

How private is your privacy?

About the constitutionality of “special investigation techniques”

Toon Moonen, Ph.D. researcher Universiteit Hasselt

Working document (5 November 2009) – content

- I. Searching for a balance of interests

- II. Council of Europe framework about special investigation techniques
 - A. Committee of Ministers
 - B. Parliamentary Assembly
 - C. European Court of Human Rights

- III. European legal principles about special investigation techniques and fundamental rights
 - A. The existence of an interference
 - B. Measure in accordance with the law
 - 1. Foreseeability
 - 2. Safeguards against abuse
 - 3. Control of surveillance
 - a. Control actors
 - b. A priori and ad hoc control
 - c. A posteriori control
 - 4. Measure necessary in a democratic society

IV. Special investigation techniques interfering with the right to privacy

A. General principles in Belgium

1. Police and prosecuting authorities
2. Security of the State
 - a. Less invasive (special) investigation techniques
 - b. Very invasive (exceptional) investigation techniques

B. Systematic observations and discrete visual checks

C. The interception and opening of mail correspondence

D. Identification, tracking and tapping of telecommunication

1. The Belgian framework
2. The European framework
 - a. Tap authorization
 - b. Tap control

E. Access to and the keeping of data

1. Access to banking and other information
2. The keeping of information in data banks
 - a. The existence of an interference
 - b. Justifiability of an interference

V. Special investigation techniques interfering with the right to a fair trial

A. The inaccessibility of a confidential record

1. Jurisprudence of the Belgian Constitutional Court
2. Jurisprudence of the European Court of Human Rights

B. Infiltration and incitement

1. Jurisprudence of the Belgian Constitutional Court
2. Jurisprudence of the European Court of Human Rights

I. Searching for a balance of interests

The search for a balance between the duty of the government to safeguard its citizens and the individual rights of those protected is a constant struggle. Although the problem seems pre-eminently a matter of the 21st century, in 1759, a time when nation-states were under full construction, Benjamin Franklin already wrote an essential and well-known wisdom on the cover of a book:

“Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety.”¹

The fact that issues of this kind have a long history, is a reason why a Belgian and more broadly a European perspective might be of particular interest. The Belgian Constitution, adopted in 1831, was the most liberal of its time. It was directly inspired by the French and American Declarations of Rights. The text contained civil liberties that were revolutionary at the time, including the right of free association, the inviolability of one’s home and an impressive, nearly absolute freedom of speech and press. Moreover, and highly relevant in relation to national security measures, the Belgian Constitution reflects strong skepticism towards executive powers:

“The center of constitutional history moved back to Europe with the Belgian constitution of 1831. It was, and still is, one of the most important constitutions in history. Throughout of the nineteenth century, it was the principal European constitutional model. (...) The prevailing constitutional ideology of the Belgian document upheld principles such as a limited monarch, a supreme legislative branch, extensive protection of civil liberties, and separation of church and state. Subtly, the Belgian constitution reflects suspicion of the king and the executive branch. This was the most appealing feature of the constitution for the forces of republicanism throughout Europe.”²

Today, it is one of the oldest constitutions in the world. Some liberties are reviewed by the Constitutional Court with a scrutiny even more rigorous than required by the European Convention on Human Rights. In that climate, one can imagine that any restrictive national security policy adopted by the government will unleash a vigorous debate. In this contribution we will examine the constitutional consequences of the application of certain special investigation methods in order to obtain information relevant to combat serious criminality, including terrorism, or to protect the State from being harmed. While States have an obligation to protect its citizens and can engage in actions to maintain itself,

¹ JACKSON, R. (ed.), *An historical review of the constitution and government of Pennsylvania*, London, Ralph Griffiths Publishing, 1759, 444 p.

² BLAUSTEIN, P., *Constitutions of the world*, Littletown, Rothman, 1993, at 33-35; see also e.g. BILLIAS, G. (ed.), *American constitutionalism abroad: selected essays in comparative constitutional history*, New York, Greenwood Press, 1990, at 27; DOWE, D., LANGEWIESCHE, D., HIGGINS, D. and SPERBER, J., *Europe in 1848. Revolution and reform*, Oxford, Berghahn Books, 2001, at 273; BOCKEN, H. and DE BONDT, W., *Introduction to Belgian law*, New York, Kluwer Law International, 2001, at 51.

question remains how far they can go while doing so. The acquisition of information is usually an early and important step. It is also a permanent State activity.

With the Act of 6 January 2003, a series of special investigation techniques were introduced into the Belgian Code of Criminal Procedure.³ These concerned the interception, confiscation and opening of mail correspondence (sec. 46*ter* and 88*sexies* CCP), the possibility for the public prosecution to inquire into bank accounts and transactions (sec. 46*quater* CCP), the observation, infiltration and the employment of informants (called special investigation techniques *sensu stricto*, sec. 47*ter* §1 and sec. 47*sexies* to 47*decies* CCP). There was also a section dedicated to incitement (sec. 47*quater* CCP). A number of these techniques existed already before in police practice, but did not have a solid legal basis. Obviously, these techniques imply a significant interference with a number of fundamental rights, such as the right to privacy, the principle of equality and non-discrimination, and the right to a fair trial. In what follows, we will examine if, and if so to what extent, these techniques have been found in violation of the Constitution and if they have been modified because of that unconstitutionality. In landmark judgments of December 2004 and July 2007, the Belgian Constitutional Court admitted that governments may be forced to engage in techniques that cause severe intrusions of the liberties of individuals – then it struck nevertheless important parts of the abovementioned Act.⁴

The mentioned regulations apply to the regular criminal investigation authorities, meaning the police, the public prosecution, and the judiciary. They do not apply to the Belgian intelligence services, whose pursuits equally imply the search for relevant information. However, the techniques the civilian secret service can engage in are not included in the 2003 Act. What about the methods of those services that are designed to protect the national security of the State? Next to the General Service information and security of the Military forces, which is the military intelligence service and will not be discussed here, there is the Security of the State, which is the Belgian civilian intelligence service. Although both judicial and intelligence officers engage in gathering information, it is not a direct assignment of the Security of the State to maintain public order or to protect the citizens – its job is, in general, to protect the nation and democracy (sec. 2 of the Act of 30 November 1998 concerning the regulation of the intelligence and security service). In practice however, the information required for both activities is often the same, as combating crime on one hand and the protection of the interests of the State can easily go together. The question remains if these activities meet the fundamental rights standards provided by the Constitution and international human rights law.

³ *Official Journal* 12 May 2003.

⁴ Constitutional Court 21 December 2004, n° 202/2004 and 19 July 2007, n° 105/2007; all decisions are available at www.constitutionalcourt.be.

As the Commission for democracy through law (also known as the Venice Commission), which is the Council of Europe's advisory body on constitutional matters, already noted, there seem to be two schools of thought on the question of how security services should be organized. In some European countries, the security services are independent organizations which are not part of the ordinary police force, whereas in other European States the security services are one of many specialized branches of the general police force: *"From a constitutional point of view, there do not seem to be convincing arguments to give preference to one of these systems over the other."*⁵ As a consequence, it is not always possible to treat the police forces and intelligence services separately. The position within the government of organs with special investigation capacities depends of the constitutional and legal framework of the State. The Venice Commission observed that in some European countries the role of internal security services is limited to the gathering of intelligence and to the subsequent analysis and interpretation of the material. Any preventive or enforcement functions lie then with the ordinary police or other organs. In other countries, internal security organs may have preventive and enforcement functions as well, especially with regard to actions directed against the security of the State. Particularly in the countries where the security services are part of the ordinary police, the security service police officers are allowed to perform the same acts as other police officers, like for example tapping telephones.⁶

Unfortunately, until now the Belgian legislation concerning the actions of the Security of State is defective. The legal basis required by the Constitution and the European Court of Human Rights to engage in techniques such as mail interception, tapping or identifying telephone calls, or systematic observation, is absent or insufficient, although they may look self-evident for intelligence services. Since many years members of Parliament have emphasized that the existing legal framework is insufficient to effectively combat terrorism, extremism, among which radicalism and other serious threats for the internal and external security of the State:

*"Only by attributing adequate means the intelligence and security services can follow up the development of a threat for the fundamental interests of the State, including the protection of individual rights and freedoms at an early stage, in order to facilitate, whenever necessary, an appropriate action."*⁷

Following the 2003 Act regarding the methodology of the regular investigation authorities, there are currently propositions to rearrange the competences of the Security of the State, in order to be adapted

⁵ Council of Europe, Commission for democracy through law (Venice commission), Report "Internal security services in Europe", adopted 7 March 1998, 5.

⁶ Council of Europe, Commission for democracy through law (Venice commission), Report "Internal security services in Europe", adopted 7 March 1998, 9.

⁷ *Parl.Doc.* Senate 2008-09, n° 4-1053/1, 4-5.

to the challenges of the 21st century. In the Senate, a bill was passed in July 2009. It is currently discussed in the House of Representatives.⁸

Faced with global problems and an increasing number of international instruments, comparative constitutionalism is an inevitability. Evidently, we can only truly understand changes and developments if we take into account larger, regional contexts. Taking the Belgian situation as a starting point, we will quickly jump to the supranational, European level. The continent has a long and outstanding history of human rights protection through the application of the 1950 European Convention on Human Rights (ECHR), which has gradually assumed the role of a pan-European Bill of Rights. Hence, we will dedicate most attention to recent positions adopted by the Council of Europe and its jurisdictional body, the European Court of Human Rights (ECtHR) with regard to certain prosecution or intelligence facilities.

Question is whether the 2003 Act and the renewal of the 1998 Act will pass the test of the Constitution and the ECHR. Many of the techniques to acquire intelligence have a strained relation with privacy or due process provisions. In this contribution, the special information gathering techniques the government can or cannot engage in when national security is at stake are discussed. They are examined primarily from a privacy point of view. Because of that, other potential human rights issues, like due process interferences, will only be referred to if the existence of the problem is an integrating part of an investigation technique (like an inaccessible record of a surveillance measure), not if they are the mere consequence of a bad application of the surveillance (like unauthorized phone tapping). What will not be discussed either, are techniques that limit fundamental rights during trial only (like anonymous testimony), the application of privacy invasive measures outside the scope of national security or criminal proceedings (like a public employer controlling email or telephone traffic of its employees), or generally accepted investigation techniques and their conditions (like identification checks on the street). These have been left out, although they are, of course, all closely connected. Either way, central in the discussion there is the delimitation of two fundamental rights of the first generation: the right to privacy, concealed generally in section 22 of the Constitution and article 8 of the ECHR; and to a somewhat smaller extent the right to a fair trial, guaranteed by a whole array of constitutional dispositions and article 6 of the ECHR.

II. Council of Europe framework about special investigation techniques

⁸ *Parl.Doc.* Senate 2008-09, n° 4-1053; *Parl.Doc.* House 2008-09, n° 2128/001.

A. Committee of Ministers

In 2005, the Council of Europe, through the Committee of Ministers, made a recommendation to the member states on special investigation techniques in relation to serious crimes, including acts of terrorism. The Committee is mindful of the obligation on member states to maintain a fair balance between ensuring public safety through law enforcement measures and securing the rights of individuals, as enshrined in the provisions of the ECHR and the case-law of the European Court of Human Rights in particular. It observed that special investigation techniques are numerous, varied and constantly evolving and that their common characteristics are their secret nature and the fact that their application could interfere with fundamental rights and freedoms. Nevertheless, the use of special investigation techniques is considered a vital tool for the fight against the most serious forms of crime, including acts of terrorism. The Committee equally pointed out that the use of special investigation techniques in criminal investigations requires confidentiality and that any efforts to pursue the commission of serious crime, including acts of terrorism, should where appropriate be thwarted with secured covert means of operation.⁹

Evidently, it is important to define the notion “special investigation technique”. However, there does not seem to be a generally accepted legal definition. In any case, certain elements are identifiable: all techniques usually called to be special involve some kind of secrecy or deception. In practice, a measure is secret when the investigating authorities try to hide what they do from the subject of the technique. If the subject knew about the technique being applied to him, he would change his plans: if a criminal knows his telephone is tapped by the police, one can reasonably assume that he will not plan further crimes by phone. As the Venice Commission noted, internal security organizations, or the police in general, are in many cases free from outside administrative interference. Freedom from outside supervision may keep the activities in question rather effectively free from surveillance by the media, the general public, or interested – or affected – individuals:

“Secrecy may, indeed, to a certain extent be necessary for the success of security operations. It may, however, also harm important general or individual interests, which makes the regulation of these questions a delicate matter.”¹⁰

Deceptive investigative techniques on the other hand are not applied in hidden conditions, but make the subject believe something to be true which in reality is not. They do not just conceal information;

⁹ Council of Europe, Committee of Ministers, Recommendation Rec(2005)10 to member states on “special investigation techniques” in relation to serious crimes including acts of terrorism, adopted on 20 April 2005, preamble, available at www.coe.int.

¹⁰ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 10.

these techniques add wrong information to the case: the core of the technique is that the authorities believe that this intentionally provoked misunderstanding will facilitate prosecution or the gathering of further information. If a police officer infiltrates a criminal organization by pretending to be a criminal, he might get access to interesting information.

