ICRI Working Paper Series

**Applying the purpose specification principle in the
age of “big data”: the example of integrated video
surveillance platforms in France**

Fanny Coudert, Jos Dumortier and Frank Verbruggen

ICRI Working Paper 6/2012

Interdisciplinary Centre for Law and ICT, K.U.Leuven

icri

25 April 2012

This paper can be downloaded without charge from the ICRI website at <https://www.law.kuleuven.be/icri/> and the Social Sciences Research Network electronic library at <http://ssrn.com/link/ICRI-RES.html>.

Applying the purpose specification principle in the age of “big data”: the example of integrated video surveillance platforms in France¹

Fanny Coudert², Jos Dumortier³, Frank Verbruggen⁴

Abstract

The proliferation of data made available to businesses, governments and individuals, also referred to as the “data tsunami” or the age of “big data”, heavily challenges the application in practice of the purpose specification principle, one cornerstone principle of the data protection framework. In order to illustrate these difficulties, this paper takes as example a growing phenomenon, the deployment of integrated video surveillance platforms that link networks originally installed for distinct purposes and managed by different actors. Focus is put on France where the government passed a law to authorize law enforcement agencies to access private video surveillance networks for purposes of fighting crimes against properties and persons. We conclude by formulating policy recommendations tending to counter the dilution of safeguards when implementing the purpose specification principle in networked systems.

1 “Big data”, big challenges for the purpose specification principle: introducing the example of video surveillance in France

As worded by O.Tene and J. Polonetsky, we live in an age of “big data”.⁵ The term “big data” refers to the avalanche of data available as raw material of production to businesses, government and individuals. The increasing interconnection of people, devices and sensors, coupled to growing storage and processing capacities, fosters the overproduction of data of an increasing economic and social value. In the more specific field of Security, the Future Group in charge of analyzing the European Security landscape referred to this phenomenon as “data tsunami” to describe the predominant role that “information” has taken in the modus operandi of Security agencies.⁶ The Future Group contended that “information is the key to protecting the public and in an increasingly connected world in which public security organisations will have access to almost limitless amounts of potentially useful information”.

This plethora of information is seen both as a challenge and as an opportunity, fostering public security entities to adjust their working methods in order to convert this enormous amount of

¹ This paper has been funded by the B-CENTRE (www.b-centre.be) with the financial support from the Prevention of and Fight against Crime Programme of the European Union.

² Interdisciplinary Centre for Law & ICT (ICRI) – B-CENTRE, K. U. Leuven, IBBT; fanny.coudert@law.kuleuven.be.

³ Interdisciplinary Centre for Law & ICT (ICRI) – B-CENTRE, K. U. Leuven, IBBT; jos.dumortier@law.kuleuven.be.

⁴ Institute of Criminal Law – B-CENTRE, K. U. Leuven; frank.verbruggen@law.kuleuven.be.

⁵ Tene O., Polonetsky J., Privacy in the Age of Big Data, A Time for Big Decision, 64 Stan. L. Rev. online 63, February 2, 2012, available at: <http://www.stanfordlawreview.org/online/privacy-paradox/big-data>

⁶ The Future Group, “Freedom, Security, Privacy – European Home Affairs in an open world”, June 2008, p.43.

information into useful intelligence. Technology is then presented as pivotal to connect the capabilities of all stakeholders with the final goal of ensuring that the right information gets to the right person in the form they are best able to use.⁷

The use of new technologies, with the correlative benefit of the collection of additional data, is often advanced as the most efficient response to security threats such as terrorism. Data collection is presented as being key to reduce offline and online criminality. Video surveillance is one of these technologies on which law enforcement increasingly relies both to prevent and to investigate the perpetration of crimes.

In France, the deployment of video surveillance systems was presented by the government as a essential technology for both the fight against terrorism⁸ and the reinforcement of everyday security (*sécurité quotidienne*), i.e. for the fight against street crime. Everyday security is a recurrent concern of French people, which has been exacerbated by the violent riots that have shaken this country at the end of 2005. Gangs massively vandalized public buildings, burned schools and cars parked on the streets in the surroundings of the main cities. These riots have highlighted a phenomenon already creeping for years in these areas. They also originated a strong political reaction toward the strengthening of security measures amongst which the deployment of modern video surveillance systems was key.

In 2007, Michèle Alliot-Marie, by then Minister of Interior, launched a plan for a massive deployment of video surveillance systems, with the aim of tripling the number of cameras already in place. In her speech for the launch of the National Committee on Video surveillance, to respond to concerns over the intrusiveness of such plan into individuals' privacy, she claimed that the efficiency of video surveillance to ensure protection against street crime had been demonstrated by the positive results obtained both in France and in the UK during criminal investigations⁹. The term "video surveillance" was then progressively replaced in official discourses by the one of "video protection", based on the argument that citizens' perceptions of this technology had evolved over the years in a positive way and that they now looked at it as a tool of safety rather than one of surveillance.¹⁰

The measures contained in this plan were not only quantitative but also qualitative. Not only did it foresee the deployment of new cameras but also the deployment of more efficient systems that

⁷ Ibid.

⁸ Speech of Nicolas Sarkozy (President of the French Republic) for the ceremony in memory of terrorism victims, Paris, 19 September 2007, <http://www.ambafrance-uk.org/Allocution-du-President-Sarkozy,9480.html>

⁹ http://www.interieur.gouv.fr/sections/le_ministre/interventions/archives-mam/commission-videosurveillance. The veracity of this claim is highly debated amongst researchers (see e.g. for a contrary analysis Norris C., A review of the increased use of CCTV and video surveillance for crime prevention purposes in Europe, Note for the European parliament's Committee on Civil Liberties, Justice and Home Affairs, doc. N°PE 419.588, April 2009). The argument is mentioned in this paper with the sole purpose of setting the context of the French law proposal, matter of analysis. It falls out of the scope of this paper to take any position on this issue.

¹⁰ Quand la "vidéoprotection" remplace la "vidéosurveillance", [lemonde.fr](http://www.lemonde.fr/societe/article/2010/02/16/quand-la-vidéoprotection-remplace-la-videosurveillance_1306876_3224.html), 16 February 2010, http://www.lemonde.fr/societe/article/2010/02/16/quand-la-vidéoprotection-remplace-la-videosurveillance_1306876_3224.html

would allow to integrate existing video surveillance networks and to give the police access to the ones already installed and used for urban management.¹¹

Video surveillance systems installed for purposes of urban management indeed provide a wealth of information. Not only can they provide valuable information for the prevention and investigation of crimes but also, as a way of example, for crisis management. In that sense, the FP6 European project DYVINE (Dynamic Visual Networks), a research project that run from 2006 to 2008, envisioned a dynamically configurable video surveillance network that would give accurate and focused information on the status of incoming catastrophes such as floods, tropical storms, etc. More particularly, it sought to provide civil protection agencies with enhanced crisis management tools. The system would link, on a permanent basis, all video surveillance networks owned by a local authorities, including the ones of police, with the possibility to extend it, on demand, to private networks.

