4-2010

Special Investigation Techniques, Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights

Toon Moonen
Hasselt University

PACE UNIVERSITY
SCHOOL OF LAW

INTERNATIONAL LAW REVIEW
ONLINE COMPANION

Volume 1, Number 9 April 2010

SPECIAL INVESTIGATION TECHNIQUES, DATA PROCESSING AND PRIVACY PROTECTION IN THE JURISPRUDENCE OF THE EUROPEAN COURT OF HUMAN RIGHTS

Toon Moonen, Assistant Professor, Hasselt University

The search for a balance between the duty of government to safeguard its citizens and the individual rights of those protected is a constant struggle. One of the key ways in which government engages in national security protection is by information gathering. National security is by definition a responsive activity – that is, a government must anticipate before, or react after someone else has taken some kind of threatening action. Because of this, acquiring information about other people's doings is essential. Most certainly through technological advancement at the end of the 20th and beginning of the 21st century, information gathering has become a booming governmental business. Never before were so many opportunities to learn things about persons or events and the means to process those data more available. As a consequence, governments adopt information gathering policies and introduce legislation by which its agents have to abide, but which can also offer specific techniques to do their jobs.

The flip side of the coin is that we have to adapt to the fact that

there is a substantial amount of information available out there, including information about our private lives – information we would sometimes like no one else to have. In general, societies directed by the rule of law consider that governments should only gather information about us when it is useful to reach a goal more important than our personal right to be the manager of what gets known about us. Even then, it is accepted that the government cannot route through such information in any way, and at any cost. A balance, therefore, must be sought between these conflicting interests. In the last decades the issue has become more precarious: today information is more abundantly available than ever, and societies and their governments are faced with wider and more differentiated security threats. Finding the difficult balance between our rights to collective protection and the right to individual freedom to live without governmental interference is a complicated matter which continues to evolve.

In what follows, the special information gathering techniques that a government can or cannot engage in when national security is at stake are discussed. They are examined primarily from a privacy point of view, but some of the techniques also raise due process questions. More specifically, the way these issues are dealt with in Europe will be discussed. The European continent has a long and outstanding history of human rights protection through the application of the 1950 European Convention on Human Rights ("ECHR"), the key treaty adopted by the Members States of the Council of Europe (not to be confused with the European Union), which has gradually assumed the role of a pan-European Bill of Rights. Logically, the jurisprudence of its jurisdictional body, the European Court of Human Rights ("ECtHR" or "the Court"), will be at the center of the discussion. It is not the intention of this contribution to provide a detailed analysis of the pro's and con's of its views, but it may provide a first look at how the Court, confronted with national security issues, deals with the protection of certain basic fundamental rights. First, the phenomenon of governments acting in secret will be illustrated (*infra* Part I). Second, the Council of Europe's political framework on special investigation techniques (*infra* Part II) and the legal principles regarding special investigation techniques and fundamental rights (*infra* Part III) are analyzed. The principles of legal certainty, judicial control on government action, subsidiarity and proportionality are key elements to the issue of privacy protection. An examination of a number of special investigation techniques interfering with the right to privacy (*infra* Part IV) and the right to a fair trial (*infra* Part V) will be made, before coming to some general conclusions (*infra* Part VI).

I. GOVERNMENTS ACTING IN SECRET

In general, different types of government agents may want to engage in the gathering of information. They are usually not all competent to do so, though. For example, there are limits on the methods tax services can engage in to get information on your assets. When national security is involved, or when a serious crime has been committed, there are often special investigation techniques available to specific government agencies, whether they be a specialized part of the police force or an intelligence agency. According to the Commission for Democracy Through Law,[1] which is the Council of Europe's advisory body on constitutional matters, there seem to be two schools of thought on the question of how those 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 specialised branches of the general police force."[2]

As a consequence, it is not always possible to treat the police forces and intelligence services separately. The position of organs with special investigation capacities within government depends on 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.[3] Any preventive or enforcement functions lie then with the ordinary police or other organs of law enforcement. 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 ordinary police, the security service police officers are allowed to perform the same acts as other police officers, . . ." like tapping telephones.[4]

Evidently, it is important to define the notion "special investigation

---

[1] Generally referred to as the "Venice Commission."

[2] Council of Europe, Venice Comm'n., *Report: Internal Security Services in Europe*, 34th Plenary meeting, CDL-INF006 (1998), *available at* http://www.venice.coe.int/docs/1998/CDL-INF(1998)006-e.asp [hereinafter Venice Commission Report].

[3] *Id.* at 9.

[4] *Id.*

technique." However, there does not seem to be a generally accepted legal definition. In any case, certain elements are identifiable. For example, 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 knew his telephone was wiretapped, one can reasonably assume that he would not plan further crimes by phone. As the Venice Commission noted, internal security organizations, or police in general, are in many cases free from outside administrative interference.[5] That freedom from outside supervision may keep the activities in question rather effectively free from surveillance by the media, the general public, and 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."[6]

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. These techniques do not just conceal information; they add false information to the case. The core of these techniques 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.

