FP7 – SEC- 2011-284725

SURVEILLE

Surveillance : Ethical issues, legal limitations and efficiency

Collaborative Project

SURVEILLE Deliverable 4.1: The use of surveillance technologies for the prevention and investigation of serious crimes

Due date of deliverable : 31.10.2012

Actual Submission date : 31.10.2012

Start date of project: 01.02.2012 Duration 39 months

SURVEILLE Work Package number and lead : WP04 Prof. Martin Scheinin

Authors : Ms. Céline COCQ (Research Fellow FP7 SURVEILLE Project) and Dr. Francesca GALLI (FNRS Post-doctoral Researcher), Institut d'Etudes Européennes – ULB

Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	X
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 members of the consortium (including the commission Services)	

Abstract

Within the context of the SURVEILLE project, which offers a legal and ethical analysis of issues surrounding the use of surveillance technologies in three phases of countering serious crimes (prevention, investigation and prosecution) at the national as well as at the EU level, this deliverable conducts a comparative study of the development in the use of surveillance technologies for the prevention and investigation of serious crime within three selected national jurisdictions – France, Italy and the United Kingdom. It tests the existence of a double shift: (a) surveillance technologies introduced in relation to serious crime are increasingly used for the purpose of preventing and investigating "minor" offences; at the same time, surveillance technologies originally used for public order purposes in relation to minor offences are now increasingly affected to the prevention and investigation of serious crime; (b) means at the disposal of each actor (intelligence and law enforcement agencies) for the prevention and investigation of serious crime are evolving so that the share of tasks and competences has become blurred. Two surveillance technologies are selected as case studies: the interception of telecommunications and video-surveillance. The human rights dimension – the right to privacy and the principle of proportionality – constitutes the normative background of the present work.

Executive summary

- Public authorities should undertake a legal impact assessment before deciding on the harmonisation of the legislation supporting the use of surveillance technologies such as the interception of telecommunications and the means of video-surveillance in the prevention and investigation of serious crimes. Such an analysis should identify potential interferences between the different legal systems of all Members States.

- The need to use surveillance technologies in order to gather information in the prevention and investigation phases must be established. Yet, its use should be evaluated with regard to the degree of intrusion into the private life of individuals in order to ensure a proportionate and least invasive outcome.

- The core of the assessment of the use of surveillance technologies in the criminal substantive and procedural law should be to highlight the similarities and differences between different States, namely France, Italy, the United Kingdom, Germany and Spain.

- The use of surveillance technologies is particular relevant for the purpose of gathering information to prevent and investigate serious crimes. However, it could also interfere with the right of privacy. The seriousness of the offence is thus the reason of the authorisation of such an intrusive measure. This deliverable provides an overview of how each surveillance technology used in the prevention and investigation phases is regulated in defining at least these elements:
    - the nature of the offences which may give rise to the use of surveillance technologies;
    - the categories of people which the technology may be used against;
    - the limit on the duration of the measures using surveillance technologies ;
    - the procedure to be followed for collecting and using the information obtained;
    - the precautions to be taken when communicating the data to other parties;
    - the circumstances in which such information may or must be erased.

- While the surveillance technologies, starting from the investigation phase, are well regulated, the use of these same technologies in the prevention phase and the share of information between actors involved in both phases are sometimes criticised by the defendant of the human rights as well as by the actors of the collect of information themselves. In this context, the use of surveillance technologies in public places must be clearly regulated by national provisions as well as European instruments in both the prevention and investigation phases. The actors responsible of the use of technologies, their competences/powers and tasks should be also clearly identified.

Table of contents

1. Introduction

The years following 11 September 2001 with the 2004 bombings in Madrid, the 2005 attacks in London, the 2011 attacks in Norway and the 2012 attacks in Toulouse show profound changes in the terrorism threat and the emergence of the parallel phenomena of home-grown terrorism and lone-wolves terrorist actors.[1]

Such changes have had a tremendous impact on the criminal justice system as a whole leading to a progressive shift towards prevention in the fight against terrorism at the national as well as at the EU level.[2] The evolving terrorist threat has had most importantly a catalysing effect on: the enactment of new inchoate offences and the criminalisation of preparatory activities[3]; and, the development of anticipative/proactive criminal investigation.[4]

The deliverable focuses on one fundamental change within this second dimension, namely the increasing use of surveillance technologies in the fight against serious crime,[5] and especially against terrorism.[6] In fact, by contrast with the DETECTER Project[7], for which the scope of the research was limited to terrorism, the FP7 SURVEILLE project covers "serious crimes"[8], which includes terrorism.[9]

Thus, this paper is to be seen in the context of the SURVEILLE project, which offers a legal and ethical analysis of issues surrounding the use of surveillance technologies in three phases of countering serious crimes (prevention, investigation and prosecution) at the national as well as at the EU level. It is based on the definitions provided within this project[10] and should be read in conjunction with the other deliverables submitted or soon to be submitted.[11]

The comparative study tests the existence of a double shift mainly resulting from the catalysing effect of serious crime.

---

[1] See EUROPOL, *EU Terrorism Situation and Trend Report (TE-SAT)* (2012); K.L. Thachuk and al., *Homegrown Terrorism. The Threat Within*, Center for Technology and National Security Policy, National Defense University (2008); T. Precht, *Home grown Terrorism and Islamist Radicalisation in Europe,* Danish Ministry of Justice (2007).

[2] See *e.g.* G. de Kerchove, "L'Union européenne et le monde dans la lutte contre le terrorisme" *in* M. Dony (ed.), *La dimension externe de l'espace de liberté, de sécurité et de justice au lendemain de Lisbonne et de Stockholm: un bilan à mi-parcours*, Editions de l'Université de Bruxelles (Bruxelles, 2012); M. Donini, « Sicurezza e diritto penale », (2008) 10 Cass pen 3558.

[3] See *e.g.* K. Sugman Stubbs and F. Galli, "Inchoate offences. The sanctioning of an act prior to and irrespective of the commission of any harm" *in* F. Galli and A. Weyembergh (eds.), *EU counter-terrorism offences: what impact on national legislation and case law*, Editions de l'Université de Bruxelles (Bruxelles, 2012).

[4] See *e.g.* M.F.H. Hirsch Ballin, *Anticipative criminal investigations. Theory and counter-terrorism practice in the Netherlands and the United States*, TMC Asser Press, (The Hague, 2012).

[5] Yet serious crime is not defined as such in EU law (art. 83(1) TFUE). For the purpose of the analysis examples are hence taken from national legislation, mostly with reference to organised crime and terrorism. Both categories are particularly relevant because they have lead to the introduction of specific legal regimes for the use of surveillance technologies within the three countries.

[6] See *e.g.* H. Fenwick (ed.), *Development in counter-terrorist measures and uses of technology*, Routledge (Abingdon, 2012).

[7] DETECTER Project (Detection Technologies, Counter-Terrorism Ethics, and Human Rights), FP7 Security Programme, www.detecter.bham.ac.uk (accessed on 27 October 2012)

[8] SURVEILLE Project FP7, SEC 2011.6.1-5, Surveillance and challenges for the security of the citizen, Annex 1 – "Description of Work", p. 12

[9] SURVEILLE Project, Annex 1 – "Description of Work", p. 4-15

[10] *See infra*.

[11] SURVEILLE, Surveillance : Ethical Issues, Legal limitations and Efficiency, FP7-SEC-2011-284725, "Report describing the design of the research apparatus for the European-level study of perceptions", D3.1, October 2012; "Survey of surveillance technologies, including their specific identification for further work", D2.1 August 2012.

Firstly, surveillance technologies introduced in relation to serious crimes (*e.g.* interception of telecommunications) are increasingly used for the purpose of preventing and investigating "minor" offences; at the same time, surveillance technologies originally used for public order purposes in relation to minor offences (*e.g.* CCTV cameras) are now increasingly affected to the prevention and investigation of serious crime.

On the one side, serious crime including terrorism has had a catalysing effect on the criminal justice system, prompting an increased use of surveillance techniques and technologies. The subsequent introduction of derogatory provisions has been first regarded as exceptional and limited in scope first to terrorism and then to organised crime. Through a normalisation process at the initiative of the legislator, specific measures have become institutionalised over time as part of the ordinary criminal justice system and they have a tendency to be applied beyond their original scope.[12]

On the other side, a parallel shift has occurred in the opposite direction. Video-surveillance technologies, which are one of the most obvious and widespread signs of the development of surveillance, were originally conceived by the private sector for security purpose. They have been subsequently employed for public order purposes and finally in the prevention of minor offences and/or petty crimes (such as street crimes or small drug dealers). In such context, they were rather a tool to deter would-be criminals rather than an investigative means.[13] At the same time, the terrorist threat has become an argument for an even more extensive use of video surveillance.

The question therefore arises as to: whether there is still a difference to be made between means that can be used only in the fight against serious crime and others applicable only to counter minor offences; or whether a mutual contamination has occurred so that means originally introduced in one or the other domain are now applicable to both the prevention and investigation of serious crime and minor offences.

Secondly, means at the disposal of each actor (intelligence[14] and law enforcement agencies) for the prevention and investigation of serious crime are evolving so that the share of tasks and competences has become blurred.

When coping in particular with the terrorism threat, democratic States have had to redraw the boundaries between the different tasks involving surveillance, namely protecting national security, maintaining public order, preventing and investigating crimes. This has taken several forms: the extension of surveillance powers in all these tasks; the emergence of new challenges resulting from the use of intelligence information gathered for national security purposes in criminal prosecutions; the sharing of information and the creation of "fusion centres" where data are merged while maintaining more or less a division of tasks between intelligence agencies and law enforcement authorities.

---

[12] O. Gross, 'Chaos and rules' (2003) 112 *Yale Law Journal* 1011, 1090; D. Dyzenhaus, "The permanence of the temporary" *in* R.J. Daniels and others (eds.), *The security of freedom*, University of Toronto Press (Toronto, 2001).

[13] *e.g.* A. Bauer and F. Freynet, *Vidéosurveillance and vidéoprotection*, PUF (Paris, 2008); EFUS, *Citizens, Cities and video surveillance, Towards a democratic and responsible use of CCTV*, ed. EFUS (Paris, 2010) pp. 183-84; Vidéo-surveillance Infos, "Dispositif de sécurité au stade de France: ergonomie et évolutivité" (14 October 2011).

[14] Intelligence information refers to "secret material collected by intelligence agencies and increasingly by the police to provide background information and advance warning about people who are thought to be a risk to commit acts of terrorism or other threats to national security".[14] K. Roach, "Secret evidence and its alternatives" *in* A. Masferrer (ed.), *Post 9/11 and the state of permanent legal emergency. Security and human rights in countering terrorism*, Ius Gentium: Comparative Perspectives on law and justice, Springer (2012) p. 180.