In the Council of Europe recommendation, special investigation techniques are defined as techniques applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target persons.¹¹ Three general principles are formulated: member states should, in accordance with the requirements of the European Convention on Human Rights, define in their national legislation the circumstances in which, and the conditions under which, the competent authorities are empowered to resort to the use of special investigation techniques. Furthermore, they should take appropriate legislative measures to allow the use of special investigation techniques with a view to making them available to their competent authorities, to the extent that this is necessary in a democratic society and is considered appropriate for efficient criminal investigation and prosecution. Finally, member states should take appropriate legislative measures to ensure adequate control of the implementation of special investigation techniques by judicial authorities or other independent bodies through prior authorization, supervision during the investigation or ex post facto review.¹²

The Committee equally proposed a number of conditions of use, many of which, as will be shown below, are part of the review process by the ECtHR. The Committee noted, in particular, that special investigation techniques should only be used where there is sufficient reason to believe that a serious crime has been committed or prepared, or is being prepared, by one or more particular persons or an as-yet-unidentified individual or group of individuals. Proportionality between the effects of the use of special investigation techniques and the objective that has been identified should be ensured. In this respect, when deciding on their use, an evaluation in the light of the seriousness of the offence and taking account of the intrusive nature of the specific special investigation technique used should be made. Furthermore, member states should ensure that competent authorities apply less intrusive methods than special investigation techniques if such methods enable the offence to be detected, prevented or prosecuted with adequate effectiveness. That adds a subsidiarity condition. They should, in principle, also take appropriate legislative measures to permit the production of evidence gained

¹¹ We will use the notion equally for the context of measures taken by intelligence services.

¹² Council of Europe, Committee of Ministers, Recommendation Rec(2005)10 to member states on “special investigation techniques” in relation to serious crimes including acts of terrorism, adopted on 20 April 2005, appendix, available at www.coe.int.

from the use of special investigation techniques before courts. Procedural rules governing the production and admissibility of such evidence shall safeguard the rights of the accused to a fair trial.¹³

B. Parliamentary Assembly

In 1998, the Venice Commission made a report on the constitutional relations between internal security services and other organs of the State at the request of the Parliamentary Assembly of the Council of Europe (PACE). It found that

“Undoubtedly a variety of internal and external situations may arise in which the executive organ of the State must act quickly and decisively to protect the fundamental interests of the State and society. There must be a consensus that only this need may possibly justify the derogation from normal human rights standards which may sometimes be necessary to ensure the proper and effective functioning of National Security Services. It is this derogation that provokes the need for particular attention to be given to the manner in which these services must be set up, the regulation and control of their activities and their proper place within the constitutional framework of the country.”¹⁴

Furthermore, the Venice Commission noted that it is not disputed that internal security services have inbred in them a potential for the abuse of State power – there have been innumerable incidences of the most serious violations of human rights being committed in the name of internal security:

“Hence the need for the constitutional order to identify what should be the role of internal security services within a democratic society, what should be their place within the constitutional framework, their functions and limitations and what method of control should be exercised over their activities.”¹⁵

According to the Commission, the aim of such services should also be to provide protection from possible espionage, terrorism and sabotage from foreign powers, to investigate actions which aim at undermining democracy and to undertake the secret surveillance of subversive elements operating within a country’s jurisdiction.¹⁶

In 2005, the Parliamentary Assembly observed that in previous years, as a result of the rise in terrorism and crime, European societies have felt an increasing need for security. According to the PACE, some of today’s security threats, such as international organized crime, international terrorism and arms proliferation, increasingly affect both internal and external security and therefore require

¹³ Council of Europe, Committee of Ministers, Recommendation Rec(2005)10 to member states on “special investigation techniques” in relation to serious crimes including acts of terrorism, adopted on 20 April 2005, appendix, available at www.coe.int.

¹⁴ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 20.

¹⁵ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 4.

¹⁶ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 20.

responses by the services of the security sector, preferably co-ordinated and overseen at European level. Accordingly, it was considered essential to strike the right balance between our concept of freedom and our need for security. The PACE raised the question of the extent to which guarantees of security in a society may entail restrictions on fundamental freedoms. The Council of Europe expressed concern about certain practices that have been adopted, particularly in the fight against terrorism, such as the indefinite imprisonment of foreign nationals on no precise charge and without access to an independent tribunal, degrading treatment during interrogations, the interception of private communications without subsequently informing those concerned, extradition to countries likely to apply the death penalty or the use of torture, and detention and assaults on the grounds of political or religious activism, which it deemed contrary to several European legal instruments.¹⁷

With regard to the security sector, the Council of Europe adopted a number of general principles. The functioning of intelligence services must be based on clear and appropriate legislation supervised by the courts. Each parliament should have an appropriately functioning specialized committee. Conditions for the use of exceptional measures by these services must be laid down by the law in precise limits of time. Under no circumstances should the intelligence services be politicized as they must be able to report to policy makers in an objective, impartial and professional manner. Any restrictions imposed on the civil and political rights of security personnel must be prescribed by the law. The delicate balance between confidentiality and accountability can be managed to a certain extent through the principle of deferred transparency, that is, by declassifying confidential material after a period of time prescribed by law. Lastly, parliament must be kept regularly informed about changes which could affect the general intelligence policy.

With regard to the police forces, the Council noted that in each State a specific legal framework for the functioning and supervision of a democratic police force must be set up. Given their different mandate and competences, it was considered important that legislation distinguishes between security and intelligence services on the one hand, and law enforcement agencies on the other. Police officers must be given training covering humanitarian principles, constitutional safeguards and standards deriving from codes of ethics laid down by international organizations such as the United Nations, the Council of Europe and the Organization for Security and Co-operation in Europe (OSCE). The Council of Europe stated that it is essential that this sector, which traditionally lacks transparency, be overseen by democratic institutions and subject to democratic procedures. Exceptional measures in any field must be supervised by parliaments and must not seriously hamper the exercise of fundamental constitutional rights.

¹⁷ Council of Europe, Parliamentary Assembly, Recommendation 1713(2005) on “Democratic oversight of the security sector in member states”, adopted on 23 June 2005, available at www.coe.int.

C. European Court of Human Rights

In general, the European Court of Human Rights, as the international safeguard for the application of the ECHR, interprets the three conditions prescribed by the Convention to limit a citizen's privacy rights (and any other fundamental right): the limitation has to be prescribed by law, it has to serve a legitimate goal, and it has to be necessary in a democratic society. To apply that last condition, the Court takes into account, among others, the existence of a "pressing social need", proportionality and subsidiarity arguments, with reference to the traditions and standards existing on the whole of the European continent. These jurisdictional will form the core of the discussion below.

III. European legal principles about special investigation techniques and fundamental rights

The Belgian Constitution provides in section 22:

"Everyone has the right to the respect of his private and family life, except in the cases and conditions determined by the law."

Any interference with an individual's right to privacy (and those rights connected, like the inviolability of the residence, guaranteed by section 15, and the inviolability of mail, in section 29) has to be prescribed by law and be limited to what is necessary to meet the objectives the legislature envisaged. If not, the infringement is considered unconstitutional.

As the Venice Commission observed, constitutional norms bearing specifically on the internal security services (and the techniques they apply) are rare. In fact, the existence of such specific constitutional norms is not necessary. What is essential, is that legislation or regulations pertaining to internal security organs be in harmony with the Constitution:

"In theory, of course, if the existence of internal security services is entrenched in constitutional provisions, built-in constitutional guarantees would increase the protection afforded to interests which are potentially threatened by the actions of internal security services. On the other hand, however, provision in the Constitution might lend undue constitutional legitimacy or status to such an institution."¹⁸

¹⁸ Council of Europe, Commission for democracy through law (Venice commission), Report "Internal security services in Europe", adopted 7 March 1998, 6.

The European Convention on Human Rights states in article 8 that

“Everyone has the right to respect for his private and family law, his home and his correspondence.”

Any interference by a public authority with the exercise of this right is prohibited,

“except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

In the words of the European Court of Human Rights,

“the cardinal issue arising under Article 8 (...) is whether the interference so found is justified by the terms of paragraph 2 of the Article. This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.”¹⁹

A. The existence of an interference

In general, the Court interprets the notion “interference” in the context of privacy rather widely. It considered that an individual can lodge an application with the Convention organs, concerning secret surveillance measures, without being able to point to any concrete measure specifically affecting him.

The Court held that

“if this were not so, the efficiency of the Convention’s enforcement machinery would be materially weakened. The procedural provisions of the Convention must, in view of the fact that the Convention and its institutions were set up to protect the individual, be applied in a manner which serves to make the system of individual applications efficacious. The Court therefore accepts that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him.”²⁰

The Court found it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be removed by the simple fact that the person concerned is kept unaware of its violation. Thus, the existence of legislation allowing secret surveillance amounts in itself to an interference with article 8.²¹ Concrete examples of interferences will be discussed below.

¹⁹ ECtHR, *Klass v. Germany*, 1978, § 42; all decisions are available at www.echr.coe.int.

²⁰ See ECtHR, *Klass v. Germany*, 1978, § 34-35; see also e.g. ECtHR, *Liberty v. United Kingdom*, 2008, § 56; ECtHR, *Iordachi v. Moldova*, 2009, § 30.

²¹ See e.g. ECtHR, *Association for European Integration and Human Rights and Ekimdzhev v. Bulgaria*, 2008, § 69.

B. Measure in accordance with the law

1. Foreseeability

The fulfillment of the first condition may seem somewhat simple. The ECtHR however is rather exigent. Settled case-law explains that the expression “in accordance with the law” not only requires that the impugned measure should have some basis in (substantive) domestic law, but that it also refers to the quality of the law in question, requiring that it should be compatible with the rule of law, accessible to the person concerned and foreseeable as to its effects. In the jurisprudence of the Court, foreseeable means that a rule is formulated with sufficient precision to enable any individual, if need be with appropriate advice, to regulate his conduct. The phrase implies – and this follows from the object and purpose of Article 8 – in addition that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities. Especially where a power of the executive is exercised in secret, noted the Court, the risks of arbitrariness are evident. Obviously, in the context of secret surveillance measures, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely, for example, to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures.²²

2. Safeguards against abuse

In addition, there have to exist adequate and effective safeguards against abuse. The Court pointed out that anything less would be unacceptable: a system of secret surveillance designed to protect national security entails the risk of undermining or even destroying democracy on the ground of defending it.²³

In the *Klass* case of 1978, which was the earliest landmark judgment, the Court noted that it

“must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the

²² The foreseeability condition is systematically reiterated by the Court in all of the cases discussed below: ECtHR, *Klass v. Germany*, 1978, § 49; ECtHR, *Malone v. United Kingdom*, 1984, § 66-67; ECtHR, *Leander v. Sweden*, 1987, § 50-51; ECtHR, *Huvig v. France*, 1990, § 29; ECtHR, *Kruslin v. France*, 1990, § 30; ECtHR, *Kopp v. Switzerland*, 1998, § 64; ECtHR, *Valenzuela Contreras v. Spain*, 1998, § 46; ECtHR, *Amann v. Switzerland*, 2000, § 50-56; ECtHR, *Khan v. United Kingdom*, 2000, § 26; ECtHR, *Rotaru v. Romania*, 2000, § 52-55; ECtHR, *Doerga v. Netherlands*, 2004, § 45; ECtHR, *Antunes Rocha v. Portugal*, 2005, § 66-67; ECtHR, *Van der Velden v. Netherlands*, 2006; ECtHR, *Weber and Saravia v. Germany*, 2006, § 93; ECtHR, *Dumitru Popescu v. Romania*, 2007, § 61; ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 2008, § 75-77; ECtHR, *Liberty v. United Kingdom*, 2008, § 59-62; ECtHR, *S. and Marper v. United Kingdom*, 2008, § 95; ECtHR, *Bykov v. Russia*, 2009, § 76; ECtHR, *Iordachi v. Moldova*, 2009, § 37-39.

²³ ECtHR, *Klass v. Germany*, 1978, § 49.

circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law.”²⁴

The Court then found a number of legal limitations to be in accordance with article 8 ECHR. The German legislation was adopted in a reaction to terrorist activities by the *Rote Armee Fraktion*, a left extremist group which had committed a number of attacks in the 1970s that heavily shocked the country. In the German legislation at stake, privacy restricting measures were confined to cases in which there were factual indications for suspecting a person of planning, committing or having committed certain serious criminal acts. The application of the measures was limited by a subsidiarity clause, and even then the surveillance could cover only the specific suspect or his presumed contact-persons. Consequently, so-called exploratory or general surveillance was not permitted by the contested legislation. Under the same legislation, surveillance could be ordered only on written application giving reasons, and such an application could be made only by the head, or his substitute, of certain services. The decision thereon had to be taken by a member of the government. Accordingly, there existed an administrative procedure designed to ensure that measures were not ordered haphazardly, irregularly or without due and proper consideration.²⁵

The contested legislation in *Klass* also laid down strict conditions with regard to the implementation of the surveillance measures and to the processing of the information obtained. The measures in question remained in force for a maximum of three months and could be renewed only on fresh application. The Court observed that they had to be immediately discontinued once the required conditions had ceased to exist or the measures themselves were no longer necessary. Any knowledge and documents thereby obtained could not be used for other ends, and documents had to be destroyed as soon as they were no longer needed to achieve the required purpose. As regards the implementation of the measures, an initial control was carried out by an official qualified for judicial office. Under the German legislation, while recourse to the courts in respect of the ordering and implementation of measures of surveillance was excluded, subsequent control or review was provided instead by two bodies appointed by the people’s elected representatives. The competent member of government had to, at least once every six months, report on the application of the legislation to a parliamentary board. Its members were appointed in proportion to the parliamentary groupings, including the opposition. In addition, the government was bound to provide the supervisory commission with a monthly account of the ordered measures. The latter decided, ex officio or on application by a person believing himself to be under surveillance, on both the legality of and the necessity for the measures in question. If it declared any measures to be illegal or unnecessary, the government had to terminate them immediately. The commission members were appointed for the current term of parliament by the

²⁴ ECtHR, *Klass v. Germany*, 1978, § 50.