Video surveillance systems can be linked more easily thanks to the use of IP technology. This technology reduces the costs of installation and it allows for the transmission of all kind of data (images but also sound, software instructions, etc.) that do not necessarily have to be stored in the camera but can be placed in a server to which the camera is remotely connected. Software can be run on the network to coordinate the action of “smart cameras”. This means that video surveillance systems are now able to identify, trace or analyse people’s behavior in an automated way. The increased flexibility permitted by IP technology further enables a growing adaptability of the configuration and characteristics of video surveillance networks to the changing circumstances. For instance, it is now possible to add new video surveillance networks to the system to extend the area monitored. Video surveillance networks become flexible, intelligent and pervasive.

In France, the costs of the linkage of video surveillance systems were supported by a dedicated State fund “for the prevention of delinquency”¹². The deployment of interoperable video surveillance systems was moreover encouraged by a series of legal provisions, namely: (a) the introduction, by way of ministerial decrees, of minimum technical standards with which video surveillance systems should comply, tending to foster their interoperability¹³; (b) the possibility for law enforcement agencies (police, gendarmerie and customs) and civil security agencies (firefighters and emergency services) to have a direct and permanent access to video surveillance systems monitoring public areas owned by third parties¹⁴; (c) the possibility for public establishments for inter-communal cooperation to deploy integrated video surveillance networks accessible to the competent

¹¹ Speech of Michèle Alliot-Marie (Minister of Interior) for the implementation of the national Video surveillance Committee, 9 November 2007, http://www.interieur.gouv.fr/sections/le_ministre/interventions/archives-mam/commission-videosurveillance

¹² Fonds interministériel pour la prévention de la délinquance created by article 5 of the Act n°2007-297 of 5 March 2007. This State fund is used to support local authorities with the deployment of projects aimed at fighting delinquency by a grant up to 20-50% of the total amount.

¹³ Article 1 of the Act n° 2006-64 of 23 January 2006 for the fight against terrorism and Ministerial Decrees of 26 September 2006 and of 3 August 2007.

¹⁴ Article 1 of the Act n° 2006-64 of 23 January 2006 for the fight against terrorism which modifies Article 10.III of the Act N°95-73. The possibility for access as well as the conditions are subject to prior authorization by the *Préfet*. The LOPPSI II has authorized Customs and emergency services to access such systems.

authorities of the cities involved¹⁵ in order both to reduce the implementation and maintenance costs and to prevent the displacement of delinquency to areas not monitored.¹⁶

But the plan was going one step further. It was foreseeing to grant police access to private networks. To give legal coverage to the measure, the Parliament included into the law proposal on gang violence¹⁷ a provision that would give law enforcement authorities “on demand” access to video surveillance systems monitoring private premises. This provision was challenged by sixty senators¹⁸ before the Constitutional Court for failing to install sufficient safeguards to protect individuals’ fundamental rights. The arguments, accepted by the Court¹⁹, mainly focused on the breach of the principle of legality, within the meaning of article 8 of the European Court of Human Rights (hereafter referred to as “ECHR”)²⁰ based on the text’s lack of clarity and foreseeability.

This provision could also have been challenged from the perspective of data protection, based on the purpose specification principle. This principle mandates personal data to be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. It was introduced as an instrument of control over data controllers. It fragments personal data processing activities and forms closed compartments in order to avoid concentration of controlling powers by limiting the amount of information processed and shared, reducing a priori the risks of harm. In words of DE HERT and GUTWIRTH, “because the power of the processors and the ability to influence behaviour expands with their increase in exchanges, sales, linkages, groupings, analyses and availability of personal data, their competence to process is limited to meet well-defined goals. In other words processing operations are not banned but separated”.²¹

By doing so, this principle also guarantees the foreseeability of data processing activities. In that sense, General Advocate Kokott, in her Opinion in the *Promusicae* case²², noted that the requirement of foreseeability of the interference, as introduced under article 8.2 ECHR, that mandates such interference to be formulated with sufficient precision by law as to allow individuals to adjust their conduct accordingly, “had found particular expression in data protection law in the criterion – expressly mentioned in Article 8(2) of the Charter – of purpose limitation.”

¹⁵ Act n° 2007-297 of 5 March 2007 for the fight against delinquency

¹⁶ For a detailed overview of the measures taken, see COURTOIS J.-P. , GAUTHIER C. , *La vidéosurveillance: pour un nouvel encadrement juridique*, Information report n° 131 (2008-2009) for the Senate, 10 Décembre 2008

¹⁷ Proposition de loi renforçant la lutte contre les violences de groupes et la protection des personnes chargées d’une mission de service public, Assemblée Nationale, doc n°1641, 9 May 2009, available at: http://www.assemblee-nationale.fr/13/dossiers/violence_groupe.asp

¹⁸ The text submitted by the sixty senators is available at: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2010/2010-604-dc/saisine-par-60-senateurs.101896.html>

¹⁹ Decision 2010-604 DC of 25 February 2010

²⁰ References to the principle of legality are here understood in the sense of the human right doctrine, i.e. as the requirement to base any interference into individuals’ fundamental rights on a legal basis. Article 8§2 ECHR stipulates that “There shall be no interference by a public authority with the exercise of this right [to privacy] except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others”.

²¹ DE HERT P. , GUTWIRTH S. , *Interoperability of police databases within the EU: an accountable political choice?*, TILT University Legal Studies Working Paper No. 003/2006, 2006.

²² Opinion General Advocate J. Kokott [2007], ECJ C-275/06, *Promusicae* vs. Telefónica.

It follows that, as far as the challenged provision of French law legitimizes the linkage of video surveillance systems originally installed for different purposes and the access to these systems by new users for additional purposes, this provisions cracks the closed compartments the purpose specification principle is supposed to guarantee. It consequently increments the amount of information, and thus of power, processed by the authorities with access to the system.

After a first analysis of the arguments of the French senators and the ones adopted by the French Constitutional Court in its ruling n°2010-604 of 25 February 2010, this paper focuses on the relation between the purpose specification principle and the principle of legality. It will highlight the difficulties that emerges from its application in practice and how the arguments raised by the senators and the solution adopted by the legislator to comply with the ruling of the Constitutional Court eventually resulted in a better application of this principle. This analysis will enable us to provide a fresh view on the challenges raised by integrated video surveillance platforms, as illustration of the more general concerns raised by the interconnection of networks for security purposes, and to suggest solutions to overcome them.

2 The French political debate around the access by law enforcement authorities to private video surveillance systems

Gang violence has been spreading in France for many years, reaching a climax in 2005 when this violence burst into riots all over the French territory. In order to tackle this phenomenon, the French Parliament submitted a law proposal to increase citizens and schools' safety. New crimes were introduced into the Criminal Code and the powers of law enforcement authorities were broadened. This section focuses on one provision that foresees to give law enforcement authorities access to video surveillance systems monitoring private premises, and that was successfully challenged before the Constitutional Court, before being reintroduced at a later stage with substantive modifications. To fully understand the terms of the debate, it is however necessary to first give an overview of the regulation of video surveillance in France and of the different actors involved in the supervision.

