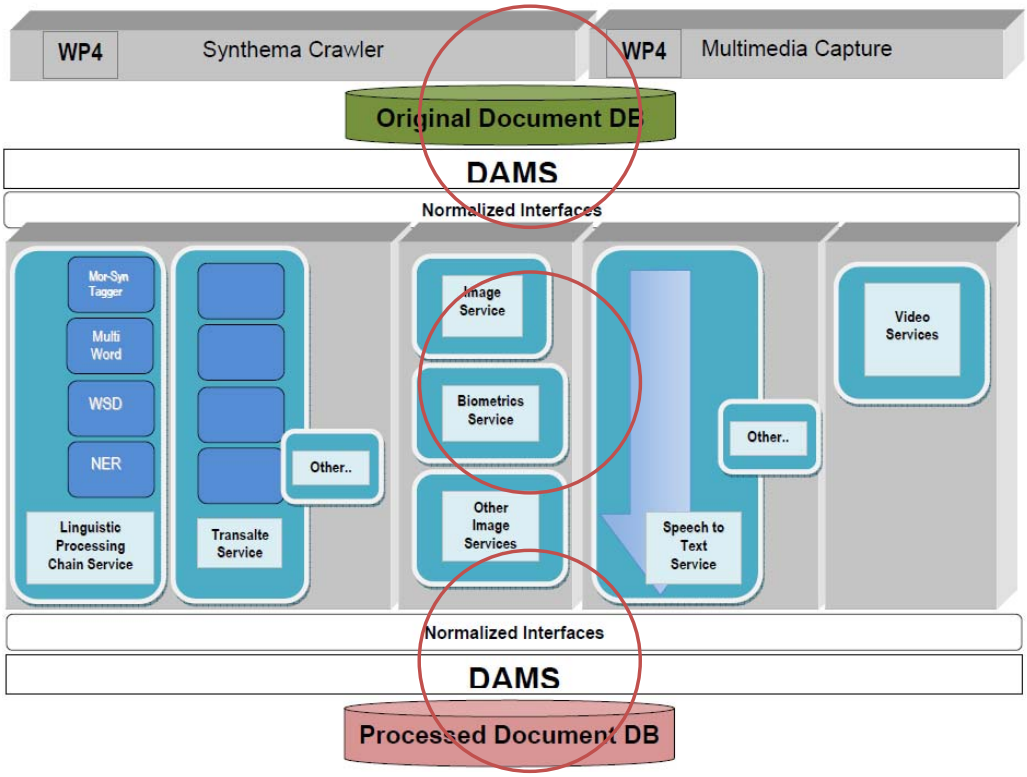

Fig. 5. CAPER Preliminary Architecture

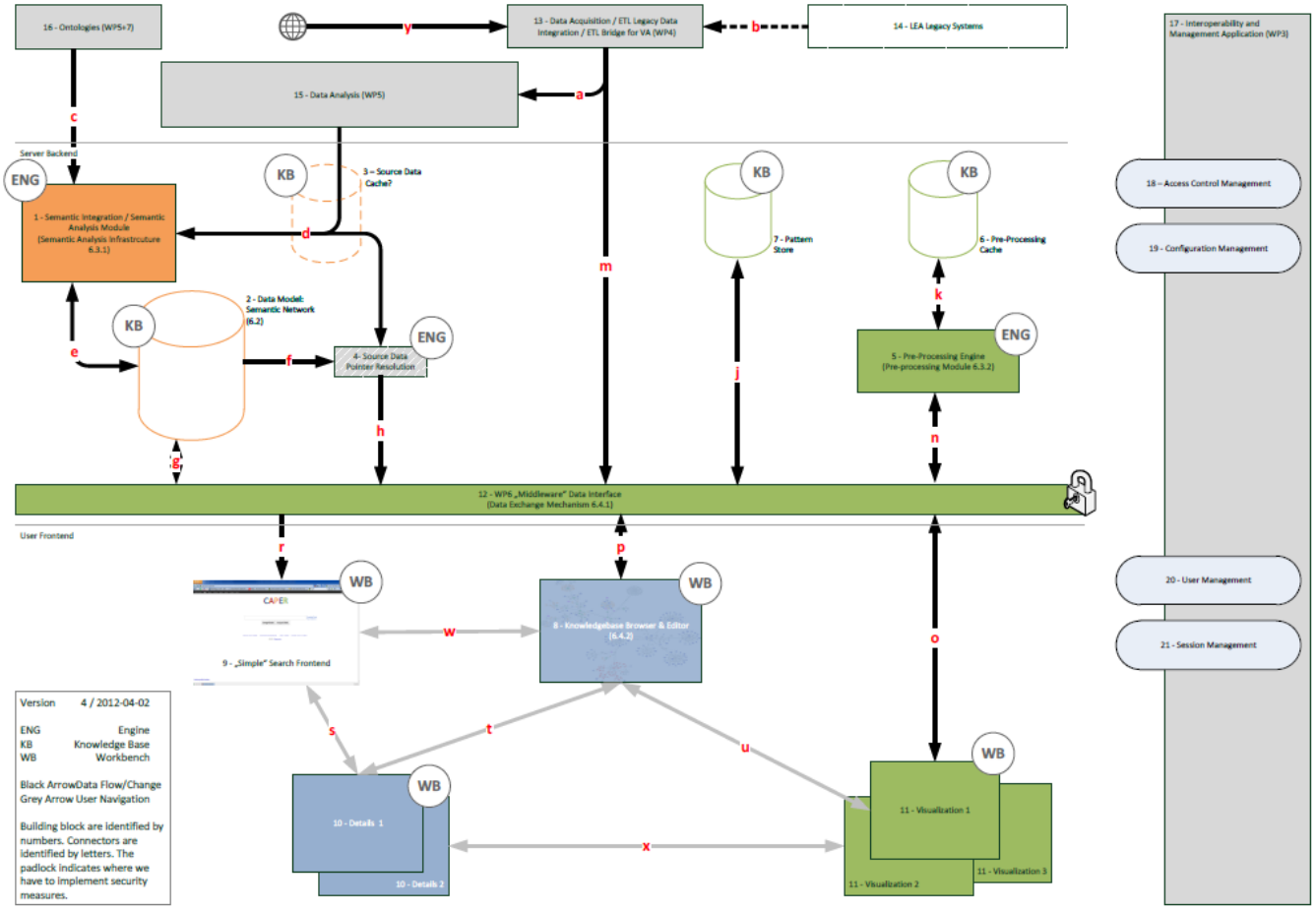

Fig. 6. CAPER Architecture

From a practical perspective however we need to come up with architectures that can enable LEAs to work with sensitive data. These are some specific requirements:

1) Each data owner (or national police unit) controls access to their own data.
2) Each data owner should comply with the different national, European, international and particular rules and pattern regulations that feed the different dimensions of the CAPER regulatory model.
3) Each data owner should protect not only the rights and data of their national citizens fellows, but the privacy requirements of all human beings, according to the principles of the proposed EU Directive and Regulation.
4) A data owner should be able to grant access to their data to other (foreigner) police units
5) Any architecture designed for data sharing should scale with the number of data owners.
6) Computation on data should be done in such a way as to not reveal anything other than the result of the computation.

This should be the lowest common denominator to build up the kernel of the regulatory model. As shown in Fig. 7, such a model is conceptually constructed stemming from four nodes, each of them with three edges:

1. Hard Law [Security, Data Governance, Data Protection]
2. Soft Law [Security, Data Protection, Privacy]
3. Networked Governance [Data Governance, Data protection, Privacy]
4. Ethics and Good Practices [Security, Privacy, Data Governance]