²⁵ See ECtHR, *Klass v. Germany*, 1978, § 51-53.

abovementioned parliamentary board. They were completely independent in the exercise of their functions and could not be subject to instructions. Having made these observations, the Court considered the whole of these measures to be an adequate protection system.²⁶ In other cases, less detailed legislative frameworks were found obscure and open to differing interpretations, and therefore the techniques engaged in were not in accordance with the law.²⁷

In an early period starting at the end of the 1970s, the Court outlined a number of general principles regarding State responsibility caused by secret surveillance measures. As this jurisprudence evolved, it can be noted that the Court is less easily convinced that national law concerning the keeping of citizen records meets the legality check. In more recent cases, the Court has grown more exigent on the quality of the law, emphasizing on its effectiveness in practice, rather than on its theoretical merits. For example, the Court considered in the 2000 *Rotaru* case against Romania in reference to the keeping of data on citizens that although information may be gathered, recorded and archived, the kind of information gathered has to be defined, as have to be the categories of people that may be subjected to it, the circumstances in which it can happen and the procedure that needs to be followed. The age of the information held or the length of time for which it may be kept should be detailed. Provisions are needed detailing the persons that are authorized to consult the files, the nature of the files, the procedure to be followed or the use that may be made of the information obtained. Equally, the ground allowing interferences with fundamental rights necessary to prevent and counteract threats to national security has to be laid down with sufficient precision.²⁸ The existing framework, which was a shadowy inheritance of the *Ceausescu* dictatorship, was largely incomplete.

Overall, the Court has developed in its case-law on secret measures of surveillance (mostly on telephone taps) a set of minimum safeguards that should be introduced in statute law in order to avoid abuses of power. Among them should be the nature of the offences which may give rise to an surveillance order, a definition of the categories of people liable to be subjected to any such measure, a limit on its duration, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which recordings may or must be erased or tapes destroyed.²⁹ The body issuing authorizations should be independent and there must be either a form of judicial control, or control by an independent body over the issuing body's activity.³⁰

²⁶ See ECtHR, *Klass v. Germany*, 1978, § 51-53.

²⁷ See e.g. ECtHR, *Malone v. United Kingdom*, 1984, § 69-70.

²⁸ See ECtHR, *Rotaru v. Romania*, 2000, § 58.

²⁹ ECtHR, *Huvig v. France*, 1990, § 34; ECtHR, *Kruslin v. France*, 1990, § 35; ECtHR, *Weber and Saravia v. Germany*, 2006, § 95; See also ECtHR, *Iordachi v. Moldova*, 2009, § 39.

³⁰ ECtHR, *Dumitru Popescu v. Romania*, 2007, § 70-73; see also ECtHR, *Valenzuela Contreras v. Spain*, 1998, § 46; ECtHR, *Weber and Saravia v. Germany*, 2006, § 95; ECtHR, *Association for European Integration and*

With regard to who should design the legal framework, the ECtHR noted that

“Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.”³¹

The Venice Commission concluded the same:

“The regulation of internal security services can only be made effective by having specific legislation. If the position is regulated by administrative practice, however well adhered to, it will never provide the guarantees required by law. Being an administrative practice, it can be changed at any time and thereby clarity as to the scope or the manner in which the discretion of the authorities is exercised would undoubtedly be lacking.”³²

The notion “law” of article 8 ECHR is interpreted by the Court in a substantive way, which means that other sources of law, such as executive orders may be used, including even unwritten law. The Belgian Constitution, in its section 22, is less permissive; only parliament can create and organize infringements on the citizens’ privacy.

In short, the enactment of specific legislation would give citizens an adequate indication of the instances and conditions in which such surveillance is admissible. It should also provide for an indication of the scope of any executive discretion and the manner of its exercise so as to afford protection against arbitrary interference.³³

3. Control of surveillance

The Venice Commission concluded concerning that legislative control over the actions of intelligence services remains an essential means of ensuring that they operate exclusively in the national interest for the realization of democracy and the rule of law. Thus, legal instruments should be provided

Human Rights and Ekimdzhiev v. Bulgaria, 2008, § 76; ECtHR, *Liberty v. United Kingdom*, 2008, § 62; ECtHR, *Iordachi v. Moldova*, 2009, § 30.

³¹ ECtHR, *Malone v. United Kingdom*, 1984, § 68; the Court pointed out the same for delegation to the judiciary. See ECtHR, *Leander v. Sweden*, 1987, § 51; ECtHR, *Huvig v. France*, 1990, § 29; ECtHR, *Kruslin v. France*, 1990, § 30; ECtHR, *Amann v. Switzerland*, 2000, § 56; ECtHR, *Rotaru v. Romania*, 2000, § 55; ECtHR, *Weber and Saravia v. Germany*, 2006, § 94; ECtHR, *Liberty v. United Kingdom*, 2008, § 62; ECtHR, *Bykov v. Russia*, 2009, § 78; ECtHR, *Iordachi v. Moldova*, 2009, § 39.

³² Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 20.

³³ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 20.

ensuring adequate checks and balances that allow these services to operate efficiently, but without overstepping their role, particularly where fundamental rights are concerned.³⁴

a. Control actors

Who should perform this supervision? The European Court considers in general that

“in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.”³⁵

The Venice Commission equally promotes judicial control. The rights of individuals cannot be adequately protected if the acts of such institutions are not made susceptible to judicial review. It concluded that

“whereas it would be unrealistic to require their activities – if they are to be effective – to be fully transparent at all times, it is, however, expected that internal security services be accountable for their acts and activities within the legal framework in which they operate. To that extent they must be transparent in the sense that their actions should be verifiable and subject to control to establish whether they had correctly exercised their functions and powers *intra vires*. This control must be a judicial one either by an *ad hoc* judicial authority, or by the ordinary courts. This is especially so where fundamental rights are involved.”³⁶

Nevertheless, the European Court admitted that the control can take other forms. A parliamentary board or a specific supervisory commission independent of the authorities carrying out the surveillance, and vested with sufficient powers and competence to exercise an effective and continuous control, can be accepted as well. The Court emphasized on the democratic character of the control, which can be reflected in a balanced membership of the parliamentary board, with representation of the opposition. In those circumstances, such supervisory bodies may be regarded as enjoying sufficient independence to give an objective ruling.³⁷ In the *Leander* case of 1987, the Court repeated that it

“attaches particular importance to the presence of parliamentarians on the national police board (...). The parliamentary members of the board, who include members of the opposition, participate in all decisions regarding whether or not information should be released to the requesting authority. In particular, each of them is vested with a right of veto, the exercise of which automatically prevents the board from releasing the information. (...) This direct and regular control over the most important aspect of the register – the release of information – provides a major safeguard against abuse.”³⁸

³⁴ See Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 6.

³⁵ ECtHR, *Klass v. Germany*, 1978, § 56.

³⁶ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 25.

³⁷ See ECtHR, *Klass v. Germany*, 1978, § 56.

³⁸ ECtHR, *Leander v. Sweden*, 1987, § 65.

The Venice Commission on its turn noticed the existence of supplemental parliamentary supervision.

“In many countries parliamentary committees have been created specifically for the supervision of internal security organs. Regular reports shall be made to the committee, which is also entitled to be provided with any additional information it requires and to issue its opinions on the activities of the security organs. The committee is not, however, a hierarchical superior to the security organs. Hence, it cannot give them any orders.”³⁹

An overall control over the system of secret surveillance being entrusted to the executive, e.g. the Minister of Internal Affairs, and not to independent bodies, is not acceptable to the Court.⁴⁰ In its policy observations, the Venice Commission also found that internal security organs are normally supervised by their hierarchical superiors, at the top level by the appropriate government Minister or even by the Prime Minister or the Head of State. The supervision often includes regular reports from the security services. It may even include the need for a supervising person or body to authorize the commencement of investigations in individual cases. Nevertheless, fundamental freedoms can never be properly guaranteed if domestic security surveillances may be conducted within the absolute discretion of the executive.

“It is an established fact that where there is unreviewed executive discretion this may very well lead to imposing pressure in order to obtain incriminating evidence and thereby overlook potential invasions of privacy. Thus, the services cannot operate uncontrolled. There have been various instances where security services have attempted to influence the political scene in the countries in which they operate.”⁴¹

b. A priori and ad hoc control

In the view of the Court, review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, it states, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual’s knowledge.

“Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual’s rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 para. 2, are not to be exceeded. One of the fundamental principles of a democratic society is the rule of law, which is expressly referred to in the Preamble to the Convention (...).”⁴²

³⁹ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 14.

⁴⁰ ECtHR, *Association for European Integration and Human Rights and Ekimdzhiiev v. Bulgaria*, 2008, § 87.

⁴¹ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 20.

⁴² ECtHR, *Klass v. Germany*, 1978, § 55

That rule of law implies, according to the Court, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally, as mentioned above, be assured by the judiciary, at least in the last resort. Judicial control offers the best guarantees of independence, impartiality and a proper procedure.⁴³ The fact that many intelligence gathering actions are carried out clandestinely so that the person who is the target of their operation will often not be aware of them, makes it in the analysis of the Venice Commission impractical to rely on judicial control at the initiative of the person who has been the target of an operation of the security services. The proportionality principle is essential in the control process.

“As such a judicial control could be seen as a vital safeguard of the rights of the individual, it might be advisable to make a recommendation that operations of the security services that involve intrusions into rights and freedoms protected by the Constitution or the European Convention on Human Rights can only be carried out under judicial control.”⁴⁴

c. A posteriori control

The Venice Commission observed with regard to *a posteriori* control that a proper balance must be struck between the interests of the individual and the interests of society at large. The principle of proportionality must be applied to assess whether a particular act that could impinge on the right of the individual citizen could be justified as acceptable in a democratic society as a necessary measure to ensure the rule of law. As an overriding principle,

“the courts should have jurisdiction to determine whether the actions complained of were within the powers and functions of the internal security services as established by law. Within the limitations laid down by law, the court should have the right to determine whether there was undue harassment of the individual or abuse of administrative discretion in his or her regard. Judicial review of the executive acts, even with proper safeguards essential in the circumstances to ensure the integrity of the State, should not be unduly withheld.”⁴⁵

In the view of the European Court,

“As regards review a posteriori, it is necessary to determine whether judicial control, in particular with the individual's participation, should continue to be excluded even after surveillance has ceased. Inextricably linked to this issue is the question of subsequent notification, since there is in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality.”⁴⁶

⁴³ See ECtHR, *Rotaru v. Romania*, 2000, § 57-59; In the Antunes Rocha case, the Court reiterated this idea, omitting however the reference to the judiciary as key player. See ECtHR, *Antunes Rocha v. Portugal*, 2005, § 76.

⁴⁴ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 13.

⁴⁵ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 13.

⁴⁶ ECtHR, *Klass v. Germany*, 1978, § 57.

Question is whether it is even feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. In the opinion of the Court, subsequent notification to each individual affected by a suspended measure might well jeopardize the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. The conclusion of the Court is that the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with article 8 ECHR.⁴⁷ However, legislation excluding such notification in any case and at any time (for reasons of classification of information), are intolerable. Under those circumstances, and unless these persons are subsequently prosecuted on the basis of the material gathered through covert surveillance (or unless there has been a leak of information) the persons concerned cannot learn whether they have ever been monitored and are accordingly unable to seek redress for unlawful interferences with their article 8 rights.⁴⁸

4. Measure necessary in a democratic society

In the context of national security measures, the second condition does not pose a problem: public safety or the economic well-being of the country, the prevention of disorder or crime and the protection of the rights and freedoms of others are described in the Convention as legitimate goals for a privacy intrusion. The measures, however, also have to be necessary in today's democratic society:

“While the Court recognizes that intelligence services may legitimately exist in a democratic society, it reiterates that powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.”⁴⁹

An interference will be considered necessary in a democratic society for a legitimate aim if it answers a so-called “pressing social need” and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are “relevant and sufficient”. The Venice Commission stated that having accepted that the unorthodox means by which internal security services must be allowed to operate can have a negative effect, it is imperative that these extraordinary measures and restrictions of fundamental rights and liberties should be proportionate to the danger involved.

⁴⁷ ECtHR, *Klass v. Germany*, 1978, § 58.

⁴⁸ ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 2008, § 91.

⁴⁹ ECtHR, *Klass v. Germany*, 1978, § 42; see also e.g. ECtHR, *Rotaru v. Romania*, 2000, § 47-48, ECtHR, *Antunes Rocha v. Portugal*, 2005, § 66.