Such a development has lead to an unclear situation as a broad range of investigation techniques and technologies may be used in relation to different offences as well as at different phases of the procedure, *e.g.* prevention or investigation.

The question to be assessed in relation to the second dimension of the shift is thus whether the current trend has provided an opportunity to clarify the share of tasks and competences between intelligence services and law enforcement authorities (including *police administrative* and *police judiciaire*) or rather whether it lead to a more blurred division.

A blurred division would lead to both a situation of legal uncertainty and a competition between the different actors involved.

Surveillance may be defined as "the keeping of watch over someone or something. Technological surveillance is the use of technological techniques or devices to detect attributes, activities, people, trends, or events."[15]

For the purpose of this research, two surveillance technologies – used by both law enforcement authorities and intelligences agencies – have been chosen as the examples of the first dimension of the double shift hypothesis: the interception of telecommunications and video surveillance (most importantly CCTV cameras).

It is noteworthy that interception of telecommunications is a broader category than "phone interception" as it encompasses also the interception of emails or other messages sent via the Internet.[16] This kind of interceptions operate in real time and may deal with the content of the telecommunications and is thus more intrusive into privacy than other measures such as identification or tracking, which do not address the content. The scope of this study does not include provisions on the retention on data by private compagnies for either commercial of law enforcement purposes which will constitute the focus of subsequent research.[17]

In relation to video-surveillance technologies, this article only focuses on the use devices installed either by public authorities (*e.g.* in the streets, train stations, airport, stadium) or by private companies (*e.g.* shopping malls, outside banks) for prevention purpose. Thus, neither the video-surveillance taking place in the framework of a criminal investigation, authorised and then executed by judicial competent authorities with reference to a targeted individual nor the video-surveillance under the supervision of public authorities in private premises are part of this deliverable.

This study focuses on three EU Member States, namely France, Italy and the United Kingdom. Various reasons justify this choice: these states have experienced terrorism before 9/11 and the fight against serious crime has long been a priority; they also are working

[15] J.K. Petersen, *Handbook of surveillance technologies*, 3d ed., CRC Press, Taylor & Francis Group (2012) p. 10. Within the SURVEILLE Project, surveillance is defined as "targeted or systematic monitoring of persons, places, items, means of transport or flows of information in order to detect specific, usually criminal, forms or conduct, or other hazards, and enable, typically, a preventive, protective or reactive response or the collection of data for preparing such a response in the future". Surveillance technologies are hence "the use of any human-made devices in surveillance" or methods "used to detect something in a security or safety context, with the focus on a law enforcement, customs or security authority". SURVEILLE Project, Annex 1 "Description of Work", p. 5.

[16] In the United Kingdom, s. 2 RIPA 2000 defines a telecommunication system as « any system which exists for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy ». Remarkably, in some countries the same rules apply to the interception of communications via the Internet, whereas in others there is a gap in the existing regulation and this constitutes part of the problem.

[17] See "Comparative paper on data retention regulation in a sample of EU Member States", SURVEILLE Project, D4.3 (submitted on 30 April 2013).

together in the EU G6;[18] their national legislation has been a point of reference for the development of EU policies and instruments such as the two Framework Decisions on combating terrorism of 2002 and 2008.[19] Moreover the chosen case studies must be representative of: both common law and civil law systems; different criminal procedure systems (accusatorial/inquisitorial/mixed); different systems of share of competences and of articulation between intelligence and law enforcement bodies (including *police administrative* and *police judiciaire*).[20]

The use of surveillance technologies and additionally the information gathered is particularly sensitive with regard to the right to privacy they may affect and the principle of proportionality with reference to the conditions allowing for their use.[21] The human rights dimension will be the backdrop of this research.

The deliverable will provide a brief overview of criminal procedure developments in the selected Member States resulting from the catalysing effect of organised crime and terrorism (2). Then it will analyse the different elements of the double shift with reference to the two surveillance technologies chosen as case studies: the interception of telecommunications (3) and video-surveillance (4). Eventually, it will ascertain the existence of a blur in the share of tasks (5).

2. The expansion of derogatory regimes to cope with serious crime

In the three Member States, specific (and often derogatory) provisions, both of substantive criminal law and criminal procedure, have been adopted over time in order to fight against serious crime, especially against terrorism and/or organised crime.[22]

Remarkably, both in France and in Italy there has been a reciprocal influence of anti-terrorism and anti-organised crime legislation during the last thirty years and the subsequent re-enactment of repealed provisions following a new outburst of terrorism or organised crime at different stages.

In Italy, since 1975 (Law 152/1975) special measures adopted to deal with the domestic terrorist threat have been progressively introduced as derogations to the ordinary

[18] The EU G6 is an internal security vanguard made up of the interior ministries of Britain, France, Germany, Italy, Poland and Spain. According to H. Brady, "with the possible exception of Poland, these countries all feel threatened by terrorism and have elaborate national counter-terror systems", H. Brady, "Intelligence, emergencies and foreign policy – The EU's role in counter-terrorism", *Centre for European Reform* (2009) p. 7.
[19] Framework Decision 2002/474/JHA on combating terrorism [2002] OJ L 164/3 and Framework Decision 2008/919/JHA [2008] OJ L 330/21. For a detailed comment on the interplay between the two instruments see Galli and Weyembergh (eds.), *EU counter-terrorism offences*, pp. 11-32, pp. 49-64; pp. 83-98; pp. 117-132.
[20] The organisation for each State differs according to his traditional system: the common law division (police intelligence, police investigation and prosecution by judicial authorities) and the civil law twofold division (administrative police and judicial police).
[21] S. Van Drooghenbroeck, *La proportionnalité dans le droit de la convention européenne des droits de l'homme. Prendre l'idée au sérieux*, Bruylant, (Bruxelles, 2001); C. Warbrick, 'The ECHR and the Prevention of Terrorism' (1983) 32 *ICLQ* 82 ; Institute for prospective technological studies, *Security and privacy for the citizen in the Post-September 11 digital age: A prospective overview,* Report to the European Parliament Committee on citizens' freedoms and rights, justice and home affairs (LIBE), EUR 20823 (July 2003); M. Levi and D.S. Wall, "Technologies, Security, and Privacy in the Post-9/11 European Information Society" (2004) 31(2) Journal of Law and Society 194.
[22] F. Galli, *British, French and Italian measures to deal with terrorism: a comparative study*, Doctoral thesis, University of Cambridge, 2009 (yet unpublished).

principles of criminal law.[23] The enactment of the new *Codice di Procedura Penale* in 1988 was meant to redress the numerous derogations brought about by the emergency legislation in the previous decade. However, from when the level of the threat from organised crime increased once again at the beginning of the 1990s, the existing tools seem inadequate and major changes in the law came along in the form of subsequent layers of new principles, rules and exceptions and not as a coherent legislative design (see *e.g.* Law 203/1991).[24] With the enactment of Law 438/2001 and Law 155/2005 the scope of many of these provisions has been extended to cope with the newly emergent international terrorist threat.

On 9 March 2004, the French Parliament enacted the so-called *Loi Perben II* (Law 204/2004), which contains the most far-reaching amendments of substantive criminal law and criminal procedure of the last decades.[25] In this context special anti-terrorist procedures (*e.g.* with regard to house searches, identification of individuals, *garde à vue*, surveillance, or interception of communications) have been applied to a long catalogue of offences classified as "organised crime". As in the case of the definition of terrorism as a criminal offence, the legislator has not attempted to define "organised crime" and has merely introduced in the *Code de Procédure Pénale* a list of more than thirty offences to which special procedures become applicable. This list also includes a number of less serious offences (such as extortion, procuring or assistance in the illegal entry of immigrants) which do not obviously justify the use of extraordinary powers. The legislator can expand this catalogue at any time.

In the United Kingdom, the counter-terrorism "arsenal" is only the tip of the iceberg of a broader phenomenon, most importantly in relation to the use of administrative measures which are no longer exceptional and temporary, nor are they necessarily linked with a genuine emergency (see *e.g.* Sexual Offences Prevention Orders (SOPO) and Risk of Sexual Harm Orders, Anti-Social Behaviour Orders (ASBOs), Serious Crime Prevention Orders and Violent Offender Orders. Not all preventive orders require a criminal offence to have been committed).[26]

In relation to the **definition of terrorism** the three countries have taken similar approaches.[27] In the first place, the aim of the attempts was to prompt the use of special procedural measures. Secondly, the definitions adopted at different stages share a common core of *mens rea* derived from international sources: the intention to make indiscriminate use of violent activities to spread intimidation or terror within a community and thus influence an institutional figure for political or subversive purposes. French law attaches to such *mens rea* a list of existing criminal offences. The British definition, by contrast, encompasses only a list of behaviours exemplifying which type of activities would be proceeded against under the Terrorism Act 2000. And in Italy the definition is left open: any act committed with the identified *mens rea* would be considered an offence with a terrorist intent.[28]

Definition of organised crime

---

[23] G. Illuminati, "Reati "speciali" e procedure "speciali" nella legislazione d'emergenza" (1981) Giustizia Penale 106.

[24] P.L. Vigna, "Il processo accusatorio nell'impatto con le esigenze di lotta alla criminalità organizzata" (1991) Giustizia Penale 462.

[25] J. Pradel, "Vers un ''aggiornamento'' des réponses de la procédure pénale à la criminalité" (2004) 19 Semaine Juridique 132 and (20) Semaine Juridique 134.

[26] Some require the subject to have been convicted or an offence, and others require the civil court imposing the order to be satisfied that he has committed one.

[27] art. 421(1) French *Code Penal*, art. 270 *sexies* Italian *Codice Penale,* s. 1 UK Terrorism Act 2000

[28] F. Galli, *British, French and Italian measures to deal with terrorism: a comparative study*, pp. 60-72 (yet unpublished).

	France	Italy	United Kingdom
Definition	*Association de malfaiteurs* [29] (no need of a number of associates)	*Association de malfaiteurs* (identification of a number of associates)	"individuals, normally working with others, with the capability to commit serious crime on a continuing basis, which includes elements of planning, control and coordination, and benefits those involved. A significant proportion of organised criminals are motivated, principally, by the desire to make money." [30]
Reference	Art. 450(1) Penal Code	Art. 416 and 416 *bis* PC	HM Government, *Local to global: reducing the risk from organised crime*, within the organised crime strategy of 28 July 2011

In France and in Italy, the law aimed at criminalising only those associations which were actively organised in gangs, the members acting with a common purpose framed by the existence of chiefs and conventions for the distribution of profits. By contrast with the parallel Italian provisions, the French Penal Code did not identify a minimum number of associates.[31]

The United Kingdom definition is less precise than the French or Italian ones. The structure and organisation of such groups may vary: they may consist of a durable group of key individuals surrounded by a cluster of subordinates or loose networks of individuals coming together for the duration of a criminal activity, acting in different roles depending on their skills and expertise. [32]

3. Towards a generalised use of surveillance technologies? The interception of telecommunications

Provisions concerning the interception of telecommunications in terrorist and organised crime cases often derogate from the ordinary regime.