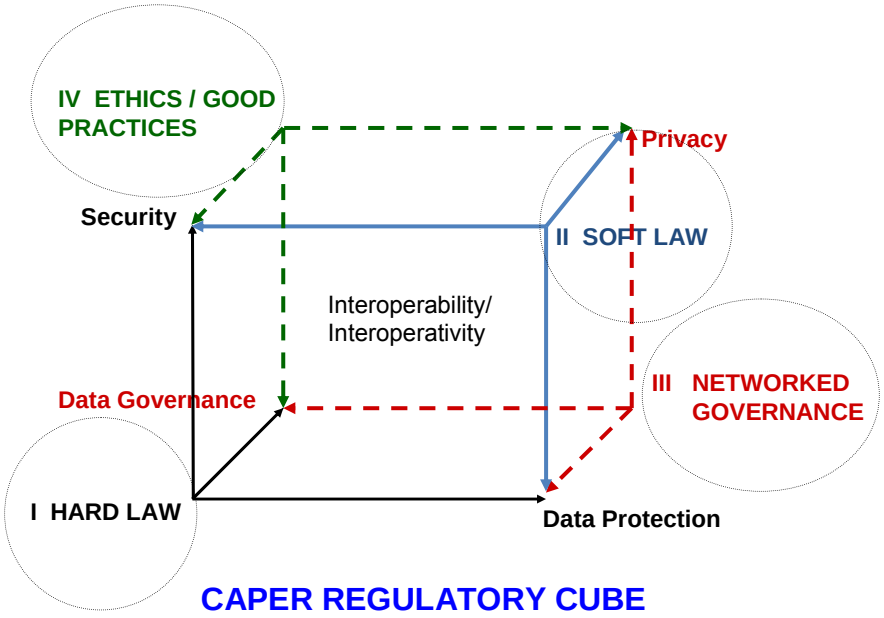

Fig. 7. CAPER Regulatory Model (CRM)

The idea behind this model is that hard law is differently compulsory for all LEAs involved. All of them must comply with the European Regulation, which can be enforced uniformly, but as for the Directive, each country will transport it into their own national legislation in a different way. Therefore, to comply both with legal requirements and with the goals of CAPER, hard law (binding law) must be complemented with other kinds of regulations —soft law, networked governance, and good practices and ethical principles. Do notice that dialogue and communication with other partners (LEAs), political representatives, social representatives, and citizens, are conditions for the overall system to work. This regulatory model cannot be in itself imposed authoritatively; CRM implementation has to be negotiated on local bases and on case-based concrete situations.

This is why we cannot represent the legal value of CRM as a discrete category application (legal or illegal decisions; valid or invalid behaviors), but as a gradual steps in a double-entry *continuum*, as plotted in Fig. 8., in which social practices, good practices, soft law, and hard law, are connected in a legal flow. Networked governance, data protection, and data governance are managed trough the compliance of regulations in different contexts and scenarios that might involve many stakeholders (citizens, police units, regulators, national

authorities, etc…). Even if police has to comply and obey to national government, the implementation of web services cannot only follow the top-down direction of criminal national policies. This is not a exclusive feature of CAPER. All web services regulations must combine top-down and bottom-up implementations. The difference is

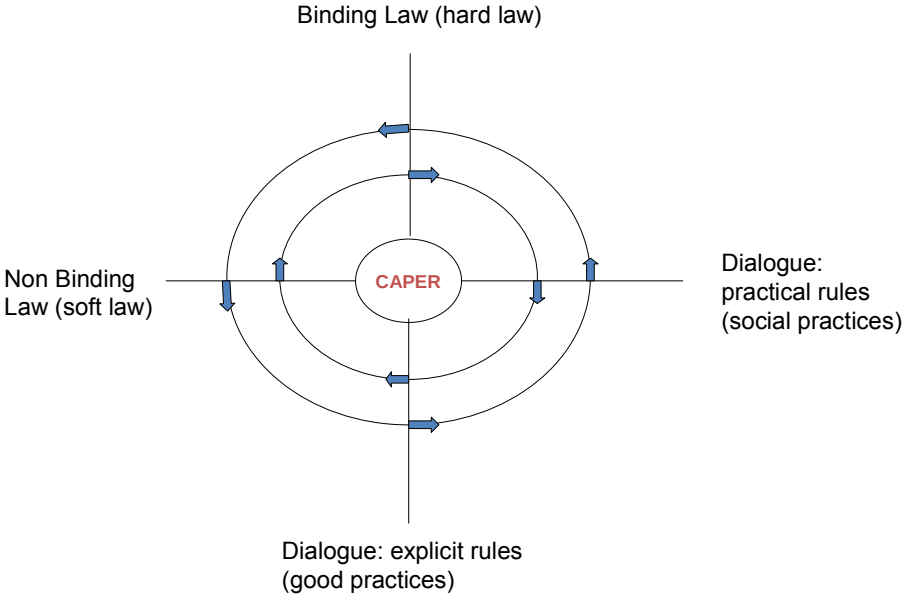

Fig. 8. Legal value flow of the CRM

We should distinguish too between two correlated and intertwined dimensions at the kernel of the regulatory cube: *interoperability*, which is related to computer systems and languages, and *interoperativity*, which covers the structural and organizational side of administrations and governments. Figure 9 reshapes Fig. 2 regarding the institutional strengthening of regulatory levels. Interoperability and interoperativity are plotted as the two axes of a scaling and gradual matrix, in which hard law, soft law, governance and good practices (and ethics) constitute the embedded regulatory layers of CAPER platform.