2.1 Overview of the French legal framework on video surveillance²³

France has a complex regulation of video surveillance that distinguishes systems monitoring public areas from the ones monitoring private areas. This distinction is issued from the option taken by the legislator back in 1995 to adopt a specific regulation applicable only to video surveillance systems monitoring public thoroughfare (*voie publique*) and places opened to the public. The enactment of a specific legislation to regulate video surveillance was motivated by the need to give legal certainty in front of the plethora of legal provisions applicable to such systems and by the differing criteria used by the CNIL, the French data protection authority, and the case law. The provision regulating video surveillance (article 10 of the Act n°95-73)²⁴ is contained into an Act on Internal Security, which may explain that the legislator has limited the scope of the regulation to the monitoring of public thoroughfare and of places opened to the public. The content of the provision is however largely

²³ For a detailed overview, see COURTOIS J.-P., GAUTHIER C., La vidéosurveillance: pour un nouvel encadrement juridique, Information report n° 131 (2008-2009) for the Senate, 10 Décembre 2008.

²⁴ Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. From May, 1st 2012, the provisions of this Act relative to vidéosurveillance will be integrated to the new Internal Security Code, Title V.

inspired by the principles of the French Data Protection Act²⁵ to balance the needs of public safety and the protection of fundamental rights:

- The purposes that can motivate the deployment of a video surveillance system are listed by the legislator
- The storage of the images is limited to thirty days
- Certain areas, more privacy sensitive such as the interior of buildings or their entries, must not be monitored
- The general public should be informed of the existence of the video surveillance system
- Security measures should be implemented to protect the confidentiality and authenticity of the recordings

This provision applies to cases where images are recorded by the system or merely transferred to a central station. The deployment of a video surveillance system is subject to prior authorization granted by the *Préfet* (the State county representative) after (indicative) opinion given by a specific committee headed by a magistrate (the committee on video surveillance). This authorization can impose additional conditions for the establishment of the systems whose infringement will motivate the withdrawal of the authorization. The imposition of additional conditions will usually result from the proportionality check and it will affect the number, the place, the orientation, and the characteristics of the cameras as well as their storage capacity and duration.

It however does not apply to cases where a) recordings are part of an automated processing or are contained into files structured according to criteria that allow to identify, directly or indirectly, natural persons; b) the images are publicly displayed on a monitor but not recorded (such as monitors placed in small shops).

The Data Protection Act is applicable to cases falling under a) and to video surveillance networks monitoring private areas or private places open to the public. Whenever the Data Protection Act is applicable, the CNIL is competent for the supervision of the video surveillance system.

This complex system was validated by Constitutional Court in 1995.²⁶ In this ruling, the Court took great care of listing the safeguards necessary for an adequate balance of the interests at stake, namely public security interests contained in the prevention of attacks on public order and the prevention of harm to public order and the search for offenders, against the protection of the right to privacy and other fundamental rights. It also required that the authorization of the system would be express. A mere declarative system is thus not allowed for video surveillance systems installed for public security purposes.

Initially providing a clear definition of the competences of the CNIL on the one hand and of the *Préfets* on the other hand, this distinction was blurred after the review of the French Privacy Act in 2004 in view of integrating the provisions of the 95/46/EC Directive. The reason is to be found in the broadening of the definitions of personal data and of personal data processing, in accordance with the text of the Directive. For instance, the CNIL had initially excluded analog video surveillance systems with no recording function from the scope of application of the Data Protection Act. Analog systems were acknowledged as manual data processing and only the recordings were considered as

²⁵ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

²⁶ Decision n°94-352 DC of 18 January 1995.

“files”. The definition of personal data processing activities contained in the 95/46/Directive is much broader and includes for instance any manual data processing activity as well as any action performed on the data, including their mere collection. A strict application of the Data Protection Act would then extend its scope of application to such data processing activities. As a consequence of the blurring of competences, the Act on Internal Security of 2011, the so-called “LOPPSI 2”²⁷ extended the competences of the CNIL to all video surveillance networks, irrespective of the area monitored.

The co-existence of these two regimes, whose application depend on the place monitored, became a source of complexity most particularly for video surveillance systems covering both public and private areas. This is the case of common areas of apartment buildings for residential use, which are being monitored by video surveillance networks installed by tenants. Some areas such as playgrounds qualify as public areas. By contrast, common areas located within the buildings (halls, stairwell, etc.) qualify as private areas. These tenants have thus to abide by both legal frameworks, applying different legal provisions to different areas. Requirements to allow law enforcement authorities to access such framework will thus differ.

2.2 The challenged article

The initial article tabled by the government stipulated that:

“When events or situations that may require intervention by police or gendarmerie or, where appropriate, the municipal police officers, occur in the common areas of apartment buildings for residential use, owners or managers of these buildings or their representatives may make such services or agents recipients of the images of video surveillance systems being deployed in these areas.”

This article is presented as the technological prolongation of existing legal provisions that authorize owners or the managers of these buildings to give a permanent access to common areas to law enforcement authorities for the reestablishment of the peaceful enjoyment of such places.²⁸

This article was however providing de facto a blanket authorization to law enforcement authorities to access private video surveillance systems. During the debates, the Senate, in order to counterweight the risks to privacy raised by the possibility of an extensive interpretation of the article, required the introduction of a series of safeguards, namely: (a) the request for the transfer should stem from the tenants, (b) the transfer of the images should be done in real time (c) it should be limited to the time necessary for the intervention, (d) the modalities for implementing this provision should be approved by a decree adopted by the State Council prior opinion of the CNIL. They succeeded in introducing the following two additional paragraphs:

²⁷ Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JORF n°0062 du 15 mars 2011 page 4582.

²⁸ Article L. 126-1 of code de la construction et de l'habitation. See in that sense, Pillet F., Rapport n°85 (2009-2010), fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur la proposition de loi (n° 2093), déposé le 4 novembre 2009, available online at : http://www.assemblee-nationale.fr/13/rapports/r2237.asp#P140_21421

“The transmission of these images is the sole initiative of the owners or operators of multiple dwellings or their representatives. It is real time and is strictly limited to the time required for the intervention of police or gendarmerie national or, where applicable, officers of the municipal police.

A Decree approved by the State Council, taken after prior opinion of the CNIL, specifies the modalities for implementing this Article”.

Despite letting to the government the task of defining the conditions for access, the safeguards introduced by the senators into the text of the article did put limits on the amount of information transferred to police forces, and tried to reduce it to what was strictly necessary, in view of ensuring the proportionality of the processing as regards the material scope of data processed. They banned the recording of images and limited the time span where law enforcement agencies might gain access to video surveillance systems. This also limited the risk of illegitimate (re-)use of the information by the police forces.

However, this new drafting left one main concern unsolved, namely the one of the loose definition of purposes for which the systems could be accessed. This article used an extremely broad formulation of the purposes for intervention, the law referring to whatever “events or situations that may require intervention by police or gendarmerie or, where appropriate, the municipal police officers.” In addition, the interpretation and application of the provision was still entirely let to the actors in place without any external safeguards or criteria for application. Such faculty was entirely let (a) in first place to the Executive in charge of drafting the application decree regulating the “details” of the data processing, (b) then to the tenants who would have decided when the transmission was required and to which police force, and (c) ultimately to police forces whose intervention had been required. It is therefore difficult to see how the additional provisions would have effectively prevented an extensive interpretation of the wording of the article.