In France and in Italy, two types of interceptions of telecommunications exist according to the phases of the procedure.

In **France**, a distinction must be drawn between interception of telecommunications during a judicial investigation for the detection and the investigation of a crime (judicial interceptions), and interceptions authorised by the executive for security reasons

[29] More narrowly drawn than the crime of conspiracy in English Law, in particular because the *association* must be demonstrated by acts putting it into execution.

[30] HM Government, *Local to global : reducing the risk from organised crime*, Policy paper, Organised crime strategy, 28 July 2011, p. 5 and 8.

[31] For a detailed account of the origins and purpose of this offence in Italy see G. Fiandaca, « I reati associativi nella recente evoluzione legislativa » *in* A. Spataro and others, *Il Coordinamento delle Indagini di Criminalità Organizzata e Terrorismo,* CEDAM (Padova 2004) pp. 1-34; and, in France, see M.C. Adolphe and M.F. Hélie, *Théorie du Code Pénal. Vol III,* Marchal et Billard (Paris 1887).

[32] Serious Organised Crime Agency at http://www.soca.gov.uk/threats/organised-crime-groups (accessed 1 March 2013); D. Blunkett, Home Secretary, White paper One Step Ahead – A 21st Century Strategy to Defeat Organised Crime, March 2004 used this definition adopted by the NCIS (National Criminal Intelligence Service); see also, M. Maguire, R. Morgan and R. Reiner (eds.), *The Oxford handbook of criminology*, 5th ed., (Oxford, 2012) p. 601.

(administrative interceptions) called *interceptions de sécurité*.[33]

Law 646/1991 provides the legal framework for both judicial (art. 100 ff *CPP*) and administrative interceptions (nowadays encompassed in the *Code de la Sécurité Intérieure*), as amended in 2002, 2004, 2006 and 2012.[34] Article 1 of Law 646/1991 reaffirms the principle of the secrecy of communications, from which only the public authority can derogate under the circumstances of public interest recognised and restricted by the law.[35]

As detailed below, over the years the legal regime of judicial interceptions has been considered by some to be too strict and inadequate and thus extraordinary provisions have been introduced for the purpose of an effective fight against organised crime.

The **Italian regime** reproduces the distinction between *ante-delictum* and *post-delictum* interceptions.[36] In ordinary cases, judicial interceptions of telecommunications are regulated by art. 266 and ff. *CPP*. Preventive interceptions are currently regulated under art. 226 *disp. att. CPP*, identifying the authorities entitled to apply for and issue interception warrants, the purpose of such application, and its specific content.[37] It is noteworthy that *ante-delictum* interceptions are not exclusively an administrative prerogative in Italian law.

The communications intercepted cannot be used as evidence when a professional privilege or a State or public secret is involved.[38] Additionally, interceptions made without complying with the relevant conditions are invalid and cannot be used at trial. This is one of the oldest 'exclusionary rules' in the Italian system.[39]

Exceptional provisions for the interception of communication under less stringent requirements were first enacted by art. 13 Law 203/1991 for the investigation of organised crime offences.[40] The complete re-organisation of the provisions on interceptions is one of the most important features of the new anti-terrorism regime (Law 431/2001 and Law 155/2005).[41]

In the **United Kingdom** there is no distinction between administrative or judicial interceptions, which is comparable to the French or Italian models. Interception of telecommunications is regulated under the Regulation of Investigatory Power Act (RIPA) 2000.[42] This Act establishes the legal regime for different surveillance techniques.[43] In doing

---

[33] F.-B. Huyghe, *Les écoutes téléphoniques*, Que sais-je ? PUF, n°3874 (Paris 2010) ; C. Guerrier, *Les écoutes téléphoniques*, CNRS (Paris, 2000) ; R. Errera, *Les origines de la loi française du 10 juillet 1991 sur les écoutes téléphoniques*, Revue trimestrielle des droits de l'homme 55 (July 2003) pp. 851-870 ; J. Pradel, 'Un exemple de restauration de la légalité criminelle' (1992) Dalloz 49.

[34] The law applies not only to phone tapping but to all means of telecommunications (telephone, fax, telex, communication by radio, broadcasting of images, electronic communication, etc.).

[35] Freedom of expression is considered of constitutional value. DC n°84-181 (1984). Also art. L241-1 *CSI*.

[36] G. Spangher, "La disciplina italiana delle intercettazioni di conversazioni o comunicazioni" 1 Archivio Penale 3, 1994; P. Balducci, *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria*, Milano, Giuffrè 2003; C. Parodi, *Le intercettazioni. Profili operativi e giurisprudenziali*, Giappichelli (2002); A. Balsamo, "Intercettazioni: gli standards europei, la realtà italiana, le prospettive di riforma"(2009) 10 Cass pen 4023.

[37] See in relation to terrorist offences G. Garuti, "Le intercettazioni preventive nella lotta al terrorismo internazionale" (2005) *Diritto Penale e Processo* 1457

[38] G. Illuminati (ed.), *Nuovi profili del segreto di stato e dell'attività di intelligence*, Giappichelli, (Torino 2011).

[39] art. 271 *CPP*.

[40] G. Melillo, "La ricerca della prova tra clausole generali e garanzie costituzionali: il caso della disciplina delle intercettazioni nei procedimenti relativi a 'delitti di criminalità organizzata'", (1997) Cassazione Penale 3512.

[41] e.g. F. Caprioli, 'Le disposizioni in materia di intercettazioni e perquisizioni' *in* G. Di Chiara (ed), *Il processo penale tra politiche della sicurezza e nuovi garantismi*, Giappichelli (Torino 2003).

[42] *e.g.* D. Ormerod and S. McKay, "Telephone intercepts and their admissibility" (2004) Criminal Law Review 15; P Mirfield, 'RIPA 2000: Part 2: Evidential Aspects' (2001) Criminal Law Review 91; M Ryder, 'RIPA reviewed',(2008) 4 Archbold News 6; Sir J. Chilcot, 'Privy Council Review of intercept as evidence: report to the Prime Minister and the Home Secretary', Chilcot Review (Cm 7324 2008).

so, it takes into account not only the latest technological developments but also the ECHR and the related case law.[44]

The most important aspect of regulation in this context is that intercepted conversations are not admissible as evidence in criminal proceedings.[45] Interception of telecommunications can be used for investigative purposes and as an instrument for crime prevention (information gathering) but not for prosecution. The contents of interception of telecommunications may provide the police with lines of enquiry but may not be used as evidence in a public court.[46] Nevertheless, because the restrictions under s. 17 RIPA apply only to interception conducted in the United Kingdom, communications lawfully intercepted by foreign authorities in their own jurisdictions may be adduced in evidence in the UK court.[47]

It is noteworthy that, in the three countries, wiretapping or interception of telecommunications without legal authorisation is an offence.[48]

After this general presentation, the comparative study focuses on the actors involved in the interception for either authorisation or execution purposes, its scope and duration.

Differences exist between *ante-* (mainly administrative) and *post-delictum* (mainly judicial) interceptions. Interceptions of telecommunications have been first developed for investigative purposes and then also used for preventive purposes. Therefore, the analysis will starts with the first one and then continue with the second one.

3.1. Post-delictum interceptions

3.1.1. Actors

With regard to actors, two issues are worth comparing: who authorises the interceptions and who executes them.

3.1.1.1. France

In most cases of **post-delictum interceptions,** the authorisation is given by a judicial authority both in France[49] and in Italy[50].

In terms of existing derogation, it is noteworthy that in **France**, Law 204/2004 extended the possibility to use judicial interceptions to preliminary and *in flagrante* police investigations (*i.e.* to cases where no *instruction* has been yet instituted) for a limited number

---

[43] The investigatory powers regulated by RIPA 2000 are: the interception of communications, the acquisition of communications data (eg telephone billing data), intrusive surveillance (on residential premises or private vehicles), covert surveillance during specific operations, the use of covert human intelligence sources (agents, informants and undercover agents) and access to encrypted data.

[44] RIPA (ch.1, s. 5) introduced numerous changes in the Interception of Communications Act (IOCA) 1985, which had been enacted in response to the condemnation of the United Kingdom by the Strasbourg Court in the *Malone* case (*Malone* v. *UK* (1984)). In that case the Strasbourg Court made it clear that the existing rules and practices in the United Kingdom did not satisfy the requirement of art. 8 ECHR that any interference with a person's privacy by a public authority should be 'in accordance with the law'.

[45] This ban has long been the most controversial feature of the interception legal regime. At present, neither the government nor civil libertarians seem to be particularly concerned by the intrusion into personal privacy, as similar kinds of evidence (covert agents, bugging, eavesdropping, video-surveillance) are already admissible in court, even where not authorised, without any particular practical difficulty.

[46] s. 15(3) and 17 RIPA. See JUSTICE, *Intercept evidence: Lifting the ban*, Report (October 2006).

[47] *R.* v. *Aujla* [1998] 2 Cr App R 16 approved by the House of Lords in *R.* v. *P.* [2001] 2 WLR 463.

[48] arts. 615, 617, 617*bis*, 623*bis* CP.

[49] art. 100 and ff *CPP*.

[50] art. 266 and ff *CPP*.

of serious offences listed in art. 706(73) *CPP*. According to art. 706(95) *CPP*, these kinds of interception are requested by the prosecutor, authorised and supervised by the *juge des libertés et de la détention (JLD)*, and carried out by the police officers (*police judiciaire*). These operations and recordings are subjects to a statement (*procès-verbal*) written by the police.

This is the technique most often used by the *JIRS* (*juridictions inter-régionales spécialisées*)[51] for the purpose of investigation and prosecution of the crimes listed in article 706(73) CPP, the most serious offences, usually committed by an organised group.[52]

3.1.1.2. Italy

In the **Italian regime,** the interception warrant is issued by the judge for preliminary investigations (*giudice per le indagini preliminary, GIP*) upon the request of the prosecutor.[53] However, when the measure is motivated by emergency[54], the prosecutor may act without the prior authorisation of the judge.