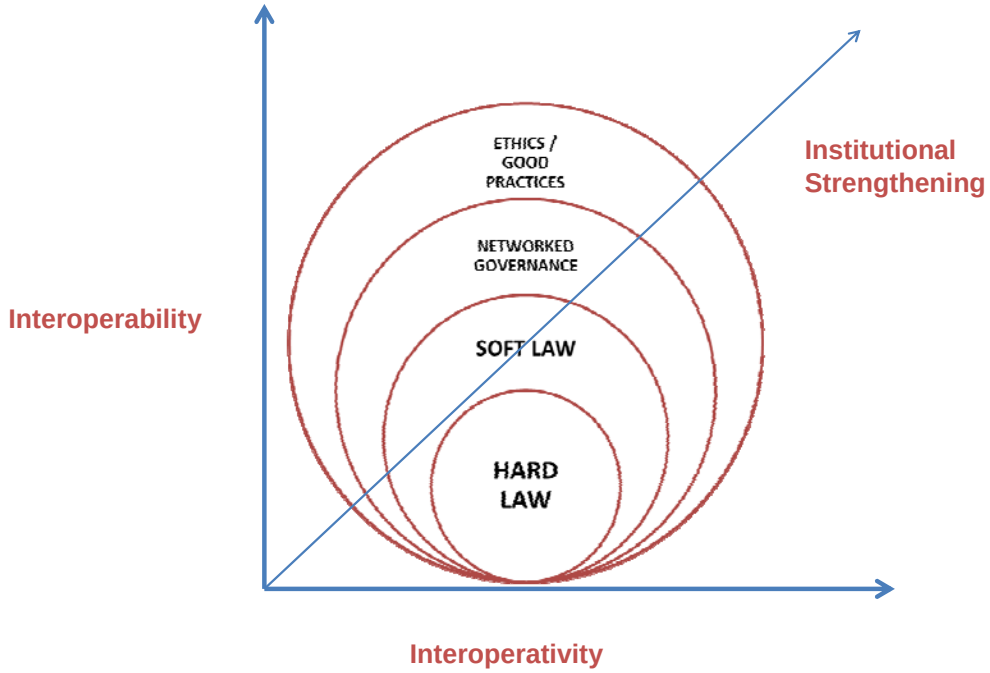

Fig. 9. CRM Interoperability/interoperativity axes

.

1.4.5 Ethical compliance

1.5 Corresponding planned work in Annex I

Give a reminder of the planned work as in annex I (copy of annex I expected outcome)

2 THE LEGAL FRAMEWORK

This section offers....

2.1 The Right to Privacy and Data Protection in Europe and Israel

Text here

2.1.1 Art. 8 of the Chart of Fundamental Rights of the European Union

Text here

2.1.2 Art. 16 of the Treaty on the Functioning of the European Union

Text here

2.1.3 Directive 95/46/EC

Text here

2.1.4 Directive 2002/58/EC

Text here

2.1.5 The Hague Programme: Ten priorities for the next five years – The Partnership for European renewal in the field of Freedom, Security and Justice. Communication from the Commission to the Council and the European Parliament COM/2005/0184

Text here

2.1.6 *TBD* (*other? e.g. new EU Regulation of the EU Parliament and of the Council on the protection of individuals with regard to the processing of personal data*)

Text here

2.1.7 Israel (*BAK to deepen the general privacy discipline applicable in the country*)

Text here

2.2 Section 2

2.2.1

2.2.2

2.2.3

2.2.4 Sub section

2.3 Section …

2.3.1 Eeeee

2.3.2 Eeee

2.3.3

2.3.4 Sub section

3 CONCLUSION

Emphasize the main achievements vs the initial objectives of the deliverables,
In summary give a conclusion on whether the deliverable has reached its goal or not, (<1 page)

4 REFERENCES

Abbott, Kenneth W.; Snidal, Duncan. "Hard Law and Soft Law in International Governance" , *International Organization*, Summer 2000, 54 (3): 421-456.