Finally, the Parliament suppressed the requirement of a prior opinion of the CNIL for the enactment of the decree specifying the conditions for access. The Parliament did not consider that the access to owners’ video surveillance systems would constitute a new data processing activity but rather a mere extension of the already existing possibility for law enforcement to visualize the images taken from these networks. The purpose of access, as understood by the Parliament, was merely to prepare the further intervention of law enforcement authorities. They also argued that the absence of recording and storage as well as the impossibility for these images to be used for identification purposes excluded the competence of the CNIL on these activities.²⁹

These arguments are debatable in the light of the new definitions of personal data and of data processing as introduced in 2004 for digital video surveillance systems. While the physical access by law enforcement authorities to private areas of buildings does not constitute a data processing activity (and as such is not subject to the Data Protection Act), the access to a video surveillance systems monitoring these areas is, with no doubt, a data processing activity. This new provision therefore creates a new data processing activity. In addition, as mentioned above, the mere collection of personal data (i.e. their visualization) will fall under the definition of data processing activity. Finally, the Article 29 Working Party has clearly set it is sufficient for an image obtained by a

²⁹ Pillet F., Rapport n°85 (2009-2010) for the Parliament on the law proposal n° 2093, 4 Novembre 2009, available online at : http://www.assemblee-nationale.fr/13/rapports/r2237.asp#P140_21421

camera to refer to people who are recognizable, to qualify as personal data.³⁰ However, the law proposal was set to be approved with these modifications and was submitted as such before the Constitutional Court.

2.3 The arguments of the senators

This provision was challenged by sixty senators before the Constitutional Court on the basis of its disproportionate impact on the right to privacy.

First of all, the senators argued that the lack of clarity and foreseeability of the drafting was contrary to the principle of legality. In that sense, the control carried out by the European Court of Human Rights (hereafter referred to as “ECtHR”) and by national Constitutional Courts bear on the conditions of the interference, namely whether such interference is (a) “in accordance with the law” (foreseeability requirement), (b) justified under one of the legitimate aim as listed in article 8§2 ECHR and (c) “necessary in a democratic society” which implies performing a proportionality test to ensure that only the minimum interference with the interest that secures the legitimate aim will be permitted. The senators considered that the general wording used by the legislator is such as to base a wide range of access to the system even in cases where the facts originating the intervention are not punishable under criminal law. The Constitutional Court ruled that article 8 ECHR requires the legislator to define offenses in terms sufficiently clear and precise as to exclude arbitrariness.³¹ It also decided that the needs of investigation of offenders and of the preservation of Law and Order, which are the interests at stake in the present case, should be balanced against the right to privacy when drafting any legislation that could interfere into the latter right.³²

It follows that, by failing to specify the situations or crimes which entail law enforcement authorities to access private video surveillance systems, this provision introduces an excessive interference into the right to privacy. In addition, according to the senators, the legislator failed to its duty of implementing clear safeguards for the access by law enforcement to video surveillance networks monitoring private areas as it let this task to the government and excluded the intervention of the CNIL.

Finally, the Senators challenged the possibility given to municipal police officers to access such systems. Municipal police in France does not enjoy specific police competences but only subsidiary ones. They furthermore operate under the authority of the Mayor, not under the one of judicial police. By granting a general authorisation to municipal police to access private video surveillance networks, the challenged article opened the door to cases where they could gain access to such networks for facts that fall outside their field of competence. Once again the senators argued this interference into the right to privacy was excessive.

³⁰ Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, WP89, 11 February 2004.

³¹ 80-127 DC of 20 January 1980, recital 7.

³² 86-211 DC of 26 August 1986, recital 2.

2.4 The Decision of the French Constitutional Court

The Decision of the Constitutional Court of 25 February 2010 is extremely concise and limited to the access by law enforcement authorities to systems monitoring private areas.³³ The Court only acknowledges that article 10 of the Act n°95-73 is not applicable to such cases and therefore that the legislator should have installed adequate safeguards to protect people living and visiting these places. It annuls the provision.

As mentioned above, article 10 of the Act n°95-73 covers the monitoring of public areas of such building and therefore the further access by law enforcement agencies to the images of public areas does not require a specific legal authorization. The legitimacy of the interference into privacy caused by the installation of video surveillance systems for purposes of “preventing harm to the safety of persons and property in areas particularly exposed to risks of assault or theft” was already validated by this Court when examining the conformity of the provision with the Constitution back in 1995.³⁴

It is regrettable that the Constitutional Court provides such little insight into the safeguards the legislator should have implemented in order to legitimate the access by law enforcement to private premises. In its ruling of 1995, the Court validated the use of video surveillance systems to monitor public areas because of the safeguards it introduced for the protection of fundamental rights such as the sanctity of home, the right to privacy and the freedom of movements that includes the right not to be subject to arbitrary and widespread surveillance.³⁵ One important safeguard listed by the Court was precisely the prohibition to visualise the interior and entries of private premises. In the 2010 decision, while the Court required sufficient guarantees to be implemented to authorize public authorities to gain access to private premises, it did not specify which should be the content of such guarantees. The Court for instance did not take position on the requirement introduced by the Senate to base such access on the prior initiative of tenants.

This Decision neither takes position on the claim of the Senators according to which a too broad definition of purposes of these new video surveillance activities failed to meet the requirement of foreseeability. As long as this decision seemed to require the legislator to introduce sufficient safeguards to prevent arbitrariness and the abusive use of the data accessed, this claim appeared pivotal.

The Parliament took good note of the Constitutional Court’s ruling and introduced a reviewed article in the Act “LOPPSI 2” to authorize and to adequately to frame the transfer of images from video surveillance systems monitoring the common areas of apartment buildings for residential use to law enforcement authorities. Before analyzing the content of the new safeguards and assessing their impact on the right to privacy, it is first necessary to understand the rationale of the purpose specification principle.

³³ Decision 2010-604 DC of 25 February 2010.

³⁴ Decision n°94-352 DC of 18 January 1995.

³⁵ For an analysis of the safeguards listed by the Constitutional Court see *ibid*.

3 The purpose specification principle as manifestation of the principle of legality

3.1 The purpose specification principle: rationale

The purpose specification principle is at the core of the fundamental right to data protection as recognised by the European Charter on Fundamental rights. Article 8 of the EU Charter requires personal data to be *“processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.”*

The purpose specification principle as recognised by the EU Charter should be read together with the 95/46/EC Directive³⁶ whose article 6 stipulates that *“personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.”* The principle of purpose specification therefore means that personal data should be collected for:

- *Specified purposes*: The purpose of collection must be determined at the time of collection of the data (Recital 28 of 95/46/EC Directive, OECD Privacy guidelines³⁷). OECD guidelines specify that “basically, the purpose specification principle implies that before, and in any case not later than at the time data collection, it should be possible to identify the purposes for which these data are to be used, and that later changes of purposes should likewise be specified.” This is meant to prevent that new purposes are introduced arbitrarily.
- *Explicit purposes*: Purposes should be made explicit to the data subject and to the public at large. The purpose specification principle acts here as a tool ensuring the transparency of the data processing and the foreseeability of the actions performed by the data controller. According to OECD Privacy guidelines, such specification of purposes can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies. It will depend on the nature of the data processing activities at stake.
- *legitimate purposes*: The grounds for making the data processing legitimate are set up by Article 7 of the 95/46/EC Directive. Whereas grounds may differ from data processing operation to data processing operation, their legitimacy will closely relate to the activity performed by the data controller.
- *not further processed in a way incompatible with those purposes*. Any changes in the originally planned data processing activities should be compatible with the original purposes. This means that personal data cannot be processed for purposes beyond the reasonable expectations of the data subject.