In ordinary cases, the interception is authorised by a reasoned decision where there are serious grounds (*gravi indizi*) to believe that a crime has been committed and it is absolutely indispensible for the purposes of the investigation.[55] However, the GIP – who is formally in charge of keeping these proceedings under scrutiny – is unaware of the facts grounding the investigation. So it is difficult for him to assess the seriousness of the file.[56] In addition, the prosecutor can exceptionally authorise interceptions when there is some urgency.[57]

After having been authorised, judicial interceptions must be carried out by the office of the prosecutor, but the measure may also be executed by the police under the supervision of the prosecutor.[58]

3.1.1.3. The United Kingdom

By contrast, in the **United Kingdom**, there is no distinction between *ante-* and *post-delictum*, thus the interception is always authorised by an administrative authority, and not a judicial one. There is a limited number of persons by whom, or on behalf of whom, the applications for issue of interception warrants may be made and all interception warrants are issued by the Secretary of State or by a senior official in urgent cases and where there is a request for international mutual assistance.[59]

Nevertheless some features of the regime are of interest. Under sections 5–8 RIPA at the request of authorised officials,[60] the Secretary of State may lawfully grant an interception warrant only if the existence of certain limited grounds are satisfied and only if necessary and proportionate.[61] The police act under this warrant. As underlined by Prof. Spencer, "in all

[51] The *JIRS*, created by Law 204/2004, bring together prosecutors and judges of the instruction and are specialised in organised crime, financial crime, but also in complex cases justifying significant investigation.
[52] J. Pradel and J. Dallest, *La criminalité organisée – Droit français, droit international et droit comparé*, Litec, (2012) p.144.
[53] art. 267 *CPP*.
[54] art. 267(2) *CPP*.
[55] F. Galluzzo, "Spunti di riflessione in tema di intercettazioni" (2010) 9 Cass pen 3141.
[56] See D. Siracusano and others, *Diritto processuale penale Vol II*, Giuffrè (Milano 2006) pp. 151-52.
[57] The prosecutor must within 24 hours ask for validation by the judge (art. 267-2 CPP) who has to decide on the validity of the measure within 48 hours. If the authorisation is not validated within the prescribed period, the interception has to stop and the results cannot be used.
[58] art. 268(3) *CPP*.
[59] art. 6(2) and 7(2) RIPA 2000.
[60] *e.g.* Chiefs Constable, Chiefs of the Intelligence and Security Services, Director of Government Communication Headquarters, Director General of the National Criminal Intelligence Service; s. 6(2) RIPA 2000.
[61] s. 5(3) RIPA 2000.

three parts of the United Kingdom warrants to intercept communications are issued not by judges, but by ministers: usually the Home Secretary. Neither they nor their civil servants wish the legality or propriety of their decisions to issue warrants to be scrutinised by judges in any prosecutions that might follow, and to avoid this, prefer a situation in which the fruit of the intercept can only be used as "operational material", even though this is a dreadful obstacle to prosecution."[62]

3.1.2. Scope

3.1.2.1. France

Regarding the **scope** of the measure, in **France**, whereas "ordinary" interception is possible for any crime or *délit* punishable with a minimum sentence of two years of imprisonment, the **post-delictum interception** allowed by art. 706(95) *CPP* is possible only in case of offences listed in article 706(73) *CPP*, namely the most serious offences linked to organised crime (*e.g.* murder committed "*en bande organisée*") and in compliance with the necessity and proportionality of the use of such technique.[63]

It is noteworthy that police officers may extend the surveillance to the whole territory after informing the prosecutor (no agreement is required but the prosecutor can object), if there are one or several plausible reasons to suspect someone of having committed one of the crimes and misdemeanours of the article 706(73).[64]

3.1.2.2. Italy

In **Italy, post-delictum interceptions** may be used in relation to most serious offences, such as intentional crimes punishable with imprisonment with a maximum penalty of at least five years (art. 266(1) *CPP*).

A specific regime applicable for organised crime was introduced in article 13 of Law 203/1991 and, then extended to terrorist cases by article 3 Law 438/2001 and more recently to human trafficking by article 9 Law 228/2003.

Three main derogations are thus introduced to the ordinary regime. Firstly, an interception can be authorised where there are sufficient (as against "serious") grounds (*sufficienti indizi*) for believing that a crime has been committed.[65] Secondly, interceptions need only to be necessary (rather than indispensable) for investigative purposes. Thirdly, the interception may aim at developing new investigative paths (rather than being merely employed in the course of an already established investigation).

In addition, article 6 of Law 438/2001 extends the authorisation of the use of interception of telecommunications (*intercettazioni ambientali*) to seek out fugitives.[66]

3.1.2.3. The United Kingdom

In the **United Kingdom**, by contrast to what have been said in the section on actors, a difference exists in relation to whether they are in the context of a prevention or investigation of offences. During the investigation phase, when law enforcement agents are gathering information, the methods used depend on the complexity of and not on the gravity of any suspected offence. Interception without a warrant is possible if one party consents and if surveillance by means of interception has been authorised under RIPA provisions.

---

[62] J.R. Spencer, "No thank you, we've already got one, Why EU anti-terrorist legislation has made little impact on the law of the UK", *in* Galli and Weyembergh (eds.), *EU Counter-terorrism offences*, p. 129.

[63] ECHR, *Huvig and Kruslin* v. *France,* 11105/84 [1990] ECHR 9, 24 April 1990 ; ECHR, *Lambert* v. *France*, 1998-V, n°86, 24 August 1998; ECHR, *Matheron* v. *France,* 57752/00, 29 March 2005.

[64] art. 706-80 *CPP*.

[65] Note that following the enactment of Law 63/2001 on due process, information resulting from police informers or security services are not admissible for this purpose (art 203(1) *CPP*).

[66] art. 295(3) *CPP*.

3.1.3. Duration

Provisions concerning the **duration** of the measure are also different for *ante-delictum* or *post-delictum* interceptions.

3.1.3.1. France

Concerning ***post-delictum* interceptions**, in **France,** in ordinary cases, the *juge d'instruction* may authorise the interception for a maximum period of four months. Such an initial period can, however, be extended as long as necessary for investigative purposes.[67] However, in the framework of the fight against the most serious crimes, the *JLD* may, at the request of the prosecutor, authorise the interception for a maximum period of one month, renewable once under the same conditions of form and duration.[68] Finally, the *procès-verbaux* are destroyed at the behest of the prosecutor and at the expiry of the limitation period for the public action.[69]

3.1.3.2. Italy

Post-delictum interceptions, in **Italy,** can last for up to fifteen days, renewable as many times as the reasons for the initial decision exist and upon authorisation of the judge for preliminary investigations.[70] Interceptions in terrorist and organised crime cases can last for up to forty days (rather than fifteen)[71], renewable for subsequent periods of twenty days (rather than fifteen), when the reasons for the initial decision still exist.[72] There is no limit on the number of possible renewals. In case of emergency, the renewal can be authorised by the prosecutor and then validated by the judge, who has to verify the existence of urgency.

3.1.3.3. The United Kingdom

In the **United Kingdom,** according to RIPA 2000, the duration of the initial interception warrant was originally meant to be of three months at most, although renewable. The Terrorism Act 2006 has amended RIPA so that the duration of the initial interception warrant issued in the interests of national security is extended to six months and it is renewable at any time before the end of the relevant period for another six-month period.[73]

Post-delictum interceptions

	France	Italy	United Kingdom
Ground 1	*Crimes* and *délits* (max penalty ≥ 2 years)	Crimes (max penalty ≥ five years (art. 266(1) CPP)	Complexity of the offence; only if necessary and proportionate
Authorisation	*Juge d'instruction* (art. 100 *CPP*)	Prosecutor after authorisation of the judge for preliminary	Secretary of State or by a senior official in urgent cases and where there is a

[67] art. 100(2) *CCP*.
[68] art. 706(95) *CPP*. An amendment to *Loi d'orientation et de programmation pour la performance de la sécurité intérieure* was adopted on 9 September 2010 on the initial deadline of 15 days changed to one month. The interception may last shorter than in oreinary cases because it is not requested by the juge d'instruction but simply at the request of the prosecutor and the judicial guarantees are thus more limited.
[69] Cass. Crim., 21 February 2007, BC 55, p. 304. The rule is not applicable to the *procès-verbaux* of the transcription of interceptions, which are procedural pieces.
[70] art. 267(3) *CPP*.
[71] art. 13 Law 203/1991.
[72] art. 13 Law Decree 152/1991, converted into Law 203/1991.
[73] s. 32 TA 2006.

		investigation (art. 267 CPP); in the case of emergency, authorisation from the prosecutor	request for international mutual assistance
Duration	4 months	15 days	6 months (Terrorism Act 2006)
Renewal	no limit	no limit	no limit
Ground 2	Suspicious deaths or disappearances	organised crime (art. 13 Law 203/1991); extended to terrorist cases by art. 3 Law 438/2001 and more recently to human trafficking (art. 9 Law 228/2003)	
Authorisation	*Juge d'instruction* (art.80(4) *CPP)*	prosecutor	
Duration	2 months	40 days (art. 13 Law 203/1991)	
Renewal	no limit	20 days each renewal (art. 13 Law 203/1991)	
Ground 3	Hunting of an individual on the run		
Authorisation	Public prosecutor under the authority of the *JLD* (arts. 74(2), 695(36) and 696(21) *CPP*)		
Duration	2 months		
Renewal	Renewable in the limit of 6 months for ordinary offences (*correctionnelle*)		
Ground 4	Organised crime		
Authorisation	Public prosecutor under the authority of the *JLD* (art. 706(95) *CPP)*		
Duration	1 month		
Renewal	once renewable		

3.2. Ante-delictum interceptions

3.2.1. Actors

3.2.1.1. France

Regarding the **administrative interception** of telecommunications, in **France,** the use of these means is possible after a written and motivated decision by the Prime Minister. This

authorisation is given on the proposal of the Minister of Defence, Minister of the Interior or of the Minister of Customs.[74] This decision is sent immediately to the *Commission nationale de contrôle des interceptions de sécurité,* which ensures compliance with procedural rules.[75]

With regards to the **execution** of these means, an interesting feature in **France** concerns the execution of administrative interceptions and their transcription, which relies upon "*les personnels habilités*" (authorised personnel)[76] and thus implies a police officer (not necessarily *police judiciaire*) or a special named judge.