Ayling, Julie*. Gang change and evolutionary theory, Crime* Law and Social Change (2011) 56:1–26

Becquai, August. "Organized Crime Goes Cyber**",** Computers & Security, 20 (2001) 475-478.

Bennell, Craig; Snook, Brent;Macdonald, Sarah; House, John C. ;Taylor, Paul J. "Computerized Crime Linkage Systems : A Critical Review and Research Agenda" *Criminal Justice and Behavior* 2012 39: 620.

Cameron, Kim. *The Laws of Identity* …as of 5/11/2005. Microsoft Corporation.

Carr, John. "New Approaches to Dealing with Online Child Pornography*", Cybersecurity Summit*, (WCS), 2011 Second Worldwide, 1-3.

Cavoukian, Ann. "7 Laws of Identity: The Case For Privacy-Embedded Laws of Identity in the Digital Age", *Technology*, Ontario Information and Privacy Commissioner, October 2006, 1-24.

Cavoukian, Ann. "Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair information Practices. Information an Privacy Commissioner, Ontario, Canada, 2010.

Choo, Kim-Kwang Raymond. "Organised crime groups in cyberspace: a typology", *Trends in Organized Crime* (2008) 11:270–295.

Choo, Kim-Kwang Raymond ; Smith, Russell G. "Criminal Exploitation of Online Systems by Organised Crime Groups", *Asian Criminology* (2008) 3:37–59.

Coen, David; Thatcher, Mark. "Network Governance and Multi-level Delegation: European Networks of Regulatory Agencies", *Jnl Publ. Pol. 29*, I (2008): 49-71.

Cunningham, Scott; Kendall, Todd D. "Prostitution 2.0: The changing face of sex work", *Journal of Urban Economics* 69 (2011) 273–287**.**

Custers, Bart. "Technology in policing: Experiences, obstacles and police needs", *Computer Law & Security Review* 28 (2012): 62-68.

Danialatou, Vasiliki; Ioannidis, Sotiris. "Security and Privacy Architectures for Biomedical Cloud Computing", *Information Technology and Applications in Biomedicine* (ITAB), 2010 10th IEEE International Conference.

De Hert, Paul; Gutwirth, Serge. “Interoperability of Police Databases within the EU: An Accountable Political Choice? “, International Review of Law Compters & technology, vol. 20, March July 1,2 (2006): 21-35.

De Hert, Paul; Papakonstantinou, Vagelis. “The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals”, *Computer Law & Security Review* 28 (2012): 130-142.

De Joode, Alex. “Effective corporate security and cybercrime”, *Network Security*, September 2011, pp. 16-18.

Goodman, Marc. “What Business Can Learn From Organized Crime”. November 2011 *Harvard Business Review* (2011) November: 27-30.

Gottschalk, Petter. “Maturity levels for interoperability in digital government”, *Government Information Quarterly* 26 (2009) 75–81

Grabosky, Peter. “The Internet, Technology, and Organized Crime”, *Asian Criminology* (2007) 2:145–161.

Hon, Kuan W.; Millard, Christopher, Walden, Ian. “Who is responsible for ‘personal data’ in cloud computing?—The cloud of unknowing, Part 2”, *International Data Privacy Law (2011) doi: 10.1093/idpl/ipr025* First published online: December 6, 2011.

Karlsson-Vinkhuyzen, Sylvia; Vihma, Antto. “Comparing the legitimacy and effectiveness of global hard and soft law: An analytical framework”, *Regulation & Governance* (2009) 3: 400–420.

Kaza, Siddarth; Xu, Jennifer; Marshall, Byron; Chen, Hsichun. “Topological Analysis of Criminal Activity Networks in Multiple Jurisdictions”, *dg.o '05 Proceedings of the 2005 national conference on Digital government research*, 2005, 251-252.

Khatri, Vijay; Brown, Carol V. “Designing Data Governance”, *Communications of the ACM* , vol. 53 , 1 (2010): 148-152.