“The same principle applies when the internal security services intervene out of necessity in the defense of the State in the political or democratic process. These services are only authorized to intervene in this manner as long as the danger their action is meant to prevent persists and with the minimum involvement for a definite and determinate purpose.”⁵⁰

While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention. A certain margin of appreciation is nevertheless left to the competent national authorities in this assessment. The breadth of this margin varies, depending on a number of factors including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual’s effective enjoyment of intimate or key rights. Equally, where a particularly important facet of an individual’s existence or identity is at stake, the margin allowed to the State will be restricted. Where, however, there is no consensus within the Member States of the Council of Europe, either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider.⁵¹

Occasionally, the Court considers not only the qualitative aspects of legislation, but also statistical evidence: so, it has considered the amount of times a government has used secret investigation during a certain period of time in relation to its population numbers, how many of these were used in criminal proceedings afterwards, and so on. For example, the Court noted in the *Ekimdzhiev* case that

“more than 10,000 warrants were issued over a period of some twenty-four months, from 1 January 1999 to 1 January 2001, and that number does not even include the tapping of mobile telephones (for a population of less than 8,000,000). Out of these, only 267 or 269 had subsequently been used in criminal proceedings. (...) Additionally, in an interview published on 26 January 2001 the then Minister of Internal Affairs conceded that he had signed 4,000 orders for the deployment of means of secret surveillance during his thirteen months in office (...). By contrast, in *Malone* (...), the number of the warrants issued was considered relatively low (400 telephone tapping warrants and less than 100 postal warrants annually during the period 1969-79, for more than 26,428,000 telephone lines nationwide). These differences are telling, even if allowance is made for the development of the means of communication and the rise in terrorist activities in recent years. They also show that the system of secret surveillance in Bulgaria is, to say the least, overused, which may in part be due to the inadequate safeguards which the law provides.”⁵²

In general, the Court upheld in the past that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant’s right to respect for his or her private life, the national authorities enjoyed a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of

⁵⁰ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 26.

⁵¹ See e.g. ECtHR, *S. and Marper v. United Kingdom*, 2008, § 101-102.

⁵² ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 2008, § 92.

protecting national security.⁵³ Since the 1990s, there are indications that that margin has steadily been narrowed. In a number of recent cases, the Court has seriously questioned the efficacy of national legislation in practice. In some situations not relating to article 8, the Court has even considered that there is no margin of appreciation at all, even if the government alleges that national security is at stake.⁵⁴

IV. Special investigation techniques interfering with the right to privacy

When it comes to privacy, the European Court accepts that government interferences can be justified even if national security has not been affected yet. That is inherent to the nature of the privacy reducing measures: the government's goal is to prevent any actual threat of being carried out. Obviously, any such danger to national security will have to be proven, at least made credible, by facts. In what follows the most important investigation techniques are examined more in detail. As explained above, every State has its own legal framework to organize the competences of the actors concerned. In Belgium, there is a separation between the police forces, performing criminal investigations, and the Security of the State, which has a proactive role. When it comes to gathering their information, and certainly under the new Security of the State bill, they have comparable instruments at their disposal. Nevertheless, both are subjected to a different set of rules regarding procedure and control. Starting from the Belgian context, the analysis of the European Court of Human Rights will form the core of this examination. Wherever that is useful, any specific views adopted by the Belgian Constitutional Court will be added.

A. General principles in Belgium

1. Police and prosecuting authorities

The Code of Criminal Procedure, as amended severely in 2003 on this point, constitutes the legal framework for the special investigation techniques the police and prosecuting authorities can engage in. Although the techniques are not very systematically structured in the Code, recurring elements in the relevant dispositions are proportionality, subsidiarity and judicial control. When it concerns less

⁵³ See e.g. ECtHR, *Leander v. Sweden*, 1987, § 59; ECtHR, *Malone v. United Kingdom*, 1984, § 81.

⁵⁴ The Court has found, for example, that there is no margin of appreciation in the application of the principle of non-refoulement under article 3 ECHR. See ECtHR, *Chahal v. United Kingdom*, 1996; ECtHR, *Saadi v. Italy*, 2008.

invasive techniques, the prosecuting authorities, under whose supervision and directives the police operates, enjoy some autonomy. For the most invasive applications, like house searches, taps or systematic observations involving technical tools, a key role is reserved for the investigating magistrate.

In the Belgian criminal law system, two types of investigations can take place: a general one, with the prosecution department in charge, or a judicial investigation, under control of an investigating judge. The latter can be ordered for example if the case is very complex, when it is of a very serious nature, or when it involves the application of special investigation techniques. By doing so, a judge can supervise the case at an earlier point than under normal circumstances. In some cases, the prosecution can ask a judge to order the application of a technique the police cannot engage in on its own initiative.

2. Security of the State

In the pending bill about the Security of State, and contrary to the rules for the police and prosecuting authorities, a systematic inventory is made of all techniques the civil intelligence service can engage in. The two categories of techniques, distinguished on the basis of the level of gravity, are under primary the control of a commission of magistrates (new sec. 43/1, §1 of the 1998 Act), and ultimately under control of a parliamentary body, which will assess the legality of the investigation decisions, including the proportionality and subsidiarity criteria (new sec. 43/2 of the 1998 Act). This body can undertake action on its own initiative, or in reaction of a complaint by a citizen. It can order the ending of the application of a technique and exclude the obtained information (new sec. 43/6, §1 of the 1998 Act).

a. Less invasive (special) investigation techniques

The Security of State bill subjects the category of less invasive techniques to a common legal framework. These techniques include the systematic observation of persons, their presence or behavior, and the observation of goods, places or actions that show importance for the exercise of the assignment, all of that in public or private places accessible to the public; the search of public or private places accessible to the public with technical resources, including the contents of any closed object found there, whenever that shows importance for the assignment; the acquainting of oneself with the identity of the sender or receiver of mail or the holder of a mail box whenever this shows an importance to the assignment; the identification of the holder or user of a service of electronic communication, the used means of communication or any relevant operator invoices and the tracking of call data of electronic communication means, or the localizing of its source or destination.

These techniques can only be applied when other methods seem insufficient, after written and motivated consent of the team leader, and notification of the supervisory commission. This commission counts three members, all magistrates, of which one examining magistrate and one member of the public prosecution (new sec. 43/1, §1 of the 1998 Act). Regular reports are required. The exploitation of irregularly acquired information is excluded, and the unlawfully applied technique concerned is suspended. A special arrangement is provided for inquiries involving attorney's, MD's and journalists (new sec. 18/3, §1 and 2 of the 1998 Act).

b. Very invasive (exceptional) investigation techniques

The Security of State bill equally subjects the most invasive techniques to a set of rules. These techniques include the systematic observation and the search of private places *not* accessible to the public, residences or their premises, or the working places of attorney's, MD's and journalists, without the knowledge or consent of the owner, and including the contents of any closed object found there; the opening of mail to acquaint oneself with its content; the tapping, acquainting and recording of communications; the gathering of information concerning bank accounts and transactions; the entering into computer systems, with or without technical resources or fake input keys, to gain access, lift its protection, or to install decoding applications or acquire data.

These techniques can only be applied when there are serious threats for the internal security of the State and the continued existence of the democratic and constitutional order, the external security of the State and its international relations or its scientific or economic potential and when these threats concern an activity related to espionage or terrorism, including radicalization phenomena, proliferation, noxious sectarian organizations and criminal organizations (new sec. 18/9, §1, 1° of the 1998 Act). The application of the technique is subjected to a subsidiarity and proportionality requirement, and can only be authorized by the team leader after concurring advice of the supervisory commission (new sec. 18/9, §2 and 3 of the 1998 Act). If the commission does not provide an advice within four days, the competent minister may be seized to take a decision (new sec. 18/10, §3 of the 1998 Act). A special arrangement is provided for inquiries involving attorney's, MD's and journalists (new sec. 18/9, §4 of the 1998 Act). The technique is only applicable for a renewable period of two months, regular reporting is required, and it has to be ended or suspended when the threats concerned have ceased to exist, when its application is no longer useful or when irregularities occur (new sec. 18/10, §1 and 3 of the 1998 Act). In case of urgency, the team leader can order the application of the technique for 48 hours, after authorization of the president of the supervisory commission or the competent minister (new sec. 18/10, §4 of the 1998 Act). The supervisory commission can check at any time the legality of the applied techniques (new sec. 18/10, §6 of the new Act).

The bill provides that when the application of the abovementioned intelligence techniques reveal serious indications about the committing of a crime or, on reasonable grounds, point at criminal facts that are to be committed or that are committed but not yet revealed, the intelligence services notify the supervisory commission. If the commission concurs, the (federal) prosecution services are informed. This information may not be, however, the exclusive or principal grounds for the conviction of a suspected person (new sec. 19/1 of the 1998 Act).

B. Systematic observations and discrete visual checks

Although ordinary observations are part of the normal police activities, the 2003 Act provides for more systematic forms: prolonged observations or with a higher degree of intensity, observations deploying technical resources (such as infrared cameras, motion detectors, etc.), observations in a transnational investigation, or observations conducted by specialized federal police units. With regard to these systematic observations, the Constitutional Court acknowledged that the Code of Criminal Procedure provides conditions that make the application of the observation technique dependent of the seriousness of the criminal acts committed or to be committed.⁵⁵ Generally, the prosecutor can order the observation if all other methods fail and if proportionate to the investigative goals (sec. 47*sexies* CCP), but in as far that the Act makes systematic observations implying technical resources possible without a judge taking automatically control over the whole investigation however, the Court considered it was unconstitutional. According to the Court, this technique has to be considered as invasive as a house search, the tapping and recording of private telephone conversations (sec. 90*ter* CCP) and fully anonymous testimony, techniques which are equally inaccessible for the prosecution without judicial control over the whole investigation.⁵⁶

The Constitutional Court followed the same reasoning with regard to discrete visual checks (sec. 89*ter* CCP), involving the entering of a private place, without the knowledge of its inhabitant (and thus contrary to a house search). The goal may be to *look around* for the presence of crime-related materials (but not *searching* for them), the gathering of evidence (samples, prints, photo's,...) or the placing of spyware (but not listening devices; for that, specific rules apply, as will be shown below). Although the technique can be allowed in principle because of its limited application to certain serious crimes or the ones committed in the context of a criminal organization, and the requirement of subsidiarity, it was considered unconstitutional in as far as the whole investigation was not

⁵⁵ See Constitutional Court 21 December 2004, n° 202/2004, B.5.6.2.

⁵⁶ See Constitutional Court 21 December 2004, n° 202/2004, B.5.6.3. to B.5.7.8.

automatically put under judicial control.⁵⁷ In the 2005 Reparation Act, a distinction was made between private places with a non-residential character (sec. 46*quinquies* CCP) and private places with a residential character, including the offices of MD's and attorneys (sec. 89*ter* CCP). Hence, discrete visual checks can be ordered for the former by the prosecutor; for the latter, a judge has to take control of the investigation, which implies the impossibility to engage in it without a crime being already committed. This distinction was not regarded as a discrimination (under sec. 10 and 11 of the Constitution).⁵⁸ The competence of the prosecution to order them without judicial intervention for the non-residential private places was not held in violation of the right to privacy either: it is allowable in as far as it is necessary to reach the legally intended purpose and if the absence of the judicial guarantee is compensated by other measures in order to prevent abuse. The Court found that this was the case, as the order by the prosecution can only be given for a certain category of specific crimes or in connection with a criminal organization and as a subsidiary means of investigation (sec. 46*quinquies*, §1 CCP). A decision can furthermore only be taken if there are specific clues of the presence of relevant materials, of which evidence can be gathered, or that it concerns places that can be considered to be used by suspects (sec. 46*quinquies*, §2 CCP). Therefore, there is no violation of the right to privacy.⁵⁹

The pending bill concerning the Security of State provides the possibility for observation of persons, their presence or behavior, and the observation of goods, places or actions that show importance for the exercise of the assignment, with or without technical resources, all of that in public or private places *accessible to the public* (new sec. 18/2, §1, 1° and 18/4 of the 1998 Act). The data concerned can be registered. The general framework for special techniques applies, as discussed above. The bill provides equally in the possibility to observe private places *not accessible to the public*, residences or their premises, or the working places of attorney's, MD's and journalists (new sec. 18/2, §2, 1° and sec. 18/11, 1° of the 1998 Act). In that case, the rules for exceptional techniques apply.

If adopted, the bill will make it possible for the intelligence services as well to search public or private places *accessible to the public* with technical resources, including the contents of any closed object found there, whenever that shows importance for the assignment. If the investigation of an object cannot take place on the spot, an object can be taken away for a limited time. It has to be returned as soon as possible, unless that endangers the assignment. The officers can be authorized to enter these places without knowledge or consent of the owner, for the needs of the search or to return a searched object (new sec. 18/2, §1, 2° and 18/5, §1 and 2 of the 1998 Act). They can equally be authorized to install technical observation equipment, repair it or take it away, with the exception of photographic

⁵⁷ See Constitutional Court 21 December 2004, n° 202/2004, B.13.5 to B.14.

⁵⁸ See Constitutional Court 19 July 2007, n° 105/2007, B.6.1 to B.6.4.

⁵⁹ See Constitutional Court 19 July 2007, n° 105/2007, B.6.2 to B.6.8.

equipment (new sec. 18/4 of the 1998 Act). The general framework for special techniques applies. Furthermore, Security of State officers will be able to search private places *not accessible to the public*, residences or their premises, or the working places of attorney's, MD's and journalists, without the knowledge or consent of the owner, and including the contents of any closed object found there (new sec. 18/2, §2, 2° and 18/12, §1, 1° and 2° of the 1998 Act). If the investigation of an object cannot take place on the spot, and if the information cannot be acquired otherwise, the object can be taken away as described above (new sec. 18/12, §1, 3° and §2 of the 1998 Act). Again, officers can enter these places in order to install or remove technical observation equipment (new sec. 18/11, 2° of the 1998 Act). The exceptional techniques regulation is applicable.