3.2.1.2. Italy

In **Italy**, in the case of *ante-delictum* interception, the Ministry of Interior[77] has general competence to apply for an interception for both organised crime and terrorism offences.[78] The warrant is issued by the prosecutor of the district that authorises the interception when the prevention interception is justified by enough elements of investigation and when it is necessary.[79] This interception may be done under the initiative of the law enforcement services and not only at the initiative of the prosecutor. In order to allow systematic scrutiny of the operations, the equipment to intercept the communications is physically located within the prosecutor's office. Law 155/2005 established a wider range of circumstances enabling the relevant authority to implement interceptions. In order to foster investigative and intelligence activities, the head of security and intelligence services (*SISMI* and *SISDE*) – acting after being delegated to do so by the Prime Minister – may apply to the prosecutor for an interception warrant whenever they are deemed to be necessary to prevent terrorist activities or subversion of the constitutional order *ex* art. 226 *disp. att. CPP*.[80] The legislator has thus attributed to the executive an important role in the political coordination of intelligence activities but has also placed a powerful new instrument in the hands of the security services.[81]

3.2.1.3. The United Kingdom

As previously said, the interception is always authorised by an administrative authority. According to the purpose of the interception and the degree of intrusion into the privacy, the level of authorisation is higher.

3.2.2. Scope

3.2.2.1. France

In **France**, ***ante-delictum* interceptions** are only used in exceptional cases as the research of information concerning national security[82], safeguarding essential elements of the scientific and economic potential of France, the prevention of terrorism, of crime and

[74] art. L 242-1 *CSI*.
[75] See the reports of the Commission nationale des interceptions de sécurité *in* La documentation française.
[76] art. L 242(5) *CSI*.
[77] Or, on his mandate, the central bodies of the police forces, the "questore", the province commander of the Carabineers and of the *Guardia di Finanza*. From the sole interpretation of the legislation one cannot understand whether these authorities can act autonomously.
[78] Whereas the director of the national Anti-Mafia Directorate has a role limited to organised crime offences.
[79] M.-L. Cesoni (ed.), *Nouvelles méthodes de lutte contre la criminalité: La normalisation de l'exception*, p. 196. Art. 5 Law 438/2001 provides for this possibility with wide discretion respecting to the ordinary regime.
[80] J.A.E. Vervaele, "Special procedural measures and the protection of human rights, General report", (2009) 5(2) *Utrecht L Rev*.
[81] On intelligence services' competence and organisation see Law 801/1977 as amended by Law 207/2007.
[82] See Commission nationale de contrôle des interceptions de sécurité, *Annual report*, 2009, 18th ed., Paris, La documentation française, p. 39 and ff.

organised crime or prevention of reconstitution or of maintaining of outlawed groups.[83] The Prime Minister motivates their use and "fishing expeditions"[84] are not allowed.

3.2.2.2. Italy

In **Italy,** *ante-delictum* interceptions are allowed to gather information when it is necessary for the prevention of organised crime, terrorism offences and human trafficking.

The extension of preventive interception is, in principle, offset by a more rigorous application of the rule of the inability to use the information within the criminal process[85], but only for investigative purposes. They are neither to be mentioned in investigative acts nor to be further disseminated by oral deposition or any other means.[86] They can be used as an element of a *notitia criminis* on which a prosecutor can start an investigation.[87] In addition, although the intercepted material cannot ground any other act or investigative tool, it can lead the police to the development of further autonomous investigations. Revealing this information is heavily penalised under Italian law.[88]

3.2.2.3. The United Kingdom

It is remarkable that in the **United Kingdom**, the use of interception of telecommunications is justified by the complexity of an offence and not by its seriousness. Hence the margin of appreciation of intelligence services and police in using this means is much broader.

For preventive purposes, the police can carry out telephone tapping in four situations: (1) in the interests of national security, (2) for the purpose of preventing or detecting serious crime, (3) for the purpose of safeguarding the economic wellbeing of the United Kingdom, (4) or in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.[89]

3.2.3. Duration

3.2.3.1. France

By contrast, in the case of **administrative interceptions** in **France** the authorisation is given for four months, renewable.[90] The recording is destroyed a maximum of ten days after the date on which it was made.[91] The transcripts of the recordings are destroyed once their storage is no longer necessary for the aforementioned preventive purposes.[92] A report of each operation is drafted, which mentions the date and time when the interception started and ended.

---

[83] art. L 241(2) *CSI*.

[84] A fishing expedition is a proactive action with surveillance technologies ; a speculative demand for information without a suspect, any real expectation about the outcome of the demand or its relevance to the investigation, where there is insufficient evidence to justify the issuing of a search warrant.

[85] art. 226(5) *disp. att. CPP* as modified by art. 5(5) Law 438/2001. See G. Melillo, 'Le recenti modifiche alla disciplina' (2002) Cass pen 904, 911; F. Ruggieri, *Divieti probatori e inutilizzabilità nelle intercettazioni telefoniche*, Giuffrè (Milano, 2001); C. Conti, "Intercettazioni e inutilizzabilità" (2011) 10 Cass pen 638; P. Sechi, "Intercettazioni e procedimento di prevenzione" (2011) 3 Cass pen 1082; S. Beltrani, "Intercettazioni inutilizzabili e procedimento di prevenzione" (2010) 9 Cass pen 2093.

[86] Two new criminal offences have been created in order to prosecute individuals who disseminate the intercepted material or the name of the officials involved in the proceedings.

[87] Cass. pen. 29 October 1998; Cass. pen. 10 November 2000.

[88] Vervaele, "Special procedural measures and the protection of human rights, General report" p. 94.

[89] s. 5 RIPA 2000.

[90] art. L242(3) *CSI*.

[91] art. L242(6) *CSI*.

[92] art. L242(7) *CSI*.

3.2.3.2. Italy

In **Italy** for *ante-delictum* interceptions, operations can last for a maximum of forty days, subject to subsequent renewals of twenty days each, where the legal requirements still exist (as confirmed by the prosecutor in his written motivated application).[93] Preventive interceptions must end once a criminal activity becomes manifest (*notitia criminis*).[94] However, the law does not limit the number of available renewals. Intercepted material and all copies, extracts and summaries identified as the product of an interception, must be securely destroyed as soon as they are no longer needed for any of the authorised purposes.

3.2.3.3. The United Kingdom

In the **United Kingdom**, the duration of interception is the same than for investigative purposes: six months renewable.

Ante-delictum interceptions

	France	Italy	United Kingdom
Ground	Prevention of terrorism, crime and organised crime; national security; scientific and economic protection; outlawed groups	Prevention of organised crime, terrorism offences and human trafficking	(1) Interests of national security, (2) prevention or detection of serious crime, (3) safeguard of the economic wellbeing of the United Kingdom, (4) or in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement (RIPA 2000)
Authorisation	Prime Minister (art. L242-2 CSI); proposal of the Minister of Defence, Minister of the Interior or of the Minister of Customs.	Ministry of Interior has a general competence; prosecutor of the disctrict authorises when there are enough elements of investigation and when it is necessary	Secretary of State or by a senior official in urgent cases and where there is a request for international mutual assistance
Duration	4 months	40 days	6 months (Terrorism Act 2006)
Renewal	no limits (art. L 242(3) CSI)	20 days each renewal (art. 226 CPP)	no limits

[93] art. 226 *CPP*. For the purpose of an increased transparency, the requirement of a written motivated application represents a novelty of the Law.

[94] At this point, the file is transferred to the Public Prosecutor who may decide to open a judicial investigation.

3.3. Particular comments

After this comparative analysis, some remarks can already be formulated.

Firstly, it is remarkable that both for judicial (ordinary cases or organised crime/terrorism offences) and administrative interceptions, the duration of a warrant is much shorter in Italy than in the other two countries. However there is no limit to the available number of renewals.

Secondly, specific elements of evolution can be underlined for each country. In **France,** judicial interceptions have long been available for both minor and serious offences. Organised crime and terrorism have played a catalysing effect in the introduction of derogatory provisions and in the expansion of powers of actors involved in either the authorisation or the execution process. Primarily introduced for the purpose of preventing and investigating terrorism and organised crime, the scope of these provisions was then extended to cover also other types of crimes of less serious nature.[95]

In **Italy,** over time the use of the judicial interception of telecommunications has expanded both for the ordinary and derogatory regimes (*i.e.* the use of interceptions is possible in a wider number of cases and more easily authorised). This trend is a clear result of the catalysing effect of serious crime as the provisions under analysis are encompassed in legislation focusing on organised crime (*e.g.* Law 152/1991) and terrorism (*e.g.* Law 438/2001). The same trend can be easily identified in relation to the provisions on *ante-delictum* interceptions (*e.g.* art. 5 Law 438/2001 on terrorism, art. 13 Law 203/1991 on organised crime and art. 9 Law 228/2003 on human trafficking).[96]

The regime in the **United Kingdom** is particularly different from the French and Italian one (*e.g.* there is no distinction between judicial and administrative interceptions). However, as in the other two countries, serious crime broadens the possibility of using this technology, leads to the multiplication of actors who can authorise and execute interceptions (*e.g.* SOCA), enlarges the scope and extends the duration in terrorism and organised crime cases.

4. From a preventive purpose to an investigative use: video-surveillance

In relation to video-surveillance, the three regimes analysed are quite similar. Most importantly video-surveillance was at first introduced in the three countries by the private sector and then by public authorities (especially at the local level) for public order, prevention purposes. The question arising over time has been to understand whether and how videos and images so gathered can be use for investigation and prosecution purposes.

In **France,** the legal regime of video-surveillance now called *vidéoprotection* systems is mainly regulated by the *Code de la Sécurité Intérieure*.[97] A section of the Code focuses on

[95] See development of art. 706(73) CPP over time.

[96] In the last years, many scandals concerning illegally obtained interceptions and their subsequent publication by newspapers have revealed how the current regime is too easily subject to abuses. Thus, a reform of the legislative framework has been discussed. Disegno di Legge 1415, "Norme in materia di intercettazioni telefoniche, telematiche e ambientali" (30 giugno 2008). See F. Ruggieri, "Il Disegno di legge governativo sulle intercettazioni: poche note positive e molte perplessità" (2008) 6 Cass pen 2239.