Langheinrich, Marc. “Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems”, in Gregory D.A. Abowd, B. Brumitt S.A. Shafer (Eds.), *Proceeding UbiComp '01 Proceedings of the 3rd international conference on Ubiquitous Computing*, Springer, London, 2001, pp. 273-291.

McDonald, Carina Louise. *Terror 2.0? Salafi-Jihadist Terrorist use of the Internet*. Thesis, The Centre for Military and Strategic Studies, Calgary, Alberta, August, ProQuest, 2010.

Morris, Mel. “Intelligence, knowledge and organised crime”, *Computer Fraud & Security,* April 2010, 13-15.

Otto, Boris. “Data Governance”, *Business & Information Systems Engineering* 4 (2011): 241-244

Pagallo, Ugo. “On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law”, in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?* , Springer Verlag, 331-346.

Ritzer, George; Dean, Paul; Jurgenson, Nathan**.** “The Coming of Age of the Prosumer”, A*merican Behavioral Scientist* 56(4): 379–39.

Roberts, Nancy C. “Beyond Smokestacks and Silos: Open-Source, Web-Enabled Coordination in Organizations and Networks”, *Public Administration Review*, 677-693.

Shaik, Rizwana; Sasikumar, M. “Security issues in Cloud Computing: A Survey”, International Journal of Computer Applications (0975-8887), vol. 44 (19) April 2012: 1-10.

Shapiro, S., Stuart. “Inside Risks Privacy By Design: Moving from Art to Practice”, *Communications of the ACM*, vol. 53, n. 6, june 2010: 27-29.

Scholl, Hans Jochen; Kubicek, Herbert; Cimander, Ralf. “Interoperability, Enterprise Architectures, and IT Governance in Government”, in M. Janssen et al. (Eds.), EGOV 2011, LNCS 6846, Springer Verlag, Heidelberg, Berlin, pp. 345–354, 2011.

Solms von, Basie; Solms, von, Rossouw, “The 10 deadly sins of information security management”, *Computers & Security* (2004) 23, 371-376.

Srivastava, Prashant; Singh, Satyam; Pinto, A. Alfred; Verma, Shyetank; Chaurasiya Vijay K.; Gupta, Rahul. “An architecture based on proactive model for security in cloud computing”, IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, MIT, Anna University, Chennai. June 3-5, 2011, pp. 661-666.

Tayebi, Mohammad; Glässer, Uwe. “Organized Crime Structures in Co-offending Networks” , 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing.

Valentine, J. Andrew. “Compliance complacency: How ‘check-box’ compliancy remains a pitfall for many organizations worldwide”, (Verizon) Information Security Technical Report 15 (2010): 154-169.

Van Der Heijden, T. “Measuring Organized Crime in Western Europe”. In Milan, Pagon (eds.) *Policing in Central and Eastern Europe: Comparing First Hand Knowledge with Experience from the West*, Slovenia: College of Police and Security Studies, 1996.

Van Dijk, Maarten. “Discussing Definitions of Organised Crime: Word Play in Academic and Political Discourse”, *HUMSEC Journal*, (2007) 1: 65-90.

Van Eecke, Patrick; Craig, Cameron; Halpert, Jim. “The first insight into the European Commission´s proposal for a New European Union Data Protection Law”, *Journal of Internet Law* , February 2012, pp. 19-22.

Vivacqua, Adriana S.; Borges, Marcos S-R "Taking advantage of collective knowledge in emergency response systems", *Journal of Network and Computer Applications* 35 (2012): 189–198.

5 ANNEXES

5.1 Planned Work

D7.1-01	Pompeu Casanovas	First Version Framework/Networked governance	
D7.1-02	Antoni Roig	Privacy and Data protection Protection Models	
D7.1-03	Esther Morón/MJR-P	Legal Framework (Europe/Spain)	
D7.1-04	M.José Rodríguez-Puerta/EM	Legal Framework (Europe/Spain)	
D7.1-05	Tomàs Gil	LEAs Issues	
D7.1-06	Francesca Gaudino	Legal Framework (EU countries)	
D7.1-07	Marta Poblet/PC	Ethical issues	
D7.1-08		CAPER Regulatory Model	