From the definition above, three basic functions can be identified for the purpose specification principle within the data protection framework: (a) it first makes possible the control of legality of the data processing by the data controller, the competent supervision authority or the Courts insofar as the purpose defined by the data controller is key for the assessment of the legitimacy of the

³⁶ The explanation attached to Article 8 of the EU Charter indicates that the right to protection of personal data is to be exercised under the conditions laid down in the Directive 95/46/EC.

³⁷ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980. References are made to OECD Privacy Guidelines whenever the 95/46/EC Directive or the Council of Europe Convention n°108 do not provide interpretative guidelines of the provisions they contain.

processing and for preventing abuses of power; (b) it then ensures the proportionality of the data processing providing a yardstick against which the data controller, the competent supervision authority or the Courts can assess data quality and limiting the amount of data collected and processed; finally (c) it is a tool of trust, providing legal certainty to data subjects, in that it requires personal data not to be processed beyond their reasonable expectations. In this paper, the purpose specification principle is approached from the role it plays to ensure the foreseeability of data processing operations and by extension of the activities of data controllers. The concept of foreseeability is understood in the sense of the ECtHR case law as requiring any interference into the right to privacy to be formulated with sufficient precision to enable individuals to adjust their conduct accordingly.³⁸

3.2 Prevention of arbitrariness and of abuse of power through a strict definition of purposes by Law

The purpose specification principle enables first the data controller but also the competent supervision authorities and the Courts to control the legality of the data processing activity (the purpose should be legitimate). The purpose, as defined by the controller, should conform one of the criteria listed by article 7 of the 95/46/EC Directive to, as indicated in the title of this article, “make the processing legitimate”.

As far as the public sector is concerned, the existence of a legitimate basis for the processing will be closely linked to the existence of sufficient legal competences vested in the data controller. During the preparatory works of the 95/46/EC Directive, the European Commission already noted that *“essentially the public sector body is established by law and the law sets out its legitimate tasks. It is relatively easy to judge, whether the processing is inside or outside the tasks of the public body. The law itself is the legal basis and the criterium for the lawfulness of the processing in the public sector.”*³⁹ The processing should be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, as defined by Law, according to the more general principle of legality that governs the whole activity of public authorities.

The principle of legality means that administrative action is subject to Law, and that Law determines the limits of discretionary powers vested in public authorities, which are liable in case of harm caused by their activities.⁴⁰ In words of MARCOU, *“The principle of legality is the legal ideal that requires all law to be clear, ascertainable and non-retrospective. It requires decision makers to resolve disputes by applying legal rules that have been declared beforehand, and not to alter the legal situation retrospectively by discretionary departures from established law.”* The principle of legality is expected to ensure a fair balance of powers and prevent arbitrariness. As stressed by MARCOU, *“in administrative law it can be seen in the desire for state officials to be bound by and apply the law*

³⁸ See e.g. ECtHR, *S. and Marper vs. the United Kingdom* [GC], nos. 30562/04 and 30566/04, 4 December 2008, ECHR 2008-..., §95.

³⁹ Ibid.

⁴⁰ MARCOU G., *The legal and regulatory framework for public administration*, report submitted to the Twelfth Meeting Of Experts On The United Nations Programme In Public Administration And Finance held in New York on 31st July- 11th August 1995, doc n° ST/SG/AC.6/1995/L.4, 20 July 1995, <http://unpan1.un.org/intradoc/groups/public/documents/un/unpan000761.pdf>

rather than acting upon whim. As such advocates of the principle are normally against discretionary powers”.

In the more specific field of privacy, account should be taken of the requirements the ECtHR has set under article 8 ECHR. Interferences into the right to privacy by the State should be justified on one of the basis listed by Article 8.2 ECHR and be “in accordance with the law” and “necessary in a democratic society”. The ECtHR case law requires the safeguards introduced by the legal provision that legitimates the data processing operation to be sufficient as to avoid arbitrariness from public authorities and abuse of powers. The doctrine of the Court has been summarized in the *Marper* case.

The expression ‘in accordance with the law’ requires first that the impugned measure should have some basis in domestic law (including both written and unwritten law –*Malone*, 1984, §85⁴¹) and be compatible with the rule of law as mentioned in the Preamble to the ECHR and inherent to the object and purpose of Article 8 (*Marper* case, 2008, §95). The law must be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice- to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and indicate accordingly with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise.

The level of precision of domestic legislation –which cannot in any case provide for every eventuality- depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed. In the *Marper* case (2008, §99) where the Court had to deal with the retention of fingerprints, cellular and DNA samples for purposes related to “the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution”, the Court held that the first of these purposes, “the prevention or detection of crime”, was worded in such general terms that it could give rise to extensive interpretation. It therefore reiterated its case law on telephone tapping, secret surveillance and covert intelligence-gathering requiring to have sufficient guarantees against the risk of abuse and arbitrariness, namely:

- clear, detailed rules governing the scope and application of measures,
- minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties,
- procedures for preserving the integrity and confidentiality of data and procedures for its destruction.

According to this case law, any legal provision that legitimates data processing activities should therefore provide adequate safeguards that will prevent arbitrariness and abuse of power, above from being specific enough to ensure the foreseeability of public activity. The more severe the interference into the right to privacy, the more stringent such safeguards should be. As a way of example, in *Marper*, the ECtHR recalls that the mere storing of data related to the private life of an individual amounts to an interference within the meaning of article 8 ECHR. In order to determine whether the personal information retained by the authorities involves any of the privacy aspects, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which the records are used and

⁴¹ ECtHR, *Malone v. the United Kingdom*, judgment of 2 August 1984, Series A no. 82.

processed and the results that may be obtained.⁴² Applying these principles to the retention of cellular samples by law enforcement authorities, the Court considered that, given the nature and amount of personal information contained in cellular samples, their retention *per se* must be regarded as interfering with the right to privacy.⁴³ This leaves the Court to rule that the permanent retention of fingerprint and DNA data of all suspected but unconvinced people is excessive in view of the risks for individuals' fundamental rights. The Court however implicitly validates the practice of other Member States to take cellular samples in criminal proceedings only from individuals suspected of having committed offences of a certain gravity.⁴⁴ Their retention is further subject to strict limitation periods after acquittal or discharge.

In that sense, the purpose specification principle acts within the data protection framework as does the more general principle of legality at the level of the legal order. Personal data processing activities will in most cases interfere into individuals' fundamental rights and as such should be "in accordance with the law". The purpose of the data processing activity is what defines the scope of the interference into individuals' fundamental rights and as such should be sufficiently clear and detailed. In that sense not only should the purpose of a given data processing operation be legitimate (have an adequate legal basis) but it should also be specified, i.e. be clear and defined with sufficient precision, and explicit to data subjects, i.e. transparent as to empower them to act accordingly. As adduced by the French senators, too broad a definition of purposes in a law authorizing new data processing activities by public authorities fails to meet the principle of legality as defined under the ECtHR case law in that it does not allow individuals to foresee the scope of the interference.