[97] *e.g.* E. Heilmann and P. Melchior, *Vidéo-surveillance ou vidéo-protection ?,* Le choc des idées, Le Muscadier, Paris, 2012; A. Bauer and F. Freynet, *Vidéosurveillance et vidéoprotection*, Que sais-je ? PUF, 2012; A. Bauer and C. Soullez, *Les politiques publiques de sécurité*, Que sais-je? PUF (Paris 2011); F. Ocqueteau, "A comment on video-surveillance in France: regulation and impact on crime" (2001) 25(1/2) *International journal of comparative and applied criminal justice* 103; N.C. Ahl, "La vidéo-surveillance en trompe-l'oeil", Le Monde, (29 October 2011); E. Heilmann, "La vidéo-surveillance, un mirage technologique et politique" *in* L. Mucchielli,

video-protection in general[98] and another section is rather devoted to the fight against terrorism[99]. Since its introduction by Law 73/1995[100], the use of this technology in the public sphere has become particularly important for anti-terrorism purposes as a tool to gather evidence when an offence is actually committed.[101]

In **Italy,** the fight against terrorism has led to a redefinition of priorities, objectives and instruments by national agencies, which significantly stimulated the use of new technologies. This lead to a larger deployment of video-surveillance systems (*videosorveglianza)* for crime and terrorism prevention purposes as a response to citizens' anxiety and need of reassurance.[102]

Video-surveillance is allowed only under certain conditions. In the public sphere, it is governed by specific data protection rules as detailed by art. 34 of the Code for data protection[103] and by the decision of 8 April 2010[104] of the Italian data protection authority.

"For the past 25 years, the **United Kingdom** has experienced an exponential increase in these technologies and is now the world leader in the use of video surveillance". [105] There are few restrictions on the use of cameras in public areas.[106] It is noteworthy that there is no specific statutory provision for video surveillance but only a CCTV code of practice, issued by the Information Commissioner's Office.[107] Such a code encompasses recommendations and not mandatory provisions. General video surveillance with CCTV operations does not need to be authorised under RIPA 2000. However, pre-planned, covert operations to follow known individuals for investigation purposes, which involve the use of CCTV, need authorisation. Members of the public need to be made aware that such systems are in use, and their operation is especially covered by the Data Protection Act 1998 and the CCTV Code of Practice.

La frénésie sécuritaire, La decouverte (Paris, 2008); N. Le Blanc, "Le bel avenir de la vidéosurveillance de voie publique" (2010) 2(62) Mouvements 32; T Le Goff, "Politique de securité: les chiffres et les impages, (2010) 3 Esprit 90; C. Laval, "Surveiller et prevenir" (2012) 2 *revue du MAUSS* 47. See also the reports of CNIL (*commission nationale de l'informatique et des libertés*).

[98] arts. L251(1) to L255(1).

[99] arts. L223(1) to L223(9).

[100] Law 73/1995.

[101] J. Pradel, *Procédure pénale*, 16th ed., Cujas (Paris, 2011) p. 407.

[102] *I sistemi di videosorveglianza 2, Videosorveglianza e privacy: quadro normativo, casistica e aspetti tecnici*, Transcrime, Inforsicurezza (4 May 2006) p.11.

[103] Legislative Decree 196/2003 bearing the adoption of the *Codice in material di protezione dei dati personali*.

[104] Garante per la protezione dei dati personali, Provvedimento in material di videosorveglianza, G.U. 99 (29 April 2010).

[105] EFUS, *Citizens, Cities and video-survellance, Towards a democratic and responsible use of CCTV*, EFUS press (Paris, 2010) p. 14.

[106] On the United Kingdom regime, on CCTV cameras in relation to terrorism prevention see *e.g.* Q.A.M. Eijkman and D. Weggemans, "Visual surveillance and the prevention of terrorism: What about the checks and balances? »; *D. Fenwick*, "Terrorism, CCTV and the Freedom Bill 2011: Achieving compatibility with Article 8 ECHR?" and *B. Sheldon*, "Camera surveillance within the UK: Enhancing public safety or a social threat?" *in* H. Fenwick, *Developments in Counter-Terrorist Measures and Uses of Technology*, Rouledge (2012); D Giannoulopoulos, « La vidéosurveillance au Royaume-Uni. La caméra omniprésente », (2010) 1 Archives de politique criminelle 245.

[107] The Protection of Freedoms Act 2012 specifically requires the Secretary of State to prepare a code of practice containing guidance on the development of surveillance camera systems and the use of processing of images or other information obtained by virtue of such system. It also appoints a person as the Surveillance Camera Commissioner in order to encourage compliance with the surveillance camera code, review its operation and provide advice about the code (including changes to it or breaches of it).

As in relation to interceptions, three elements may be used to highlight similarities and differences of the legal regimes in the three countries: the actors, the scope and the duration of video-surveillance.

4.1. Actors

In terms of **actors**, unlike in Italy, in France and in the United Kingdom, both the installation and the use of video-surveillance is authorised by an administrative authority.

4.1.1. France

In **France,** *vidéoprotection* can be authorised to ensure security when the places and buildings are especially exposed to a risk of assault and theft[108] and only if *vidéoprotection* does record neither the interior of dwellings and private buildings nor their entrances.[109] When the images gathered allow the identification of an individual, their use must comply with provisions of Law 17/1978 on data protection.

This measure is submitted to the authorisation of the *Préfet*, which can be made at any time by *arrêté préfectoral*, after consulting the *Commission départementale*.[110] It prescribes all necessary precautions, especially about the status of the persons in charge of the exploitation of the video-protection system or viewing images.[111] The authorisation is given to certain categories only, identified in relation to a specific case only, namely police agents and *gendarmerie*. It specifies the method of transmission and the duration of conservation of images. The *Commission départementale de vidéoprotection* gives an opinion on the implementation of such a technology, if these cameras are filming public roads or places or establishments open to the public.[112]

Yet, for the purpose of preventing terrorist acts, the representative of the State in the Department and, in Paris, the *Préfet* of police may prescribe the implementation of *vidéoprotection* systems and authorise also a broader category of individuals to view and use images.[113]

In urgent cases and in particular when under exposure to the risk of terrorist acts, the representative of the State in the Department and, in Paris, the *Préfet* of police may issue, without prior notice to the *Commission départementale de vidéoprotection*, provisional authorisation to install a video-protection system. The Chairman of the Commission will be informed of this decision so that the Commission provides its opinion.[114]

In order to best reconcile security needs and the right to privacy, ethics committees have been introduced. An institution, solely established for this purpose, monitors video-protection, in some French cities such as Lyon and Le Havre, with the specific aim of ensuring the respect of freedoms.[115]

For **investigative purposes**, a police officer can have access to the information gathered by video-protection via an ordinary judicial warrant (prosecutor or judge on the basis of specific provisions).

---

[108] art. L 251(2) *CSI* as introduced by Law 267/2011 that explains the purpose of video-protection. DC 2011-625, 10 March 2011.
[109] art. L 251(3) *CSI*.
[110] art. L 252(2) and L 252(3) *CSI*.
[111] art. L 252(1).
[112] art. L 251(4) *CSI*; the *Commission nationale de vidéoprotection* created by Law 2011/267 has a mission of advice and evaluation of the effectiveness of the video-protection at the level of the Ministry of Interior.
[113] art. L 223(2) *CSI*; see also J.-P. Courtois and C. Gautier, *Rapport d'information sur la vidéosurveillance*, Senate, n°131, 10 December 2008.
[114] art. L223-4 and L223-5 CSI.
[115] EFUS, *Citizens, Cities and video surveillance*, pp.141-142.

4.1.2. The United Kingdom

The use of CCTV cameras, in the **United Kingdom,** was motivated by the will to fight against street crime around shopping malls and stadium. Originally managed at the local level, it became a national policy thus engendering a need to coordinate local activities and favour the share of information.[116] CCTV cameras are overt and do not constitute intrusive and directed surveillance[117] (unless they focus on a specific group of people or individual and thus record movement and activities of a private person) and thus do not require an authorisation under Part II of RIPA 2000.

In the case where they are used as law enforcement activities, authorisation must be obtained, setting out what is authorised, how it will be carried out (*e.g.* which cameras are to be used), and what activity is to be caught and held on the tape or disk that results. Authorising officers have to take into account the risk of collateral intrusion into the privacy of persons who are not the subjects of the investigation.

4.1.3. Italy

By contrast, in **Italy,** since Law 38/2009, municipalities may use video-surveillance systems in order to guarantee urban security in public area[118] for public order purposes.

The Municipal Police manages the installation with the help of technicians from a private company and with the advice of the National Police. The National Police, the Municipal Police and the *Carabinieri* control the cameras. When the images are sent to the operator in the National Police Headquarters, they can, on the one hand, view the images from all cameras and, on the other hand, control the cameras remotely. The choice of operators is limited by national legislation to judicial police officers.

In the Municipal Police's video surveillance central operations office, three police officers work relayed shifts to ensure 24 hours coverage. Meanwhile, in the National Police headquarters, a State Police Inspector and two assistants are on hand 24 hours a day.

The images are sent simultaneously to the headquarters of both the national and municipal police forces. The National Police Headquarters can then send the images to the judicial authorities as items of evidence. In total, a dozen operators drawn from the national police, municipal police and *Carabinieri* consult images, which cannot be shared in real time with other services. Only agents of the judicial police can access the saved images, with the authorisation of a judge. To view the images, not only authorisation but also physically the key is needed. However, only the system manager has permission to consult the recordings and must use a specific access key.

4.2. Scope

In all these Member States, the **scope** of the use of video-surveillance technologies is crime prevention.

4.2.1. France

In **France**, *vidéoprotection* is built to record what happen in public area in order primarily to prevent[119] and then to investigate offences, whether serious or not. In fact, this instrument has been recently extended to judicial investigation. The government announced that video-protection is an important component of urban safety policies. If video-protection was developed originally to fight against common offences,[120] the anti-terrorism context

[116] *ibid.*, pp.184-185.
[117] s. 26(2)(a)/1(2)(a) RIPA 2000, defining directed surveillance.
[118] art. 6(7) Law 38/2009.
[119] Law 125/1995 as amended by *Ordonnance* 351/2012.
[120] art.4 Law 73/1995. Priority tasks of the police are for example the fight against urban violence and the

mainly justified further development and multiplication of *vidéoprotection*. As mentioned above, specific provisions exist in the code (an actual separate section) in relation to video-surveillance for the prevention and investigation of terrorism. These derogatory provisions grant more powers and more margin of manoeuvre to the authorising[121] (larger number of circumstances justifying the installation) and executing authorities.

There is no special offence motivating the use of video-protection but the transmission and recording images collected by this system are submitted to various conditions depending on the criminal context; the level of powers granted to authorities depends on the type of offences concerned. Terrorism extends the permitted space of video-protection to the immediate vicinity of buildings and facilities by other legal persons and places likely to be exposed to acts of terrorism.[122] It can be carried out in exceptional circumstances and under strict conditions.