Within the European Convention of Human Rights framework, the justifiability of such measures depends on what particular actions have been undertaken. The systematically retaining of information on a person's whereabouts and doings will have to be in accordance with the abuse safeguards described above. When observations are conducted (and the results stored) with some kind of technical equipment, the principles of communication taps or private information data banks may apply. Obviously, whenever private places are physically searched, that constitutes a serious interference with a person's private life. As always, the European Court attaches great importance to preceding judicial control.⁶⁰ In the *Murray* case, the Court found that

“it remains to be determined whether [the searches] were necessary in a democratic society and, in particular, whether the means employed were proportionate to the legitimate aim pursued. In this connection it is not for the Court to substitute for the assessment of the national authorities its own assessment of what might be the best policy in the field of investigation of terrorist crime (...).”⁶¹

Thus, a certain margin of appreciation in deciding what measures to take both in general and in particular cases should be left to the national authorities. The Court continued by reaffirming the responsibility of an elected government in a democratic society to protect its citizens and its institutions against the threats posed by organized terrorism and to the special problems involved in the arrest and detention of persons suspected of terrorist-linked offences.

“These two factors affect the fair balance that is to be struck between the exercise by the individual of the right guaranteed to him or her under paragraph 1 of Article 8 and the necessity under paragraph 2 for the State to take effective measures for the prevention of terrorist crimes (...).”⁶²

As there existed evidence resulting in a genuine and honest suspicion that the applicant committed a terrorist linked crime, the Court accepted that there it was reasonable to search her house.⁶³ In general,

⁶⁰ See e.g. ECtHR, *Chappell v. United Kingdom*, 1989, § 59.

⁶¹ ECtHR, *Murray v. United Kingdom*, 1994, § 90.

⁶² ECtHR, *Murray v. United Kingdom*, 1994, § 91.

⁶³ ECtHR, *Murray v. United Kingdom*, 1994, § 92.

the existing of specific legislation dealing with situations in which officers enter private places without conducting a normal house search is appropriate. With regard to cases concerning telephone tapping, listening and visual surveillance including, for example, the planting of electronic devices and the use of video cameras to observe the activities of persons in private places, the Venice Commission noted in 1998 that the introduction of such legislation would ensure that, while the security services are provided with the necessary tools, they do not exceed their powers:

“Although the State requires powers of interception in order to gather information about serious crime and terrorism, these powers should not be unlimited.”⁶⁴

In any case, authorities will have to be careful, even when doing observations in a public environment: according to the European Court of Human Rights, there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life. It cannot be excluded that a person’s private life may be concerned in measures effected outside a person’s home or private premises. His reasonable expectations as to privacy is a significant, though not necessarily conclusive factor.⁶⁵

C. The interception and opening of mail correspondence

Although section 29 of the Constitution, guaranteeing secrecy of correspondence, does not provide for exceptions, the Constitutional Court accepts that infringements can be necessary if other fundamental rights are at stake, such as the right to life, liberty and property, in as far as the limitations are proportionate to these goals. *Intercepting and confiscating mail* (sec. 46ter CCP) can be ordered by the public prosecutor if there are serious clues that a crime was committed punishable with at least one year imprisonment. If he wants to intercept mail in a proactive investigation (before any criminal act has taken place), it is only possible for crimes that the expected crimes will be committed in the context of a criminal organization, or for certain serious crimes. E-mail is excluded from this procedure, as it is not protected by the inviolability of correspondence. The authority to order the *opening* of mail and acknowledging its contents is only attributed to a judge in charge of the investigation, which excludes the prosecution, unless the suspect is caught in the act (sec. 88sexies CCP). As a judge can only be in control of a reactive investigation, the technique is principally excluded in a proactive investigation. Therefore, the Court did not consider it to be unconstitutional.⁶⁶

⁶⁴ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 21.

⁶⁵ See e.g. ECtHR, *P.G. and J.H. v. United Kingdom*, 2001, § 56-57; ECtHR, *Perry v. United Kingdom*, 2003, § 36-37.

⁶⁶ See Constitutional Court 21 December 2004, n° 202/2004, B.12.1 to B.12.5.

The prosecutor can also ask authorization of an investigating magistrate without that the latter takes full charge of the investigation.

With regard to the intelligence service, the bill concerning the Security of State provides the possibility to acquaint oneself with the identity of the sender or receiver of mail or the holder of a mail box whenever this shows an importance to the assignment (new sec. 18/2, §1, 3° and sec. 18/6, §1 of the 1998 Act). The general framework for special techniques applies, as discussed above, but contrary to that framework, the order of the team leader can be given orally in case of extreme urgency. A written confirmation is required as soon as possible (new sec. 18/3, §1 and sec. 18/6, §2 of the 1998 Act). The bill provides equally in the possibility to open mail and to acquaint oneself with its content (new sec. 18/2, §2, 4° and sec. 18/14, §1 of the 1998 Act). In that case, the framework for exceptional techniques applies.

Obviously, the European Court of Human Rights has already dealt with protection of correspondence problems. In fact, many problems occur with regard to the mail traffic between a prisoner and his attorney. The Court found that the prison authorities may open a letter from a lawyer to a prisoner

“when they have reasonable cause to believe that it contains an illicit enclosure which the normal means of detection have failed to disclose. The letter should, however, only be opened and should not be read. Suitable guarantees preventing the reading of the letter should be provided, e.g. opening the letter in the presence of the prisoner. The reading of a prisoner’s mail to and from a lawyer, on the other hand, should only be permitted in exceptional circumstances when the authorities have reasonable cause to believe that the privilege is being abused in that the contents of the letter endanger prison security or the safety of others or are otherwise of a criminal nature. What may be regarded as “reasonable cause” will depend on all the circumstances but it presupposes the existence of facts or information which would satisfy an objective observer that the privileged channel of communication was being abused.”⁶⁷

In the *Erdem* case, the Court accepted that it is necessary in a democratic society, among others for reasons of national security, that correspondence of prisoners specifically suspected of belonging to a terrorist organization may be monitored. The Court stressed that the monitoring power was vested in an independent judge who had to be unconnected with the investigation and was under a duty to keep the information thus obtained confidential. For these reasons, the interference was considered falling in the margin of appreciation of the State to assess the balance between defending democratic society and the individual rights and not disproportionate to its goal.⁶⁸ Having interception warrants issued by courts would, according to the Venice Commission, also serve to dismiss any objection to introducing the transcripts as admissible evidence in a prosecution case.⁶⁹

⁶⁷ ECtHR, *Campbell v. United Kingdom*, 1992, § 48.

⁶⁸ ECtHR, *Erdem v. Germany*, 2001, § 67-69.

⁶⁹ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 21.

D. Identification, tracking and tapping of telecommunication

1. The Belgian framework

In criminal investigations, the *identification* of telephone numbers and users needs no intervention of a judge, and can even in urgent matters be conducted by a police officer on agreement of the prosecutor (sec. 46bis, §1 CCP). For the *tracking and localizing* of calls a judge is required to control the investigation (sec. 88bis CCP), with an exception for the next 24 hours if a suspect was caught in the act. An investigating magistrate can exceptionally also authorize the tracking of calls without taking control of the investigation. The entering of a private place in order to *install telephone tapping equipment* (sec. 90ter CCP) is only allowed when a judge is in control of the criminal investigation (as opposed to the public prosecutor's office), and is therefore not considered unconstitutional. The Constitutional Court considered that to be a sufficient guarantee, in the knowledge that the actual tapping (by analogy to tapping by a telephone operator) is subjected to severe conditions.⁷⁰

Tapping calls is possible if a judge is in control of the investigation, if all other methods failed, and if the person tapped is seriously suspected of having committed one of a limited enumeration of crimes (sec. 90ter, §1 CCP), a number of which closely connected to national security. It concerns among others attack or conspiracy against the head of state or the form of government, serious violations of international humanitarian law, terrorist crimes, membership of and participation in a criminal organization, the taking of hostages, manslaughter and murder, human trafficking, crimes concerning nuclear material, drug trafficking, or arms and people smuggling. The prosecutor can only order the measure when caught in the act, and then only for extortion and the taking of hostages; contrary to the tracking of calls, he cannot ask for simple authorization by a judge. In Belgium, proactive tapping is legally excluded in criminal investigations (something the ECHR does not, see *Lüdi v. Switzerland* below), although attempts to commit one of the mentioned crimes are enough to justify the measure. Equally, conspiracy to commit one of those crimes can form a basis, if the conspiracy is set up to assault the people or properties connected to those crimes. It is noteworthy that tapping not only includes classic phone or cell phone traffic, but also the *sending* of e-mail and direct tapping by using microphones. It is noteworthy that e-mails, prints thereof or cell phone messages which are saved to the phone or another carrier are not protected by the procedure: they can be read or confiscated during a house search, just like (any other) paper work. E-mail, other than telephone or classic mail correspondence, enjoys no specific protection.

⁷⁰ See Constitutional Court 21 December 2004, n° 202/2004, B.15.1 to B.16.

The bill concerning the Security of the State provides the possibility to take any measure to identify the holder or user of a service of electronic communication, the used means of communication or any relevant operator invoices. The acting officer can equally engage in tracking call data of electronic communication means or in localizing its source or destination (new sec. 18/2, §1, 4° and 5°, sec. 18/7, §1 and sec. 18/8, §1 of the 1998 Act). Contrary to the abovementioned rules for this type of techniques, the order of the team leader can be given orally in case of extreme urgency. A written confirmation is required as soon as possible (new sec. 18/3, §1, sec. 18/7, §2 and sec. 18/8, §2 of the 1998 Act). Identification measures are special techniques in the context of the bill.

If adopted, the text will also enable the Security of the State to tap, acquaint and record communications (new sec. 18/2, §2, 7°, and sec. 18/17, §1 of the 1998 Act). To do so, officers can be authorized to enter private places with or without access to the public or residences and their premises, including the working places of attorney's, MD's, and journalists, at any time, and without knowledge or consent of the owner (new sec. 18/2, §2, 7°, sec. 18/17, §1 and §2 of the 1998 Act). After their exploitation, the recordings are destroyed (new sec. 18/17, §7 of the 1998 Act). The general framework for exceptional techniques applies, as discussed above.

2. The European framework

The European Court of Human Rights has taken a differentiated approach. In the *Klass* case mentioned above, the Court noted the technical advances made in the means of espionage and, correspondingly, of surveillance, but most importantly it noted that due to the development of terrorism in Europe in recent years,

“democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction.”⁷¹

For that reason, the Court accepted that the existence of legislation

“granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.”⁷²

The domestic legislature enjoys a certain discretion: the Court does not consider itself to be a substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field. Nevertheless it stressed that

⁷¹ ECtHR, *Klass v. Germany*, 1978, § 48.

⁷² ECtHR, *Klass v. Germany*, 1978, § 48.

“this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.”⁷³

Regarding the existence of an interference with the right to privacy, the Court assesses that the mere existence of tapping legislation entails, for all those who might fall within its reach, a menace of surveillance (see also above). This menace necessarily strikes at freedom of communication between users of the postal and telecommunications services and thereby constitutes an interference by a public authority with the exercise of the applicants’ right to respect for correspondence.⁷⁴ In the *Malone* case of 1984, the Court considered that the registering of numbers dialed on a particular telephone and the time and duration of each call by its very nature is to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. Hence, the measures taken in order to prevent arbitrariness are not under the same scrutiny as in cases of actual tapping of conversations. The Court does not accept, however, that the use of that data, whatever the circumstances and purposes, cannot give rise to an issue under article 8.⁷⁵

In the *Huvig* and *Kruslin* judgments of 1990, the Court considered that tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a law that is particularly precise: in the view of the Court, it is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.⁷⁶ The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures.⁷⁷ It is noteworthy that contrary to Belgian legislation, the proactive ordering of a telephone tap (before any crime is committed) is not necessarily a violation of article 8 of the ECHR. The Court noted in the *Lüdi* case that the tap was aimed at the prevention of crime, and the Court, as it said, had no doubt as to its necessity in a democratic society.⁷⁸ The principles regulating telephone tap apply equally to the use of

⁷³ ECtHR, *Klass v. Germany*, 1978, § 49.

⁷⁴ See e.g. ECtHR, *Klass v. Germany*, 1978, § 41; ECtHR, *Liberty v. United Kingdom*, 2008, § 62; ECtHR, *Iordachi v. Moldova*, 2009, § 34.

⁷⁵ See e.g. ECtHR, *Malone v. United Kingdom*, 1984, § 83-84; ECtHR, *P.G. and J.H. v. United Kingdom*, 2001, § 42-47.

⁷⁶ See e.g. ECtHR, *Huvig v. France*, 1990, § 32; ECtHR, *Kruslin v. France*, 1990, § 33; ECtHR, *Kopp v. Switzerland*, 1998, § 72; ECtHR, *Valenzuela Contreras v. Spain*, 1998, § 46; ECtHR, *Weber and Saravia v. Germany*, 2006, § 93; ECtHR, *Liberty v. United Kingdom*, 2008, § 62; ECtHR, *Iordachi v. Moldova*, 2009, § 39.

⁷⁷ See e.g. ECtHR, *Huvig v. France*, 1990, § 29; ECtHR, *Kruslin v. France*, 1990, § 30; ECtHR, *Kopp v. Switzerland*, 1998, § 64; ECtHR, *Weber and Saravia v. Germany*, 2006, § 93; ECtHR, *Iordachi v. Moldova*, 2009, § 39.