4 Limits of an exclusive legalistic approach to adequately frame the activity of public authorities

Concerns have been raised about the efficiency of the principle of legality as a barrier against arbitrary power. The Law has to be general. According to LEISNER this transfers the risks of arbitrary power from the enactment of the norm to its application as long as the interpreter is the one fitting the provision (made by law) to reality, thus recreating the norm according to its needs.⁴⁵ This author contends that the more normativism tends to totality, to ubiquity of its rules, the more the power of decision goes to the ones the norm should have controlled. In this sense, SCHWARZE notes that "*when a legal system develops, there must be not only legal principles, but also rules for interpreting these principles.*"⁴⁶ Real-life situations can generally not be mechanically allotted to a certain rule. What is required is an "interpretation" of the provision in question, to bring it into service in resolving the dispute. Control over the interpretation of the norm is seen as pivotal in framing the power given to the interpreter.

Similar concerns have been raised within the field of data protection very soon by authors such as SIMITIS. In 1992, when analysing the first generations of data protection, SIMITIS pointed out the limits

⁴² ECtHR, Marper, §67

⁴³ ECtHR, Marper, §73 and §121

⁴⁴ ECtHR, Marper, §108

⁴⁵ LEISNER W., *L'Etat de droit - une contradiction?*, Hommages à Charles Eisenmann, Cujas, Paris, 1975, 65-79.

⁴⁶ SCHWARZE J., *European Administrative Law*, Revised 1st ed., London: Sweet and Maxwell, 2006, 1562p.

of the “global approach” to computerized processing of personal data.⁴⁷ Countries that have adopted such approach, such as Germany, have drafted Privacy Acts which consist of a few very broad statements with the hope that using sufficiently abstract terms would offer a better flexibility and higher possibilities of reaction in the face of technological shifts. The biggest advantage of this approach, namely the adaptability of its rules, appeared to be its weakest point.⁴⁸ As observed by SIMITIS this led to the implementation in the public sector of the general principle according to which *“public bodies should store and retrieve only the data “required” for the fulfilment of their tasks”*. The Law therefore puts limits on the amount of data that such authorities can collect and process. In words of SIMITIS, *“they have to make a careful choice and legitimate the retrieval by establishing its connection with their particular functions”*.

The main issue identified by SIMITIS is not whether the wording of the law should be flexible enough to be comprehensive but rather to whom the power of interpretation is devoted. In that sense, SIMITIS points towards the most pernicious effect of such broad provisions, namely the one of giving public authorities the power to decide which data are “required” for the processing. Their expectations determine the extent of the data collected. The Law therefore fails to limit the amount of data collected by public authorities, to adequately frame their power and ensure foreseeability. In words of SIMITIS:

“Consequently, police authorities, for example, continued to retrieve data in exactly the same way they did before the laws were passed. For them nothing has changed. Data they always considered necessary for their work, were in their view, of course, still indispensable. A provision intended to restrict retrieval was thus turned around by using its very wording and exploiting the chances, the interpretation of the extremely vague terms employed by the law, offers.”

SIMITIS further criticises the solution offered by data protection laws against abusive practices, namely the right to correct the data processed or ex-post remedies. This author denounces that *“the law at the best allows to demand corrections ex post, a rather illusory expectation, at least in the case of those, whose data have been processed.”*⁴⁹

5 Critical analysis of the final provision adopted by the French Parliament in the light of the purpose specification principle

The French Parliament decided to reintroduce the provision authorizing the transfer of images from video surveillance systems monitoring the common areas of apartment

⁴⁷ SIMITIS S., *New trends in national and International data Protection Law*, in Dumortier J. (ed.), *Recent developments in Data Privacy Law*, Leuven University Press, 1992, pp. 17-28. Other approaches include regulation as learning process, which paradigmatic example is Sweden, where the legislator openly admits that he has no answer to the new situation and seeks to establish a control mechanism, combining a close control of the processing with a constant increase of information on the aims and techniques. The key notion here was licensing. The other model identified is the one developed in the United States based on a sectoral approach. Behind it is a close conviction that a really efficient regulation presupposes a close adaption to the specific contexts. The author however stresses that most legislators did not opt for one specific model but rather tried to combine them.

⁴⁸ Ibid.

⁴⁹ IBID.

buildings for residential use to law enforcement authorities into the “LOPPSI 2” Act. This provision creates a new provision into the Code of Construction and Housing (article L. 126-1-1). It establishes new safeguards to improve the level of protection of the right to privacy which mirror the ones contained in Article 10 of the Act n° 95-73. This might explain why its conformity with the French Constitution was not challenged before the Constitutional Court.⁵⁰

The new provision L. 126-1-1 of the Code of Construction and Housing reads as follows⁵¹:

“The transfer to law enforcement authorities of the images taken for the protection of the common areas of apartment buildings for residential use in circumstances raising fears of an imminent commission of serious harm to property or persons is authorized by decision of the majority of owners under the conditions laid down in Article 25 of Law No. 65-557 of 10 July 1965 establishing the status of the condominium buildings, and in social buildings, of the manager. The images that can be transferred must not relate to the entrance of private houses or to public roads.

This transfer is done in real time and is strictly limited to the time required for the intervention of police or gendarmerie or, if relevant, of municipal police officers.

⁵⁰ This is one major weakness of the French constitutional review. The Constitutional Council is solely competent to control the constitutionality of law in two cases: a) when a proposed law specifies the functioning of the public administration (organic law) or when 60 deputies and senators present a special request for reviewing the constitutionality of the law, after its approval but before its promulgation. This means that once a law has been promulgated, it is considered to conform to the Constitution, without any possibility to challenge it. See, COUDERT, F., DEBET A., DE HERT P., 'Chapter 4: Constitutional Rights and New Technologies in France' in 'Constitutional Rights and New Technologies. A comparative study', eds. KOOPS, B.J., LEENES, R. and DE HERT, P., IT&Law n°15, TMC Asser Press, The Hague, 2008

⁵¹ Non official translation. The original text reads as follows: « *La transmission aux services chargés du maintien de l'ordre des images réalisées en vue de la protection des parties communes des immeubles collectifs à usage d'habitation lors de circonstances faisant redouter la commission imminente d'une atteinte grave aux biens ou aux personnes est autorisée sur décision de la majorité des copropriétaires dans les conditions fixées à l'article 25 de la loi n° 65-557 du 10 juillet 1965 fixant le statut de la copropriété des immeubles bâtis et, dans les immeubles sociaux, du gestionnaire. Les images susceptibles d'être transmises ne doivent concerner ni l'entrée des habitations privées, ni la voie publique.*

Cette transmission s'effectue en temps réel et est strictement limitée au temps nécessaire à l'intervention des services de la police ou de la gendarmerie nationale ou, le cas échéant, des agents de la police municipale.