4.2.2. Italy

In **Italy,** video-surveillance have diverse purposes, some of which can be grouped into the following categories: "(1) protection and integrity of individuals – including urban security; public order; public bodies' prevention, detection and/or suppression of offences; streamlining and improving publicly available services also in order to enhance user safety; (2) protection of property; (3) detecting, preventing and controlling breaches of the law; (4) gathering of evidence."[123]

As in the other countries, the use of video-surveillance in urban transports (where it was most importantly installed at the beginning) has rapidly spread because of the terrorist threat.[124] Its purpose remains the prevention of more petty crime but its use is extended to the prevention of and information gathering in relation to more serious offences, including terrorism.[125]

The preventive aspect is less clear. Citizens' satisfaction is nonetheless high, even if the system does not meet all the expectations. A greater surveillance gives citizens a feeling of greater protection, with the possibility of a more rapid response from the police. The displacement effects (relocation of criminal activities) are not quantifiable, due to a lack of reliable statistics. However, a research study claims that the message given to the public opinion was "+ video-surveillance = + prevention of offences = - criminality".[126]

4.2.3. The United Kingdom

In the **United Kingdom,** video-surveillance is used for a number of monitoring and surveillance purposes, but is mainly used for security purposes. The development of CCTV was felt by many to be a major breakthrough in crime prevention. It forms a major part of crime prevention strategy in the United Kingdom and is often used as important evidence in court trials and in the identification of suspects.[127] CCTV may have other deterrence and safety-related benefits, although these are debated. However, its multiplication in the country is considered as an erosion of civil liberties.

---

control of public order.

[121] *e.g.* larger number of circumstances justifying the installation; the *Préfet* may authorise an installation before that the commission has given his advice.

[122] art. L223-1 and art. 223-2 CSI.

[123] Garante per la Protezione dei dati personali , *Video surveillance*, Decision (8 April 2010).

[124] *I sistemi di videosorveglianza 2, Videosorveglianza e privacy: quadro normativo, casistica e aspetti tecnici*, Provincia autonoma di Trento, Transcrime, Inforsicurezza (4 May 2006) p.49

[125] F. Caprioli, "Nuovamente al vaglio della Corte Costituzionale l'uso investigative degli strumenti di ripresa visiva", (2008) 3 Giur Cost 1832.

[126] See *I sistemi di videosorveglianza 2,* p.11.

[127] Unlike the interception of telecommunication, which cannot be used as evidence at trial .

4.3. Duration

With regard to the **duration**, two issues are of importance. On the one side, how long the authorisation given by the authority to deploy the video-surveillance system lasts; and, on the other side, how long the information gathered by the video-surveillance device can be retained for.

4.3.1. Duration of the installation

Concerning the length of deployment, only in France, the installation of video-surveillance devices lasts only to a limited amount of time: 5 years renewable. By contrast, in Italy and the United Kingdom, there is no duration limit to the deployment.

4.3.2. Duration of the retention of information gathered by video-surveillance

On the second issue, the situation of the Member States varies broadly. In all of them, information can be retained until they are no longer necessary. Besides, some jurisdictions provide for specific delays.

4.3.2.1. France

In **France** the authorisation prescribes the duration of retention of images within one month after the transmission or access to them, without prejudice to the necessity of their conservation for the needs of the criminal proceedings.[128] Except in case of investigation of *flagrante delicto*, a preliminary investigation and an *information judiciaire*, the retention of images may not exceed one month.[129] If the conditions of urgency and of exposure of the risk of terrorist acts are present, video-protection is installed for four months[130] and the renewal is possible after a consultation of the *Commission départementale de vidéoprotection*.[131]

4.3.2.2. Italy

In **Italy,** concerning the video-surveillance devices installed by municipalities for public order purposes, the local and national Police can view the encrypted images and keep them for up to seven days until their destruction except if the information is subject to special needs for further storage.[132] However, the duration can be extended in places particularly exposed to terrorist threat up to thirty days.[133] In cases where video-surveillance systems had been installed (*e.g.* by private individuals or companies) for other purposes than public order, data may be retained for a maximum of 24 hours.

4.3.2.3. The United Kingdom

Finally, in the **United Kingdom,** an indication on duration is provided in a non-statutory instrument, *i.e.* a code of practice. The indication is moreover extremely vague. According to the Code of practice, "[y]ou should not keep images for no longer than strictly necessary to meet your own purposes for recording them. On occasion, you may need to retain images for a longer period, where a law enforcement body is investigating a crime, to give them opportunity to view the images as part of an active investigation."[134] An example of

---

[128] art. L252-3 CSI
[129] art. L252-5 CSI
[130] art. L223-4 CSI
[131] art. L223-5 CSI.
[132] art. 6(8), Law 38/2009. In cases where video-surveillance systems had been installed (*e.g.* by private individuals or companies) for other purposes than public order, data may be retained for a maximum of 24 hours.
[133] Garante per la protezione dei dati persnali, *Prescrizioni per la videosorveglianza presso i siti di interesse culturale maggiormente esposti alla minaccia terroristica* (12 March 2009).
[134] CCTV code of practice, Data protection, Information Commissioner's Office (revised ed. 2008) p. 14

duration is given, "images from a town centre system may need to be retained for enough time to allow crimes to come to light, for example, a month. The exact period should be the shortest possible, based on your own experience."[135]

Installation of video-surveillance

	France	Italy	United Kingdom
Ground 1	Security purposes/public order, especially for areas exposed to a risk of assault and theft but also to a risk of terrorism	Security purposes/public order	Security purposes/public order
Authorisation	Representative of the State in the Department and, in Paris, *Préfet* of police after consulting the *Commission départementale*	Municipalities	Chiefs Constable, Chiefs of the Intelligence and Security Services, Director of Government Communication Headquarters, Director General of the National Criminal Intelligence Service
Duration	5 years renewable	no limit	no limit
Ground 2	In case of emergency		
Authorisation	State in the Department and, in Paris, *Préfet* of police without consulting the *Commission départementale* (informed after)		
Duration	4 months renwable after consultation of the *Commission départantale de la vidéoprotection*		

Retention of information gathered by video-surveillance

	France	Italy	United Kingdom
Ground	public order and investigation of crimes	public order and investigation of crimes	Public order and investigation of any offences
Authorisation	police officer, prosecutor and judge	law enforcement authorities	law enforcement authorities
Duration	1 month, without prejudice to the necessity of their conservation for the needs of the criminal proceedings; in flagrante delicto, no more than one month	7 days; if gathered for other purposes than public order, retained for max 24 hours	"no longer than necessary"

The comparative analysis validates the second dimension of the first shift tested in this paper. In the three states under scrutiny, video-surveillance was at first introduced by private

[135] *ibid.*

citizens and companies and then by public authorities (especially at the local level) for public order prevention purposes. The data gathered are now used in the context of the prevention and investigation of serious crimes, including terrorism.

5. Interplay between intelligence services and law enforcement agencies: Mutual contamination

According to a strict principle of separation, traditionally the activities of intelligence services and police authorities in the prevention and investigation of crime were clearly distinct. In fact, there is a profound difference (at least in general terms) in the specific purposes of the two bodies. The police, in its judicial function, have the task of gathering information in relation to a specific offence for prosecution purposes; intelligence services do not have the objective of investigating offences but rather to recognize threats and to provide intelligence assessments to policy makers. In this framework, intelligence information is mostly secret, whereas police information is subject to scrutiny via cross-examination in court. However, nowadays the distinction is not always so clear, intelligence is also given operational tasks and this leads to a problematic coordination and overlap.[136]

The shift towards prevention in the fight against serious crimes, including terrorism, attributes a greater role to ductile means of intelligence to the detriment of more traditional means of investigation. The current trend leads to an intense and dangerous osmosis and blur between criminal justice and secret investigations (significantly much of the activities of the intelligence falls within the realm of State secret[137]). Intelligence activities and police investigations tend to converge as of their object, scope, means, particularly in relation to offences such as terrorism and organised crime where intelligence is crucial to understand at best the organisational dimensions of complex, widely spread and long-lasting phenomena which threaten national security.[138]

In addition, intelligence must only be accountable in front of the executive. Given the new role of intelligence in public order activities and the investigative domain, the issue at stake is hence that of the relationship, yet to be defined, between intelligence and the judiciary.

The second shift the authors are testing in this paper is thus the evolution, potentially leading to a blur, of the share of roles, competences and means of intelligence services and law enforcement authorities. The question to explore is whether, and to what extent, the three countries have established structures of coordination/centralisation between intelligence, police and judiciary in particular in the field of organised crime and terrorism in order to manage the overlap of competences and avoid the blur.

5.1. France

France constitutes, from a law enforcement perspective, a very effective example of coordination between intelligence services, police, prosecutors and *juges d'instruction* via its

[136] The distinction of roles and information sharing between intelligence services and law enforcement authorities with a view of preventing an combating terrorism has been highly discussed and let to controversial case-law also in other UE countries such as the Netherlands. See J.A.E Vervaele, "Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law? » (2005) 1(1) *Utrecht Law Review* 1.

[137] See, re. Italy, R. Orlandi, "Segreto di Stato e limiti alla sua opponibilità fra vecchia e nuova normativa" (2010) 6 Giur cost 5224; A Pace, "L'apposizione del segreto di Stato nei principi costituzionali e nella legge n.124 del 2007, (2008) 5 Giur Cost 4041.

[138] See R. Orlandi, "Attività di intelligence e diritto penale della prevenzione" and F. Sommovigo, "Attività di intelligence e indagine penale" *in* G. Illuminati, *Nuovi Profili*.

centralised investigation and prosecution of terrorist offence and the coordination of organised crime cases in Paris.[139]

Since the first anti-terrorist law in 1986, co-ordination between the various intelligence and police services and the French government has improved with the creation of the *Unité de Co-ordination de la Lutte Anti-Terroriste* and the 14th section of the Parquet of Paris. By contrast, in the field of organised crime, there is no centralisation of prosecutions and trials but only a coordination of investigations.