⁷⁸ See ECtHR, *Lüdi v. Switzerland*, 1992, § 39.

a radio-transmitting device, which is, in terms of the nature and degree of the intrusion involved, virtually identical to telephone tapping.⁷⁹

According to the Court, a distinction has to be made between two stages of interception: the authorizing of the measure and the actual carrying out of the surveillance.⁸⁰

a. Tap authorization

In the first stage, the general conditions to justify secret surveillance have to be fulfilled: the applicable legislation should provide the nature of the offences which may give rise to the tapping, a definition of the categories of people liable to be subjected to the measure, limits on its duration, the procedure to be followed for examining, using and storing the data, the precautions to be taken when communicating the data to others, and the circumstances in which recordings or tapes are erased or destroyed. In the context of telephone tapping, this means a definition of the categories of people liable to have their telephones tapped by judicial order and the nature of the offences which may give rise to such an order. The absence of an obligation to set a limit on the duration of telephone tapping, of specification of the procedure for drawing up the interception reports, and of the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and by the defense, is considered problematic.⁸¹

The Court stresses the value of a decision by an investigating judge or by the president of the indictment division of the court, who is an independent judicial authority.⁸² Interceptions ordered only by the public prosecution, without any *a priori* control possibility by a judge, do not meet the required standards of independence.⁸³ The Court considers it equally necessary to stress that telephone tapping is a very serious interference with a person's rights and that only very serious reasons based on a reasonable suspicion that the person is involved in serious criminal activity should be taken as a basis for authorizing it.⁸⁴ The Venice Commission advised the same: a phone tap should only be installed when the judge is satisfied that there is imminent danger of serious crime and that more routine methods of investigation would be unlikely to succeed. Provision should be made for the transcripts to

⁷⁹ ECtHR, *Bykov v. Russia*, 2009, § 79.

⁸⁰ ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 2008, § 84; see also ECtHR, *Iordachi v. Moldova*, 2009, § 41.

⁸¹ See e.g. ECtHR, *Huvig v. France*, 1990, § 34; ECtHR, *Kruslin v. France*, 1990, § 35; ECtHR, *Valenzuela Contreras v. Spain*, 1998, § 46; ECtHR, *Prado Bugallo v. Spain*, 2003, § 30; ECtHR, *Weber and Saravia v. Germany*, 2006, § 92; ECtHR, *Iordachi v. Moldova*, 2009, § 39.

⁸² See e.g. ECtHR, *Huvig v. France*, 1990, § 33; ECtHR, *Kruslin v. France*, 1990, § 34; ECtHR, *Kopp v. Switzerland*, 1998, § 72; ECtHR, *Amann v. Switzerland*, 2000, § 60.

⁸³ ECtHR, *Dumitru Popescu v. Romania*, 2007, § 70-73.

⁸⁴ ECtHR, *Iordachi v. Moldova*, 2009, § 51.

be handed first to the judge, who then releases to the investigating services such portions as he deems relevant to the investigations being carried out.⁸⁵ As it appears, the so-called “*John Doe*” taps provided for in section 206 of the U.S. Patriot Act (expiring in principle in 2009), being anonymous regarding either person or place monitored, do not meet the requirements of the European Court. Its accordance with the 4th Amendment of the U.S. Constitution can, in fact, equally be questioned.

b. Tap control

With regard to the second stage, control over the surveillance should be put under control of a judge or another independent body.⁸⁶ The Court has found that the situation whereby all those who have conversations on a telephone line other than their own, in practice are deprived of the protection of the law, would render the protective machinery largely devoid of substance.⁸⁷ An investigating judge whose role is limited to issuing interception warrants and to decide on the storage of the tapes and transcripts is not enough if the law makes no provision for acquainting him with the results of the surveillance and does not require him to review whether the requirements of the law have been complied with. Leaving that competence to the prosecutor is not sufficient, certainly not when the situations protected are only those during pending criminal proceedings, and not any surveillance outside of that scope.⁸⁸ Leaving the task to draw up the reports of the monitored conversations to a judicial clerk is equally insufficient.⁸⁹ According to the Court, the requirement that the effects of the “law” be foreseeable means, in the sphere of monitoring telephone communications, that the guarantees stating the extent of the authorities’ discretion and the manner in which it is to be exercised must be set out in detail in domestic law, so that it has a binding force which circumscribes the judges’ discretion in the application of such measures.⁹⁰ Also, in the absence of any effective judicial control possibilities, the Court is not impressed by a mere theoretical resort to Parliament:

“De l’avis de la Cour, la simple possibilité pour un particulier (...) de saisir les commissions de la défense et de l’ordre public des deux chambres du Parlement national ne saurait suppléer à l’absence de tout contrôle a priori ou a posteriori des écoutes par une autorité judiciaire indépendante et impartiale. Tel qu’il était régi par la loi, le contrôle du pouvoir législatif semblait plutôt théorique et, en tout cas, dépourvu d’effet pratique pour l’individu, dans la mesure où une personne mise sur écoute n’était pas censée prendre connaissance de l’existence de telles mesures secrètes à son égard. De plus, la loi ne prévoyait aucune sanction ou mesure que les commissions parlementaires auraient été compétentes de prendre en cas de méconnaissance de la loi par les autorités ayant réalisé ou autorisé les interceptions (...).”⁹¹

⁸⁵ Council of Europe, Commission for democracy through law (Venice commission), Report “Internal security services in Europe”, adopted 7 March 1998, 21.

⁸⁶ See e.g. ECtHR, *Prado Bugallo v. Spain*, 2003, § 30; ECtHR, *Dumitru Popescu v. Romania*, 2007, § 70-73; ECtHR, *Iordachi v. Moldova*, 2009, § 30.

⁸⁷ See ECtHR, *Lambert v. France*, 1998, § 38.

⁸⁸ See ECtHR, *Iordachi v. Moldova*, 2009, § 47.

⁸⁹ See ECtHR, *Prado Bugallo v. Spain*, 2003, § 30.

⁹⁰ See ECtHR, *Valenzuela Contreras v. Spain*, 1998, § 60.

⁹¹ ECtHR, *Dumitru Popescu v. Romania*, 2007, § 77 (only available in French).

The Court has also paid attention to the circumstances in which recordings may or must be erased or the tapes be destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court.⁹² The Court noted that

“dans certaines circonstances, il soit excessif, ne serait-ce que d'un point de vue pratique, de transcrire et de verser au dossier d'instruction d'une affaire la totalité des conversations interceptées à partir d'un poste téléphonique. Cela pourrait certes aller à l'encontre d'autres droits, tel, par exemple, le droit au respect de la vie privée d'autres personnes qui ont passé des appels à partir du poste mis sous écoute. Si tel est le cas, l'intéressé doit néanmoins se voir offrir la possibilité d'écouter les enregistrements ou de contester leur véracité, d'où la nécessité de les garder intacts jusqu'à la fin du procès pénal, et, plus généralement, de verser au dossier d'instruction les pièces qui lui semblent pertinentes pour la défense de ses intérêts.”⁹³

E. Access to and the keeping of data

1. Access to banking and other information

Belgium has no legal system of banking secrecy. Nevertheless, until 2003 the prosecution and judges in charge of the investigation had to depend on the voluntary cooperation of the financial sector. They had of course the possibility to perform searches, but the conditions to do so are very strict. The inquiry into bank account information is now not a prerogative of the investigating magistrate, but can also be ordered by the public prosecutor. In order to meet the requirements of sec. 22 of the Constitution, the measure should be proportionate to its goal. The limitation to investigations in which there are serious indications of a crime punished by a sentence of at least one year imprisonment (sec. 46^{quater} §1 CCP) fulfills that requirement, according to the Constitutional Court. The fact that there is no time limit provided for inquiries into the past and for control in the future is not disproportionate.⁹⁴ The prosecution has access to the list of accounts, vaults or financial instruments of which a suspect is the holder, the transactions made to these accounts and the origin or destination of the funds, and the identity of the people who have received from or paid to these accounts. Following the transactions in real-time is also an option. The 2005 Reparation Act enlarged the possibilities to bank vaults and certain other financial instruments, and made a congelation of assets possible for certain serious crimes (sec. 46 §2 CCP). The fact that these measures can be carried out by the prosecutor, and need not be ordered by a judge, is not unconstitutional.⁹⁵

The pending bill concerning the Security of State provides the possibility to gather information concerning bank accounts and transactions (new sec. 18/2, §2, 5° and sec. 18/15, §1 of the 1998 Act).

⁹² See e.g. ECtHR, *Huvig v. France*, 1990, § 34; ECtHR, *Kruslin v. France*, 1990, § 35; ECtHR, *Valenzuela Contreras v. Spain*, 1998, § 46; ECtHR, *Prado Bugallo v. Spain*, 2003, § 30; ECtHR, *Weber and Saravia v. Germany*, 2006, § 92; ECtHR, *Iordachi v. Moldova*, 2009, § 39.

⁹³ ECtHR, *Dumitru Popescu v. Romania*, 2007, § 78 (only available in French).

⁹⁴ See Constitutional Court 21 December 2004, n° 202/2004, B.17.1 to B.21.

⁹⁵ See Constitutional Court 19 July 2007, n° 105/2007, B.5.5 to B.5.10.

Officers can also force an entrance into computer systems, with or without technical resources or fake input keys, to gain access, lift its protection system, install decoding applications or acquire data, in as far as no irreparable destruction or modifications take place. To do so, they can be authorized to enter private places with or without access to the public or residences and their premises, including the working places of attorney's, MD's, and journalists, at any time, and without knowledge or consent of the owner (new sec. 18/2, §2, 6° and sec. 18/16, §1, 1°, 2°, 3°, 4°, and §2 of the 1998 Act). If Security of State officers are planning to apply this technique to other governmental services, it is only possible after consent of the concerned department, although the data banks of the judicial branch cannot be subjected to the technique (new sec. 18/16, §1). Because it is considered a very invasive procedure, the general framework for exceptional techniques applies. When it comes to make personal reliability assessments (outside the scope of criminal proceedings), the Security of State already now has access to a wide range of governmental data banks: they can rely on information from the military secret service, police records, criminal records, or the civilian register of population, and from commerce, taxation or social security authorities.⁹⁶

2. The keeping of information in data banks

In the *Leander* judgment, the ECtHR already stated that

“There can be no doubt as to the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting the competent domestic authorities power, firstly, to collect and store in registers not accessible to the public information on persons and, secondly, to use this information when assessing the suitability of candidates for employment in posts of importance for national security.”⁹⁷

In the case of *P.G. and J.H. v. United Kingdom*, the it added that

“since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character.”⁹⁸

Nevertheless, the Court concluded that private-life considerations may arise once any systematic or permanent record comes into existence of such material from the public domain.

⁹⁶ Order in Council of 24 March 2000 in execution of the 11 December 1998 Act concerning the classification and the security authorizations, security certificates and security recommendations, *Official Journal* 31 March 2000.

⁹⁷ ECtHR, *Leander v. Sweden*, 1987, § 59.

⁹⁸ See ECtHR, *P.G. and J.H. v. United Kingdom*, 2001, § 57.

a. *The existence of an interference*

Nowadays, data can take a multitude of forms: not only plain biographic information on an individual's identity, but also photographic material, video or voice recordings, finger prints, DNA or cellular material. One of the questions is when the gathering of such data on a person amounts to an interference with article 8 ECHR.

In the *Friedl* case, which involved the use of photographs taken by the authorities during a public demonstration the European Commission for Human Rights⁹⁹ attached importance to whether the photographs amounted to an intrusion into the applicant's privacy (as, for instance, by entering and taking photographs in a person's home), whether the photograph related to private or public matters and whether the material thus obtained was envisaged for a limited use or was likely to be made available to the general public. In *Friedl*, the Commission noted that there was no such intrusion into the inner circle of the applicant's private life, that the photographs taken of a public demonstration related to a public event and that they had been used solely as an aid to policing the demonstration on the relevant day. In this context, the Commission attached weight to the fact that the photographs taken remained anonymous in that no names were noted down, the personal data recorded and photographs taken were not entered into a data-processing system and no action had been taken to identify the persons photographed on that occasion by means of data processing.¹⁰⁰ In *Lupker*, the Commission noted firstly that the photographs were not taken in a way which constitutes an intrusion upon the applicants' privacy, secondly that the photographs were kept in police or other official archives since they had been either provided voluntarily or taken by the police in connection with a previous arrest, and thirdly that the photo's

“were used solely for the purpose of the identification of the offenders in the criminal proceedings against the applicants and there is no suggestion that they have been made available to the general public or used for any other purpose.”¹⁰¹

Also, the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life.¹⁰²

Storing and releasing of information from a secret police file without opportunity to refute it is, however, considered an interference.¹⁰³ Furthermore, the Court is not persuaded that recordings taken

⁹⁹ Until the adoption of the 11th Protocol additional to the ECHR individual complaints were first assessed by an accessory organ to the Court. It was abolished in 1998.

¹⁰⁰ See ECmHR, *Friedl v. Austria*, 1994, § 49-51.

¹⁰¹ See ECmHR, *Lupker and others v. Netherlands*, 1992.

¹⁰² See ECmHR, *Herbecq and the association "Ligue des droits de l'homme" v. Belgium*, 1998.

for use as voice samples can be regarded as falling outside the scope of the protection afforded by article 8, since a permanent record has been made of the person's voice and it is subject to a process of analysis directly relevant to identifying that person in the context of other personal data.¹⁰⁴ Equally, a card containing data relating to an individual's private life that is being stored in a national card index has been considered an interference. In that connection the Court points out that it is not its job to speculate as to whether the information gathered is sensitive or not, or as to whether the individual has been inconvenienced in any way. It is sufficient to find that data relating to the private life of an individual are stored by a public authority to conclude that the creation and storing of the impugned card amounted to an interference within the meaning of Article 8.¹⁰⁵

Today, on a moment that many States across the world more and more tend to systematically keep biometrical data on persons (for example, of all people charged in a criminal case, or more general, all people entering the country), the question what status should be given to cellular and DNA material is highly important. With regard to the keeping of cellular samples and DNA profiles, the Court found in the landmark *S. and Marper* judgment of 2008 that this amounts to an interference with the right to privacy. The Court considered that

“an individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the issue of whether there has been an interference. Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today.”¹⁰⁶

The Court noted, however, that legitimate concerns about the conceivable use of cellular material in the future are not the only element to be taken into account. In addition to the highly personal nature of cellular samples, the Court observed that they contain much sensitive information about an individual, including information about his or her health. Moreover, samples contain a unique genetic code of great relevance to both the individual and his relatives. Given the nature and the amount of personal information contained in cellular samples, their retention per se must be regarded as interfering with the right to respect for the private lives of the individuals concerned. That only a limited part of this information is actually extracted or used by the authorities through DNA profiling and that no immediate detriment is caused in a particular case, does not change this conclusion.¹⁰⁷

¹⁰³ ECtHR, *Leander v. Sweden*, 1987, § 48.