Une convention préalablement conclue entre le gestionnaire de l'immeuble et le représentant de l'Etat dans le département précise les conditions et modalités de ce transfert. Cette convention prévoit l'information par affichage sur place de l'existence du système de prise d'images et de la possibilité de leur transmission aux forces de l'ordre.

Lorsque la convention a pour objet de permettre la transmission des images aux services de police municipale, elle est en outre signée par le maire.

Cette convention est transmise à la commission départementale de vidéoprotection mentionnée à l'article 10 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité qui apprécie la pertinence des garanties prévues et en demande, le cas échéant, le renforcement au représentant de l'Etat dans le département.

Ne sont pas soumis au présent article les systèmes utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques, qui sont soumis à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés »

An agreement previously reached between the property manager and the county state representative specifies the terms and conditions of this transfer. This agreement provides that the information on the existence of an image acquisition system and on the possibility of transfer of such images to law enforcement should be displayed on the site.

When the Agreement is to allow the transfer of images to municipal police services, it is also signed by the mayor.

This agreement is forwarded to the county committee of video surveillance referred to in Article 10 of the Act No. 95-73 of January 21, 1995, which will appreciate the relevance of the safeguards introduced and requires them to be strengthened, whenever relevant, to the County state representative.

Are not subject to this Article the systems used in automated processing or in files structured according to criteria allowing to identify, directly or indirectly, individuals who are subject to [the Data Protection Act]."

It is worth noting that the exclusion of the data processing activities falling under the Data Protection Act from its scope of application maintain the complexity in the application of the provisions applicable to video surveillance. As mentioned above, the LOPSSI 2 Act however extends the supervision powers of the CNIL to all video surveillance systems, which should at least tend to the application of more uniform criteria for the interpretation of the different provisions.

5.1 Specified, explicit, legitimate purposes and secondary uses

The first criteria to be assessed are the ones listed in article 6 of the 95/46/EC Directive and article 6.2 of the French Data Protection Act, i.e. whether this new provision entails the personal data to be collected for specified, explicit and legitimate purposes and whether it ensures these data not to be further processed in a way incompatible with the purpose of collection.

As regards the specific wording of the purposes, it is worth noting that the Parliament defines more narrowly the type of events that could trigger the transfer of images to law enforcement authorities. The new provision no longer refers to "events or situations that may require intervention by police or gendarmerie or, where appropriate, the municipal police officers". Rather it refers to "circumstances that make fear the imminent perpetration of a serious breach of property or of attacks to persons". The definition of the events that can trigger such transfer is thus more limited as it refers to categories of crimes that are serious enough as to justify the intervention of law enforcement authorities. While the mere reference to types of crimes seems reasonable in view of the rationale of the provision, which is to protect owners against attacks to their property and themselves, the use of the word "serious" introduces a degree of uncertainty that could have been solved by referring to the articles of the Penal Code that sanction this type of behavior.

The definition of purposes that can legitimate the transfer is defined in the Law and it echoes article 10 of the Act n°95-73 which lists as one legitimate purpose for the installation of a video surveillance network the prevention of serious breaches of property or serious attacks to persons. The situations that can motivate the access are thus not only more narrowly limited and but also coherent with other provisions of the legal framework regulating video surveillance. In addition, the new provision requires an additional ground of legitimization, namely the prior consent of the owners or managers

of buildings. This additional condition echoes the existing one allowing owners, under certain conditions, to grant law enforcement authorities a permanent access to common areas of their building for the purposes mentioned above.

The requirement to make the purpose of the processing explicit is complied with the obligation to inform the persons monitored, though a sign informing of the existence of a video surveillance system and of the possibility of these images to be transferred to law enforcement authorities.

Finally, the fact that the access is limited to the time required for the intervention and does not include the recording of such images by law enforcement authorities limits the risks linked to the further processing of these images. The images remain within the owners' video surveillance system. Access to these images by law enforcement authorities should thus be based on a different ground, which will in most case relate to the investigation of offenses and crimes.

5.2 Data quality

The second set of criteria that should be assessed refers to the question of proportionality of the data collected (also referred to as data quality principle), i.e. to what extent the definition of purposes allows to limiting the amount of personal data collected and processed.

The new provision introduces in that regard a set of limitations that helps better defining the scope of the interference into individuals' privacy rights. As mentioned above, the data processing activities of law enforcement only refer to the visualization of the images and it is limited to the time necessary to perform the intervention required. But the provision also limits the content of the images that can be transferred. Images of entrance to private habitations and of public areas must not be transferred. Again, these safeguards echoes the ones introduced by article 10 of the Act n°95-73 and listed by the Constitutional Council in its Decision of 1995. It should however be noted that this new provision weakens the initial requirement set in article 10 of the Act n°95-73 and the relative Constitutional Court Decision as it forbade the visualization of both the entrance and the interior of private premises. By contrast, the new provision allows the visualization of common areas, which are private by nature. However, as mentioned earlier, the Constitutional Court in its ruling of 2010 did not seem to object to the widening of places that could be monitored provided adequate safeguards were implemented.

5.3 Controlling the interpreter

Finally, a new provision is introduced to tailor the general provisions of the law to the specificities of the case at stake. The owners or manager of the building should enter into an agreement with the *Préfet* in order to regulate the conditions for the transfer. We can expect that one element of the agreement will bear on the definition of the competent law enforcement authority to access the video surveillance network as well as the situations that will trigger such intervention. This would not anymore let to the owners the appreciation of whether a certain event is serious enough as to require the intervention of law enforcement authorities. It also delegates to the competent State authority, closer to the owners than the Government, the task of defining the concrete conditions for access.

This agreement is further checked by the competent Committee for video surveillance. This new safeguard should act as an a priori check that will ensure the proportionality of the transfer and the adequacy of the additional safeguards implemented. If seriously performed, this check should limit the risks pointed out by SIMITIS of letting the power of interpretation of the Law to the persons to whom it applies, thus weakening the effectiveness of the provision.

6 Applying the purpose specification principle in interconnected systems: the way forward

This example illustrates how the balance between the requirement of generality of the law and the one of foreseeability can be achieved. The former requirement usually seems to constraint the legislator to a broad wording of the purposes in order to cover a wide range of situations and to ensure sufficient flexibility for their application in practice. By contrast, the later requirement calls for the enactment of clear and detailed rules governing the scope and application of the measures that will interfere into fundamental rights. We have seen how the French legislator appeared to have reached, at least in theory, a balance between a) the requirements of foreseeability through a strict definition of purposes and the definition of limits ensuring a minimum quality of data collected, and b) the requirements of flexibility for an effective application of the law through the introduction of a new instrument, the drafting of agreements between the *Préfets* and the owners of buildings, while counterbalancing c) the risks inherent to this flexibility by introducing an a priori mechanism of supervision.

Whereas the issue raised by SIMITIS, i.e. the challenge of drafting laws broad enough to fit their purposes while installing efficient mechanisms of supervision that ensure an effective application of the law, may not have an easy solution, data protection laws have evolved and developed greatly since the enactment of the 95/46/EC Directive, coming to a new level of maturity. It may now be possible to learn from the lessons of the past and explore new instruments that would provide solutions to the new challenges posed by the emerging technologies such as multi-purposes video surveillance networks.