The new *Direction Centrale du Renseignement Intérieur* (*DCRI*), the French internal intelligence service, is the centralised agency responsible for the preventive and investigative phases. The *DCRI*[140], operational since 1st July 2008, combines law enforcement and intelligence service agents and is meant to monitor, detect and investigate individuals. Thus this service, which can be used by prosecutors and *juge d'instruction* in serious crime investigations, encompasses both police and intelligence agents. Its composition and structure favours the sharing of information both at the prevention and investigation phases between the two services in an effective and rapid manner, leading to the so-called "judiciarisation" of intelligence information.[141]

Such a centralisation offers some advantages as it results in the competent judges and prosecutors being more specialised and in them having more knowledge and expertise in terrorist matters as well as the establishment of closer links with the intelligence services. However, at the same time, it has been considered as a dangerous concentration of very far-reaching powers in the hands of only a few.[142]

Remarkably, no specific rule forbides the use of intelligence (including the information gathered via administrative interceptions) as evidence during criminal proceedings. However, in practice, intelligence services have never used so far the results of administrative interception at trial.[143] Intelligence can always be used as a lead for initiating judicial investigations. Moreover, despite the establishment of central coordination structures, the police sometimes do not trust the intelligence information received because they cannot have access to sources. In the Merah case, the sharing of information between the intelligence services and the police was particularly deficient; Merah was under surveillance by intelligence services but the information was never passed on to the police in order to start an investigation and thus arrest the suspect.[144]

5.2. Italy

A similar overlap and blur of competences between intelligences services and police authorities may be seen in **Italy** in relation to offences which threaten not only individual

---

[139] The French system is currently evolving towards a centralisation of the execution and the consequent use of judicial interception based on the model of the centralised system of administrative interceptions (art. 4 Law 91/73). See *plate-forme nationale des interceptions judiciaires* and *Commission nationale de controle des interceptions de sécurité.*

[140] Gathering of the *Direction de la surveillance du territoire* (DST) and of the *Direction centrale des Renseignements Généraux* (RG).

[141] Interview with P. Caillol, Deputy Director of the *Institut national des hautes études de la sécurité et de la justice* (Paris, 28 November 2012).

[142] L. Caprioli and J.-P. Pochon, "La France et le terrorisme international, Les racines historiques et organisationnelles du savoir policier", round table organised by J. Ferret and A. Wuilleumier, (2004) 55 *Cah. S.I.,* pp. 147-179; FIDH, *Paving the way for arbitrary justice*, (1999) 271(2).

[143] This is probably because the transcription of the interception is only possible for the purpose of article L241-2 CSI (art. L242-5). In addition, the recording is destroyed within ten days (art. L242-6) and the transcription within four months (L 242-3). No article provides for any extension of preservation for judicial purpose. Information from P. Caillol, Deputy Director of the *INHESJ* (22 April 2013).

[144] Interview with T. Fragnoli, Procureur, Parquet anti-terrorisme, Tribunal de Grande Instance (Paris, 29 November 2012).

citizens but also national security. A number of legislative provisions thus increasingly involve intelligence services in public order policies. A good example is that of the Law 155/2005 enabling intelligence services to apply to the prosecutor for an interception warrant where deemed to be necessary to prevent terrorist activities or subversion of the constitutional order *ex* art. 226 *disp. att. CPP*.[145]

Already Law 410/1991 established a general Council for the fight against organised crime, including intelligence service agents with the task of intelligence gathering in relation to any form of subversion by any type of organised group threatening institutions and public life.[146] The intelligence agents had only an obligation to communicate to judicial police forces any information on Mafia organised crime groups.

In addition, the *Agenzia Informativa di Sicurezza Interna* (AISI) – created in 2007 to replace the SISMI – has a specific competence of information gathering in the domain of subversion, terrorism (particularly international terrorism) and organised crime offences. In these domains, a precise distinction of the field of intervention of police and intelligence is particularly complicated.[147]

At the stages of pre-trial and trial, there is no centralisation of powers in the fight against serious offences. However, with a view to favoring effective prosecution of terrorist offences and valid judicial scrutiny of police investigations, a coordination of different cases to share knowledge and information on terrorist networks has certainly been considered fruitful. This has lead to a specialisation of investigating judges, prosecutors and the police. In relation to terrorism cases, during the 1970s and 1980s, informal networks for the prosecutors grew up in order to share information and competences. Judges have often advocated the establishment of coordination between prosecutors who would deal with terrorism offences under the auspices of the National Anti-Terrorism Directorate.[148] In relation to organised crime, judicial and police investigations, as well as preventive actions, are coordinated respectively by the National Anti-Mafia Directorate (DNA) and the Anti-Mafia Investigations Directorate (DIA). The coordination ensures information sharing between judicial authorities and police services among themselves and among each other on all investigations concerning organised crime. The DNA may directly rely upon the DIA in the case of specific investigations. However, the two Directorates do not directly involve members of the intelligence services.

In 2004, a *Comitato di Analisi strategica anti-terrorismo* has been created within the Ministry of Interior to assess any information on international and domestic terrorist threats and thus coordinate any intervention. The agency involves members of police forces, carabineers, guardia di finanza and intelligence services. Law 207/2007 concerning the re-organisation of intelligence services establishes the *Dipartimento delle Informazioni per la Sicurezza* (*DIS*) which also coordinates the exchange of information between intelligence services and police authorities.

For the purpose of improving the cooperation, Law 207/2007 has also introduced art. 118 *bis CPP* so that the Prime Minister may ask to the judiciary information which are relevant to the activities of the intelligence even in derogation to the secrecy of investigations (art. 329 *CPP*). Meanwhile, the judiciary may ask the intelligence services to obtain documents or information relevant to a judicial investigation (art. 256 *bis CPP*).

---

[145] Vervaele, "Special procedural measures and the protection of human rights, General report", *Utrecht L Rev.*
[146] Law 410/1991.
[147] See Law 124/2007, art. 7. More information available at www.sicurezzanazionale.gov.it (accessed 23 May 2013).
[148] G. Melillo and A. Spataro, "Senza la creazione di una Procura nazionale" (2005) 33 Guida Dir 48.

5.3. The United Kingdom

In the **United Kingdom**, the coordination of law enforcement authorities and intelligence services has been achieved through the creation of dedicated coordinating bodies that have provided a central mechanism for disseminating information and availing inter-agency operations.[149]

The lack of trust between police and intelligence and different counter-terrorism agencies have often hampered an effective information sharing.

The most important interface between the intelligence community and the police departments is the National Criminal Intelligence Service (NCIS). Over the past decade, the Security Service has become more involved in judicial investigations by providing evidence at trials involving terrorist and serious criminal offences.

Within police departments, the link with intelligence services (mostly the MI5) is ensured by Special Branches, having counter-espionage, counter-proliferation, and counter-subversive functions. They constitute the primary instrument to translate intelligence information into operational activities, investigations and prosecutions. Thus Special Branches provide national operational support to the Security Service.

Moreover, in June 2003 the United Kingdom has established a fusion centre, the Joint Terrorism Analysis Center (JTAC), comprised of representatives from eleven government departments relating to international terrorism (*e.g.* Home Office, Police, FCO and Ministry of Defence) and meant to produce finished intelligence for a wide variety of audience. Such a fusion centre aims at the inclusion in the intelligence arena of non-traditional players.

The blur of competences between law enforcement authorities and intelligence services in the country has been favoured by a fundamental shift in policing towards a strategic, future-oriented and targeted approach to crime control - broadly represented in the concept of "intelligence led policing" (ILP) - built around analysis and management of problems and risks, rather than reactive responses to individual crimes (a "forward looking" focus on threats to community safety).[150]

6. Concluding remarks

The overview of each Member State's response to serious offences of two surveillance technologies identified previously (interceptions of telecommunication and video-surveillance) allows to understand the specificity of each regulatory framework as well as the most important similarities and differences between national regimes in relation to actors involved, the scope and the duration of the two surveillance technologies chosen as case studies in the prevention and investigation phases.

In general terms, one can argue that there has been an overall toughening, and a parallel higher curtailment of civil liberties, of the provisions concerning the use of surveillance technologies in the prevention and investigation of serious crime. Indeed, both terrorism and organised crime certainly had a catalysing effect on this development.[151]

As underlined in this deliverable, serious crime has certainly played a catalysing effect on the introduction of derogatory provisions and in the expansion of powers of actors

[149] P. Chalk and W. Rosenau, " Confronting the Enemy Within", Security Intelligence, the Police, and Counterterrorism in Four Democracies, RAND (2004).

[150] M. Maguire and T. John, "Intelligence Led Policing, Managerialism and Community Engagement: Competing Priorities and the Role of the National Intelligence Model in the UK" (2006) 16(1) *Policing and society* 67-85.

[151] France developed an anti-terrorist arsenal and centralised its approach as well as increased its use of surveillance technologies (often on the basis of derogatory provisions) such the interception of telecommunications for the purpose of preventing and investigating serious crimes.

involved in either the authorisation or the execution process of the interception of telecommunications. Primarily introduced for the purpose of preventing and investigating terrorism and organised crime, the scope of these provisions was then extended to cover also other types of crimes of less serious nature. In addition, the comparative analysis validates the hypothesis that video-surveillance was, at first, introduced by the private sector and then by public authorities for public order prevention purposes. The data gathered are now used in the context of the prevention and investigation of serious crimes, including terrorism.

Besides, serious crime has had a catalysing effect in redefining the competences of intelligence services and police authorities leading to an overlap of roles and tasks and potentially a blur. With regards to the interception of telecommunications, the blur is less visible in the United Kingdom than in France or Italy. In fact, in the United Kingdom, there has never been a difference between *ante-delictum*/preventive interceptions (allowing for an involvement of intelligence services and not admissible as evidence at trial) and judicial interceptions (prerogative of the police conducted under judicial scrutiny). The increasing involvement of intelligence services in any kind of interception is thus less remarkable!

However, the blur of competences between law enforcement and intelligence services had the positive consequence of stimulating an increased coordination and sharing of information between the two bodies and the creation of infrastructure to institutionalise this relationship, which enhances the effectiveness and the rapidity of the investigation. There is not yet a well-defined share of competences and a new balance and the three countries are still in a situation of blur and uncertainty. This blur is once again less noticeable in the United Kingdom where the distinction between the phase of prevention and investigation is less important than in the other two countries where the "charge" plays a more important role.

After having examined the use of surveillance technologies for preventive and investigative purposes, it would be interesting to focus on the next phase of criminal procedure, *i.e.* the retention and use of information gathered via surveillance technologies for the prosecution and trial of serious crimes, including terrorism.[152] A huge amount of information is nowadays retained by private companies such as networks and service providers, but also by different CCTV operators. The question is under which circumstances such information can be accessed and used by different actors of criminal procedures (police officers, intelligence services, prosecutors and judges) for the purposes of investigating and prosecuting serious crimes. The question is whether serious crime had a catalysing effect on the increasing use of data retained by telecommunication companies and Internet service providers by law enforcement officials not for preventive but for judicial investigation purposes; and whether data retained were originally only related to serious crime and then expanded to less serious ones.

The retention of data for investigation and prosecution purposes raises the question of the collaboration between public authorities and private companies and what kind of obligations one may impose upon them. An additional question relates to the role of information gathered by intelligence services within the criminal proceedings in the investigation, prosecution and trial of serious crimes, including terrorism.

[152] See "Comparative paper on data retention regulation in a sample of EU Member States", SURVEILLE Project, *op. cit.*