¹⁰⁴ See *P.G. and J.H. v. United Kingdom*, 2001, § 59.

¹⁰⁵ See ECtHR, *Amann v. Switzerland*, 2000, § 70.

¹⁰⁶ ECtHR, *S. and Marper v. United Kingdom*, 2008, § 71.

¹⁰⁷ See ECtHR, *S. and Marper v. United Kingdom*, 2008, § 72-73.

As regards DNA profiles themselves, the Court noted that they contain a more limited amount of personal information extracted from cellular samples in a coded form. Nonetheless, the profiles contain substantial amounts of unique personal data. While that information may be considered objective and irrefutable, the processing through automated means allows the authorities to go well beyond neutral identification. In the Court's view, the DNA profiles' capacity to provide a means of identifying genetic relationships between individuals is in itself sufficient to conclude that their retention interferes with the right to the private life of the individuals concerned. The frequency of familial searches, the safeguards attached thereto and the likelihood of detriment in a particular case are immaterial in this respect. This conclusion is similarly not affected by the fact that, since the information is in coded form, it is intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons. The possibility the DNA profiles create for inferences to be drawn as to ethnic origin makes their retention all the more sensitive and susceptible of affecting the right to private life.¹⁰⁸

With regard to the keeping of finger prints, the Court reassessed the whole of the existing case-law in *S. and Marper*. In the past, the Commission concluded that fingerprints are neutral identifying features and therefore did not contain any subjective appreciations. As such, the retention of that material did not constitute an interference with private life.¹⁰⁹ The Court now came to the conclusion that the general approach in respect of photographs and voice samples should also be followed in respect of fingerprints. Fingerprints objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting private life and retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant. The Court accordingly considered that the retention of fingerprints on the authorities' records in connection with an identified or identifiable individual may in itself give rise, notwithstanding their objective and irrefutable character, to important private-life concerns.¹¹⁰

b. Justifiability of an interference

In order to maintain such data bases, the conditions of the second paragraph of article 8 will have to be fulfilled: any interference should be prescribed by law, pursue a legitimate goal and be necessary in a democratic society. As stated also in the *Rotaru* case (see above), for the measures to be in accordance with the law, in first, the Court reiterated

¹⁰⁸ See ECtHR, *S. and Marper v. United Kingdom*, 2008, § 74-76.

¹⁰⁹ See e.g. ECmHR, *Kinnunen v. Finland*, 1996.

¹¹⁰ See ECtHR, *S. and Marper v. United Kingdom*, 2008, § 84-85.

“that it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness (...).”¹¹¹

That the keeping of this information can serve a legitimate aim is not an issue. The Court had no difficulty in accepting that the compilation and retention of a DNA profile serves the legitimate aims of the prevention of crime and the protection of the rights and freedoms of others. This is not altered by the fact that DNA plays no role in the investigation and trial of the offences committed by an applicant. Furthermore, the Court did not consider it unreasonable for the obligation to undergo DNA testing to be imposed on all persons who have been convicted of offences of a certain seriousness.¹¹²

Question remains whether it is necessary in a democratic society to do so in certain situations. The Court found it to be beyond dispute that the fight against crime, and in particular against organized crime and terrorism depends to a great extent on the use of modern scientific techniques of investigation and identification. Nor is it disputed that the member States of the Council of Europe have since that time made rapid and marked progress in using DNA information in the determination of innocence or guilt.¹¹³ The Court noted that there can be no doubt about the substantial contribution which DNA records have made to law enforcement in recent years. Furthermore, sometimes the applicant may also reap a certain benefit from the inclusion of his DNA profile in the national database in that he may thereby be rapidly eliminated from the list of persons suspected of crimes in the investigation of which material containing DNA has been found.¹¹⁴ In the *S. and Marper* case, the Court emphasized nevertheless that it cannot limit itself to an assessment in abstracto of the technique:

“While it recognizes the importance of such information in the detection of crime, the Court must delimit the scope of its examination. The question is not whether the retention of fingerprints, cellular samples and DNA profiles may in general be regarded as justified under the Convention. The only issue to be considered by the Court is whether the retention of the fingerprint and DNA data of the applicants, as persons who had been suspected, but not convicted, of certain criminal offences, was justified under article 8, paragraph 2 of the Convention.”¹¹⁵

The Court considered the issue with due regard to the relevant instruments of the Council of Europe and the law and practice of the other Contracting States. According to the Court, the core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage. As regards, more particularly, cellular samples, most of the Contracting States allow these materials to be taken in criminal proceedings only from individuals

¹¹¹ ECtHR, *S. and Marper v. United Kingdom*, 2008, § 99.

¹¹² ECtHR, *Van der Velden v. Netherlands*, 2006.

¹¹³ See ECtHR, *S. and Marper v. United Kingdom*, 2008, § 105.

¹¹⁴ ECtHR, *Van der Velden v. Netherlands*, 2006.

¹¹⁵ ECtHR, *S. and Marper v. United Kingdom*, 2008, § 106.

suspected of having committed offences of a certain minimum gravity. In the great majority of the Contracting States with functioning DNA databases, samples and DNA profiles derived from those samples are required to be removed or destroyed either immediately or within a certain limited time after acquittal or discharge. A restricted number of exceptions to this principle are allowed by some Contracting States.¹¹⁶

The Court remarked that all Contracting States but the United Kingdom have chosen to set limits on the retention and use of such data with a view to achieving a proper balance with the competing interests of preserving respect for private life: the protection afforded by article 8 ECHR would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. In the Court's view, the strong consensus existing among the Contracting States in this respect is of considerable importance and narrows the margin of appreciation left to the State in the assessment of the permissible limits of the interference with private life.¹¹⁷

The Court equally answered the question whether there can be relevant and sufficient reasons for the permanent retention of fingerprint and DNA data of all suspected but not convicted people. In *S. and Marper*, while neither statistics nor examples in themselves at that time could establish that the successful identification and prosecution of offenders could not have been achieved without the permanent and indiscriminate retention of the fingerprint and DNA records of all persons in the applicants' position, the Court accepted that the extension of the database has nonetheless contributed to the detection and prevention of crime. The question, however, remained whether such retention is proportionate and strikes a fair balance between the competing public and private interests. In this respect, the Court considered a number of facts to be problematic:

“The Court is struck by the blanket and indiscriminate nature of the power of retention (...). The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed (...); in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.”¹¹⁸

¹¹⁶ See ECtHR, *S. and Marper v. United Kingdom*, 2008, § 107-108.

¹¹⁷ See ECtHR, *S. and Marper v. United Kingdom*, 2008, § 110-112.

¹¹⁸ See ECtHR, *S. and Marper v. United Kingdom*, 2008, § 114 and 117-119.

The Court acknowledged that the level of interference with the applicants' right to private life may be different depending on the category of personal data retained. The retention of cellular samples is particularly intrusive given the wealth of genetic and health information contained therein. However, such an indiscriminate and open-ended retention regime as the one in issue called for careful scrutiny regardless of these differences. The risk of stigmatization (stemming from the fact that persons who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons), as the Court emphasized, is of particular concern. Their perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while the data of those who have never been suspected of an offence are required to be destroyed. The Court finally considered that the retention of the unconvicted persons' data may be especially harmful in the case of minors, given their special situation and the importance of their development and integration in society. In conclusion,

“the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.”¹¹⁹

V. Special investigation techniques interfering with the right to a fair trial

It is clear that the application of special investigation techniques cannot only give cause to violations of an individual's privacy, but also touch to other fundamental rights, including the right to a fair trial. For example, the Belgian Constitutional Court examined whether the fact that ordinary residence observations, infiltration, interception and confiscation of mail and the inquiry of bank information can be ordered by the public prosecutor (and not by a judge) is not a violation of the right to a fair trial. It concluded that the legislature had assessed correctly that certain techniques causing a smaller interference with fundamental rights do not require judicial authorization.¹²⁰ Equally, the fact that the control over the application of special investigation techniques in proceedings that are dismissed by the prosecution afterwards is exercised by the attorney-general, and not by a judge, is no violation of the right to privacy or fair trial.¹²¹ On the other hand, the possibility to engage in the special

¹¹⁹ See ECtHR, *S. and Marper v. United Kingdom*, 2008, § 120-125.

¹²⁰ See Constitutional Court 21 December 2004, n° 202/2004, B.23.1 to B.23.3.

¹²¹ See Constitutional Court 19 July 2007, n° 105/2007, B.17.2 to B.17.8. In the absence of a minimum degree of protection to which citizens are entitled under the rule of law in a democratic society, the ECtHR found however

investigation techniques of observation, infiltration and informant employment, enlarged by the 2005 Reparation Act to investigations regarding irregularities in the execution of criminal sentences (for example, to find a fugitive), was found unconstitutional, as no independent and impartial judge can control the application during such investigations.¹²² Below, the keeping of observation and infiltration data (which are special investigation techniques themselves) in confidential records will be discussed more profoundly.

Apart from these issues, the application of certain techniques concerning the gathering or treatment of information can in themselves form an interference with due process rights: in that case, the interference with the right to a fair trial is not accessory to the technique (see examples above), but a direct consequence of the obtaining of information. Infiltration (or, when its conditions were not respected, incitement) is a clear example.

In addition, the European Court does not accept that article 6, guaranteeing due process, has no application to pre-trial proceedings. The reasonable time mentioned in paragraph 1, for instance, begins to run from the moment a charge comes into being, within the autonomous, substantive meaning to be given to that term; the Court has occasionally even found that a reasonable time has been exceeded in a case that ended with a discharge or at the investigation stage. Other requirements of article 6 may also be relevant before a case is sent for trial if and in so far as the fairness of the trial is likely to be seriously prejudiced by an initial failure to comply with them.¹²³ Often, the question about the admissibility during trial of the information obtained before is linked. The European Court is, in principle, reluctant to make a judgment about particular evidentiary issues when examining an alleged violation of article 6 ECHR, guaranteeing due process. It holds that the admissibility of evidence is primarily a matter for regulation by national law, and as a general rule, it is for the national courts to assess the evidence before them. The Court's task is rather to ascertain whether the proceedings as a whole, including the way in which evidence was taken, were fair.¹²⁴ Overall, as it will appear, there is a certain leniency towards due process restrictions when national security is at stake. But it is very limited, and including within the Court, not uncontroversial.

A. The inaccessibility of a confidential record

that even if citizens suffer little or no harm because the used technique did not serve as a basis for the prosecution, a violation of the Convention is conceivable. See ECtHR, *Huvig v. France*, 1990, § 35; ECtHR, *Kruslin v. France*, 1990, § 36.

¹²² See Constitutional Court 19 July 2007, n° 105/2007, B.7.3 to B.7.8.

¹²³ See e.g. ECtHR, *Imbrioscia v. Switzerland*, 1993, § 36.

¹²⁴ See ECtHR, *Van Mechelen and others v. Netherlands*, 1997, § 50; ECtHR, *Teixeira de Castro v. Portugal*, 1998, § 34; ECtHR, *Rowe and Davis v. United Kingdom*, 2000, § 62; ECtHR, *Eurofinacom v. France*, 2004; ECtHR, *Ramanauskas v. Lithuania*, 2008, § 52.

1. Jurisprudence of the Belgian Constitutional Court

In Belgium, the 2003 Act prescribes that observation and infiltration information has to be kept in a confidential record by the public prosecution. This information included the authorization to apply the techniques, the information that gives cause for that application, the names or descriptions of the persons targeted, the methods of application, the duration thereof, and the identity of the police officers conducting the research. Concerning infiltration, it contains equally the authorization given by the prosecutor to commit criminal acts and a report on each phase of the investigation (see sec. 47septies, 47octies, 47novies, and 47decies CCP). Initially, investigating magistrates had only access to the information if they ordered the application of the special techniques themselves or when they were in charge of the investigation, but they could not divulge the information therein. Other judges, the suspects or victims had no access.

This situation has been found unconstitutional. The Constitutional Court declared that the principle of equal arms between the prosecuting party and the defense, as is the contradictory character of the trial, including the procedure, are fundamental elements of the right to a fair trial.

“Hence, all evidence should be presented to the defense. Yet that right is not absolute. In some criminal procedures there can be contradictory interests, like national security, that necessitate to protect witnesses or keep investigation methods secret, that have to be balanced with the rights of the accused. In some cases it can be necessary to keep some elements of evidence secret for that party to safeguard the fundamental rights of other persons or a worthy general interest.”¹²⁵

With reference to *Edwards and Lewis vs. UK*, (see below) the Court then nevertheless struck that part of the 2003 Act, on the grounds that an interference with the rights of defense can only be justified if they are strictly proportionate to the goals they pursue and if they are compensated by a procedure allowing an independent and impartial judge to examine the legality of the procedure.¹²⁶

With the introduction of sec. 235ter CCP, the 2005 Reparation Act intended to resolve this problem. The indictment division of the Court of Appeals, ruling on procedural matters before trial on the merits, was designated to control the regularity of the confidential file on observation and infiltration actions. Considering that only that information of nature to endanger the protection of the executioners and the application of the investigation techniques are unavailable to the defense, through the procedure before the indictment division of the Court of Appeals, this measure is in accordance to the Constitution. The Court considered:

¹²⁵ See Constitutional Court 21 December 2004, n° 202/2004, B.27.6.