Law should remain the instrument through which personal data processing by public authorities should be legitimized, setting up the cases and conditions under which data processing activities will be socially acceptable. Similarly, as long as the purpose specification principle enables the legality check, the proportionality check and as long as it ensures legal certainty of data processing activities, this principle should still continue to play a key role in ensuring the foreseeability of such activities. Foreseeability is a key element of any legal framework to generate trust and thus to ensure its sustainability. The societal debates that should accompany the drafting of laws remain the most adequate place to make important social choices. This for instance refers to defining in which cases law enforcement agencies can gain access to video surveillance networks and to limit it, as suggested by the French senators and further enacted by the legislator, to cases where a specific kind of (serious) criminal offenses are involved. The control of the constitutional judge should bear on the action of the legislator in its obligation to define with sufficient precision the scope of powers given to police forces. It does not seem realistic however to advocate for a too strict definition of purposes of data processing activities carried out by public authorities by law. This would entail a greater

rigidity of the legal framework incompatible with the increased flexibility often required to public authorities in the performance of their tasks.

Law is by definition abstract and rather inflexible. It is not suited, by itself, for ensuring an effective application of data protection safeguards in a technological context where interoperability and information sharing have become the rule. The definition of purposes and conditions for data processing by the Law should be completed by other tools, more flexible, closer to data controllers, to their day-to-day activity. These tools should serve the purpose of fostering the emergence a culture of data protection amongst data controllers, bringing data protection constraints closer to their needs. Three different instruments which act on an a priori basis likewise the purpose specification principle and whose use is progressively been promoted can be suggested: (a) privacy impact assessments that compel data controllers to take into account privacy constraints from the very beginning of the conception of the system and further on during the whole life of the data processing; (b) licensing systems relying on data protection authorities for most harmful data processing activities such as the one involving genetic data as suggested by the European Commission in the proposals for the review of the Data Protection framework⁵², (c) data protection officers in charge of dealing with data protection aspects within the data controllers organization and who could bridge concerns of data controllers with the ones of data protection authorities and vice et versa, opening a window for dialogue. These instruments would allow to reducing the concentration of power that now mainly relies in the hands of the interpreter, i.e. the one who decides upon the personal data to be processed, in what way and for what purposes. It is worth noting that all three instruments are contained in the proposals put forward by the European Commission in the context of the review of the European data protection framework.

Whereas privacy impact assessments retain the power of decision for data controllers, they compel to a greater motivation of the choices made, to provide evidence of the needs the organization may have in processing such data.⁵³ The integration of video surveillance networks together with the use of video analytics tools turn such technology in a very powerful instrument of control whose use should be carefully assessed and limited. With regard to video surveillance, the U.K. Information Commissioner and other European data protection authorities such as the data protection authority of the Madrid Region (Spain) have advocated that controllers bear an obligation to carry out privacy impact assessments. This would allow to identifying and managing privacy risks at an early stage. Follow-up assessments can then be made by such organizations to assess whether the sharing of information is having the desired effect, for example in terms of reducing crime or providing a more efficient service to the public.⁵⁴

⁵² European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25.01.2012. COM(2012) 10.

⁵³ For an example of Privacy Impact Assessment framework, see Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, available at http://ec.europa.eu/information_society/policy/rfid/pia/index_en.htm

⁵⁴ Information Commissioner Office, Privacy Impact Assessment handbook and surveillance society conference website, http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_conference.aspx.

Licensing systems on the other hand give a major role to independent authorities, namely data protection authorities, in assessing the legitimacy of the data processed, the adequacy of the technical and organizational safeguards implemented. They enable data protection authorities to ensure a more efficient application of the safeguards implemented by data protection laws. To that effect, the 95/46/EC Directive enables Member States of the European Union to subject to prior checking data processing operations more likely to present specific risks to the rights and freedoms of data subjects (Article 20). Such a move would allow the relevant authorities to define the boundaries within which such processing could operate, based on the application of the principle of proportionality. This would reinforce the role of data protection authorities whose primary mission is, as recalled by the European Data Protection Supervisor, “to ensure compliance and to promote effective protection. It is only through these concepts that data protection rules and principles can become a reality in practice”.⁵⁵ This solution is one for which the French legislator when regulating the transfer from private video surveillance systems to law enforcement authorities has opted for by compelling owners to sign an agreement with the State representative which should be further checked by a National Committee for video surveillance.

Finally, data protection officers could play a significant role in bridging expectations of data controllers and the ones of data protection authorities. According to the 95/46/EC Directive, they should act in complete independence (Recital 49). They are endorsed by the Directive with the following functions: (a) ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive; (b) keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2); (c) thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by processing operations. The Directive also empowers them to carry out prior checks (Article 20). Data protection officers are therefore closer to the needs of the organization in which they evolve at the same time they act as independent observers in terms of data protection obligations. They could perform Privacy Impact Assessments and engage in prior checks together with data protection authorities.

7 Conclusion

The spread of IP based video surveillance technology eases interconnections of networks and cameras and the deployment of comprehensive monitoring systems. Ad hoc or permanent access to video surveillance networks are facilitated but also encouraged for purposes of increasing public safety and security. The technological facilities given to different actors to access one video surveillance networks or third parties’ video surveillance networks raise similar challenges for an efficient application of the purpose specification principle to the ones raised by the interoperability of police databases. Growing possibilities of information sharing crack the closed compartments that a strict application of the purpose specification principle was expected to create. Broader definition of purposes to give greater flexibility to public authorities activities prevent data subject to adequately foresee to what extent their personal data are processed. Linking the legitimacy of public data processing activities on the processing of data required for the performance of their tasks also fails to limit the scope of the interference into individuals’ right to privacy as long as the power of

⁵⁵ P. HUSTINX, The role of data protection authorities, Speech at the International Conference on Re-inventing data protection, 12-13 October 2007, Brussels, available online at: <http://edps.europa.eu/EDPSWEB/edps/lang/en/pid/23>.

interpretation remains exclusively into the hands of the data controller. These weaknesses are identified as source of failures of the purpose specification principle to adequately ensure the foreseeability of data processing activities.

The purpose specification principle remains however a cornerstone principle of data protection framework and as such it should continue to play a pivotal role in ensuring the foreseeability of data processing activities and by extension the one of public authorities when processing personal data. It however appears insufficient by itself to install strong barriers. Solution to this difficult issue should go through the implementation of additional procedural safeguards that will, in a way similar to the purpose specification principle, act a priori in limiting the scope of the data processing activities. These safeguards are identified in a broader use of privacy impact assessments, of licensing systems for interconnected video surveillance networks or the appointment of data protection officers. Such instruments would moreover foster the emergence of a data protection culture amongst data controllers. Data protection would then ideally become part of the “technical and organizational” constraints, integrated to the day-to-day of system designers and of video surveillance operators and would not be seen anymore as an external constraint. This is also the way forward proposed by the European Commission in both the draft general data Protection Regulation⁵⁶ the draft Directive on the protection of individuals with regards to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data.⁵⁷

⁵⁶ European Commission, 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, COM(2012) 11 final, Brussels, 25 January 2012.

⁵⁷ European Commission, COM(2012) 10 final, Brussels, 25 January 2012.