¹²⁶ See Constitutional Court 21 December 2004, n° 202/2004, B.26 to B.29.

“The will of the legislature to combat efficiently organized crime and the necessity for that goal to keep certain sensitive information secret, would be endangered if, for that kind of criminality, the accused, at the moment of control of the confidential file by the indictment division of the Court of Appeals, would have access to that file. It is not unreasonable to organize a procedure which differs from those for which secrecy is not necessary and in which the parties may consult all the pieces of the criminal file.”¹²⁷

Following the same reasoning, the fact that the hearing of the parties on the moment of control is settled separately, does not violate the Constitution. Referring to the *Jasper* case discussed below, the Court found that the parties have access to the criminal file and can conduct a meaningful defense. The right to a fair trial is therefore not violated.¹²⁸

The fact however that under the 2005 Reparation Act the decision of the indictment division of the Court of Appeals was not open for appeal to the Court of Cassation, was considered a violation of constitutional due process rights and cannot be justified only by reference to the importance of secrecy of the confidential file. The Court concluded:

“It is alleged furthermore that the protection of the confidential file is a higher interest and that no risk whatsoever may be taken, as notably the life of the infiltrators is at stake. Since any magistrate is held by professional secrecy, it is not justified that the Court of Cassation is denied access to a file that is under control of the indictment division of the Court of Appeals, as the confidentiality of that file can be guaranteed in both courts in the same way.”¹²⁹

The gap in the legislation was repaired by the Act of 16 January 2009, providing appeal to the Court of Cassation.

2. Jurisprudence of the European Court of Human Rights

According to the European Court, it is a fundamental aspect of the right to a fair trial that criminal proceedings, including the elements of such proceedings which relate to procedure, should be adversarial and that there should be equality of arms between the prosecution and the defense. The right to an adversarial trial means, in a criminal case, that both the prosecution and the defense must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party. In addition, article 6 requires that the prosecution authorities disclose to the defense all material evidence in their possession for or against the accused.

“However, the entitlement to disclosure of relevant evidence is not an absolute right. In any criminal proceedings there may be competing interests, such as national security or the need to protect witnesses

¹²⁷ Constitutional Court 19 July 2007, n° 105/2007, B.12.1 to B.12.5.

¹²⁸ See Constitutional Court 19 July 2007, n° 105/2007, B.14.1 to B.14.5.

¹²⁹ Constitutional Court 19 July 2007, n° 105/2007, B.16.3 to B.16.11. Note that according to the jurisprudence of the ECtHR, article 6 does not at itself contain a right to appeal.

at risk of reprisals or to keep secret police methods of investigating crime, which must be weighed against the rights of the accused (...).”¹³⁰

In some cases it may be necessary to withhold certain evidence from the defense so as to preserve the fundamental rights of another individual or to safeguard an important public interest. Nevertheless, only measures restricting the rights of the defense which are strictly necessary are permissible under article 6. Moreover, in order to ensure that the accused receives a fair trial, any difficulties caused to the defense by a limitation on its rights must be sufficiently counterbalanced by the procedures followed by the judicial authorities.¹³¹

The Court upholds that a procedure whereby the prosecution itself attempts to assess the importance of concealed information for the defense and weigh this against the public interest in keeping the information secret, cannot comply with the requirements of article 6. It is important that material relevant to the defense be placed before the trial judge for his ruling on questions of disclosure at the time when it can serve most effectively to protect the rights of the defense.¹³² In the *Jasper* case, the Court found that the fact that it was the trial judge, with full knowledge of the issues in the trial, who carried out the balancing exercise between the public interest in maintaining the confidentiality of the evidence and the need of the defendant to have it revealed, was sufficient to comply with article 6. The Court was satisfied that the defense were kept informed and permitted to make submissions and participate in the decision-making process as far as was possible without disclosing to them the material which the prosecution sought to keep secret on public interest grounds.¹³³ In the *Edwards and Lewis* case however, the Court drew the opposite conclusion. The applicants were denied access to the evidence, and it was not, therefore, possible for the defense representatives to argue the case in full before the judge. Moreover, the latter had already seen prosecution evidence which might have been relevant to the issue: it was the same judge that had to assess the necessity of secrecy who judged the case on the merits afterwards. The parties alleged that they were the victim of police incitement, so the judge’s appraisal of the evidence was essential to determine whether the prosecution could be continued.¹³⁴

In the *Rowe and Davis* case, the Court considered that a procedure before an appeal court about the disclosure of information is at itself not necessarily sufficient to remedy the unfairness caused at the trial by the absence of any scrutiny of the withheld information by the trial judge. Unlike the latter,

¹³⁰ ECtHR, *Jasper v. United Kingdom*, 2000, § 51.

¹³¹ See e.g. ECtHR, *Jasper v. United Kingdom*, 2000, § 51-52; ECtHR, *Rowe and Davis v. United Kingdom*, 2000, § 60-61; ECtHR, *Dowsett v. United Kingdom*, 2003, § 41-42; ECtHR, *Edwards and Lewis v. United Kingdom*, 2003, § 52-53.

¹³² See ECtHR, *Dowsett v. United Kingdom*, 2003, § 44 and 50.

¹³³ See ECtHR, *Jasper v. United Kingdom*, 2000, § 55-56.

¹³⁴ See ECtHR, *Edwards and Lewis v. United Kingdom*, 2003, § 58.

who is fully versed in all the evidence and issues in the case, appeal judges are sometimes dependent for their understanding of the possible relevance of the undisclosed material on transcripts of hearings and on the account of the issues given to them by prosecution. In addition, the first-instance judge is in a position to monitor the need for disclosure throughout the trial, assessing the importance of the undisclosed evidence at a stage when new issues are still emerging. In contrast, the Court of Appeal was obliged to carry out its appraisal *ex post facto*.¹³⁵

B. Infiltration and incitement

1. Jurisprudence of the Belgian Constitutional Court

Belgian law provides for a number of infiltration techniques the police can engage in during criminal investigations. They are described in an Order in Council of 9 April 2003 and include diverse forms of false sale, controlled delivery and front stores.¹³⁶ Undercover operations can in principle only be carried out by police officers, but exceptionally, civilian experts can be engaged as well (sec. 47*octies*, §1 CCP). Infiltration is only possible if there are serious clues that the suspect has committed crimes in the context of a criminal organization or a number of specific, serious crimes (see the telephone tapping list above). It can be organized by the prosecution. The bill concerning the Security of State for its part provides the possibility to set up or use corporations to support operational activities, and the deployment of officers under the cover of a fictitious identity or capacity (new sec. 18/2, §2, 3° and sec. 18/13 of the 1998 Act).

In order to distinguish legal infiltration from illegal incitement actions, the 2003 Act provided for a specific (and restrictive) definition of incitement. It was found unconstitutional, however, because it created the possibility for a discrimination with regard to the consequences of acts of incitement between those persons with regard to whom the 2003 Act was applied, and those to whom common criminal law was applied, including a general definition of incitement.¹³⁷ The 2005 Reparation Act resolved the problem by defining incitement (and as consequence the nullity of the proceedings) for all criminal law, and not just in the application of special investigation techniques. That solution was held constitutional.¹³⁸

¹³⁵ See ECtHR, *Rowe and Davis v. United Kingdom*, 2000, § 65.

¹³⁶ *Official Journal* 12 May 2003. The fact that the legislature has delegated the power to determine what specific techniques the police can engage in within the framework of an infiltration to the executive (in order to be able to adapt them efficiently to evolutions in the field), was not considered unconstitutional. See Constitutional Court 21 December 2004, n° 202/2004, B.7.1 to B.7.3.

¹³⁷ See Constitutional Court 21 December 2004, n° 202/2004, B.10.1 to B.11.

¹³⁸ See Constitutional Court 19 July 2007, n° 105/2007, B.4.1 to B.4.4.

Apart from infiltration in the strict sense, the 2005 Reparation Act (sec. 47*decies*) provided with regard to informants (police officers and civilians alike) the possibility commit crimes under certain conditions. Any such possibility was considered unconstitutional however, in so far as it involves the permission to violate the physical integrity of other persons. Equally, the fact that the technique could be ordered not only during investigations of terrorism or humanitarian law related crimes, but also during investigations of any serious crime committed in connection with a criminal organization, deprived it of its exceptional character and violated sec. 12 of the Constitution, prescribing that any criminal prosecution has to be foreseeable. Furthermore, the absence of indications of the consequences the permission to commit a crime has for the criminal situation of the informant (violation of sec. 10 and 11 of the Constitution), and the impossibility for an independent and impartial judge to exercise control over the application of the technique (sec. 10 and 11 of the Constitution *juncto* article 6 ECHR), rendered the provision unconstitutional on several other accounts as well.¹³⁹ The pending bill provides with regard to the Security of State equally the possibility to commit criminal acts, whenever they are strictly necessary for the efficiency of their assignment or to insure their own or other persons' safety. Additional condition is that these acts can only take place when engaging in certain specific intelligence activities, not in all. The criminal acts committed have to be proportionate to their goal and may not affect other persons' physical integrity. Preceding and express consent of the supervising commission is necessary (new sec. 13/1 of the 1998 Act).

2. Jurisprudence of the European Court of Human Rights

The European Court at its turn has observed the difficulties inherent in the police's task of searching for and gathering evidence for the purpose of detecting and investigating offences. To perform this task, they are increasingly required to make use of undercover agents, informers and covert practices, particularly in tackling organized crime and corruption. The Court noted that the use of special investigative methods – in particular, undercover techniques – cannot in itself infringe the right to a fair trial. However, on account of the risk of police incitement entailed by such techniques, their use must be kept within clear limits.¹⁴⁰ In the *Lüdi* case, the Court found that the sending of an undercover agent into what was thought as to be a large criminal network does not interfere with the right to privacy of the suspects. A suspect who is aware that he is engaged in a criminal act, should equally be aware that he is consequently running the risk of encountering an undercover police officer whose task is in fact to expose him.¹⁴¹ The use of undercover agents must be restricted, however, and safeguards put in place. While the rise in organized crime undoubtedly requires that appropriate measures be taken, states the Court, the right to a fair administration of justice nevertheless holds such a prominent

¹³⁹ See Constitutional Court 19 July 2007, n° 105/2007, B.8.5 to B.8.22.

¹⁴⁰ See ECtHR, *Ramanauskas v. Lithuania*, 2008, § 49-51.

¹⁴¹ See ECtHR, *Lüdi v. Switzerland*, 1992, § 40.

place that it cannot be sacrificed for the sake of expedience. In the *Teixeira de Castro* case, the Court concluded that the public interest cannot justify the use of evidence obtained as a result of police incitement, as to do so would expose the accused to the risk of being definitively deprived of a fair trial from the outset.¹⁴²

Crucial in the *Lüdi* case, for example, was the determination that the police officer concerned had been sworn in, the investigating judge had not been unaware of his mission and that the authorities had opened a preliminary investigation. By doing so, the police officers' role had been confined to acting as an undercover agent. That was not the case in *Teixeira*. The fact that the authorities have "good reason to suspect" the defendant of having a propensity to commit an offence would tend to suggest that an operation is more akin to "infiltration" than "instigation". As the government did not provide evidence to support that the applicant was predisposed to commit offences, the Court concluded that

"the police officers did not confine themselves to investigating Mr. Teixeira de Castro's criminal activity in an essentially passive manner, but exercised an influence such as to incite the commission of the offence."¹⁴³

In that connection, suspicion must be based on concrete evidence showing that initial steps have been taken to commit the acts constituting the offence for which the defendant is subsequently prosecuted. The Court holds that police officers act only as undercover agents in such circumstances, since significant steps preparatory to the commission of the offence had been taken before their participation in the investigation.¹⁴⁴ The Court also checks whether there is evidence indicating that, without such intervention, the offence would not have been committed.¹⁴⁵ In any event, it falls to the prosecution to prove that there was no incitement, provided that the defendant's allegations are not wholly improbable. In the absence of any such proof, it is the task of the judicial authorities to examine the facts of the case and to take the necessary steps to uncover the truth in order to determine whether there was any incitement. The criminal courts must carry out a careful examination of the material in the file, since for the trial to be fair within the meaning of article 6, all evidence obtained as a result of police incitement must be excluded.¹⁴⁶

¹⁴² See e.g. ECtHR, *Teixeira de Castro v. Portugal*, 1998, § 35-36; ECtHR, *Vanyan v. Russia*, 2005, § 46-47; ECtHR, *Ramanauskas v. Lithuania*, 2008, § 54.

¹⁴³ See e.g. ECtHR, *Teixeira de Castro v. Portugal*, 1998, § 36-38; ECtHR, *Eurofinacom v. France*, 2004.

¹⁴⁴ See ECtHR, *Sequiera v. Portugal*, 2003.

¹⁴⁵ See ECtHR, *Eurofinacom v. France*, 2004.

¹⁴⁶ See e.g. ECtHR, *Khudobin v. Russia*, 2006, § 133-135; ECtHR, *Ramanauskas v. Lithuania*, 2008, § 60.