II. COUNCIL OF EUROPE POLITICAL FRAMEWORK REGARDING SPECIAL INVESTIGATION TECHNIQUES

Among the Council of Europe's political bodies, the Committee of Ministers (*infra* Part A) and the Parliamentary Assembly (*infra* Part B), have issued a number of guidelines to the Member States concerning special investigation techniques and guaranteeing fundamental rights.

A. The Committee of Ministers

In 2005, the Council of Europe, through its Committee of Ministers, made a recommendation to the Member States on special investigation

---

[5] *Id.* at 10.
[6] *Id.*

techniques relating 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 ECtHR in particular. In the Council of Europe's 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, aim[ed] at gathering information in such a way as not to alert the target persons."[7]

The Committee observed that special investigation techniques are numerous, varied, and constantly evolving and that their common characteristics are their secret nature and that their application could interfere with fundamental rights and freedoms.[8] 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 also pointed out that the "use of special investigation techniques in criminal investigations requires confidentiality and that . . . the commission of serious crime, including acts of terrorism should, wherever appropriate, be thwarted with secured covert means of operation."[9]

Three general principles are formulated: (1) Member States should, in accordance with the requirements of the European Convention on Human Rights, define in their national legislation the conditions under which the authorities are empowered to resort to special investigation techniques; (2) define when this is considered necessary in a democratic society and is considered appropriate for efficient criminal investigation and prosecution; and (3) Member States should "ensure adequate control of the implementation of special investigation techniques by judicial authorities or other independent bodies through prior authorisation [and]

---

[7] Council of Europe, Comm. of Ministers, *Recommendation: Special Investigation Techniques in Relation to Serious Crimes Including Acts of Terrorism*, 2, Rec(2005)10 (Apr. 20, 2005), *available at* https://wcd.coe.int/ViewDoc.jsp?id=838445&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864 [hereinafter Committee of Ministers, *Recommendation*].

[8] *Id.* at 1-2.

[9] *Id.* at 7.

supervision during the investigation or ex post facto review."[10]

Many of these conditions of use proposed by the Committee, as will be shown below, are part of the review process of the ECtHR. The Committee noted 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 unidentified individual or group of individuals. Proportionality between the effects of the use of special investigation techniques and the objective that has been identified is essential. In this respect, an evaluation should be made in light of the seriousness of the offense and the intrusive nature of the specific special investigation technique used. Furthermore, Member States need to ensure that their authorities apply less intrusive methods if such methods enable the offence to be detected, prevented or prosecuted with adequate effectiveness. This principle adds a condition of subsidiarity. Member States are equally required to "take appropriate legislative measures to permit the production of evidence gained from the use of special investigation techniques" in court, in order to "safeguard the rights of the accused to a fair trial."11

B. The Parliamentary Assembly

In 1998, the Venice Commission issued 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).[12] It found that:

> [U]ndoubtedly, 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.[13]

The Venice Commission recalled that internal security services have in-

---

[10] *Id*. at 8.
[11] *Id.* at 9.
[12] Venice Commission Report, *supra* note 2.
[13] *Id.* at 4.

bred in them a potential for the abuse of State power – as the Commission pointed out, there have been innumerable incidences of the most serious violations of human rights committed in the name of internal security.[14] "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.[17] "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 responses by the services of the security sector, preferably co-ordinated and overseen on a European level."[18] With regard to the security sector, the Council of Europe recommended a general framework, including the following principles: (a) the functioning of intelligence services must be based on clear and appropriate legislation supervised by the courts; (b) each parliament should have an appropriately functioning specialized committee; (c) conditions for the use of exceptional measures by these services must be laid down by the law in precise limits of time; and (d) 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 need to be prescribed by law.[19] In addition, confidentiality and accountability interests can be managed through the principle of deferred transparency, that

---

[14] *Id.*

[15] *Id.*

[16] *Id.* at 20.

[17] Eur. Consult. Ass. Deb., 23rd Sess. 1713 (June 23, 2005), *available at* http://assembly.coe.int/Documents/AdoptedText/ta05/EREC1713.htm [herein-after Parliamentary Assembly Resolution].

[18] *Id.*

[19] *Id.*

is, by declassifying confidential material after a period of time prescribed by law. Finally, the PACE considered that parliament must be kept regularly informed about changes which could affect the general intelligence policy.[20]

With regard to the police forces, the Council recommended that (a) in each State a specific legal framework for the functioning and supervision of a democratic police force must be set up; (b) given their different mandate and competences, it is considered important that legislation distinguishes between security and intelligence services on the one hand, and law enforcement agencies on the other; (c) the police must remain neutral and not be subject to any political influence; and (d) 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).[21] The PACE 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 should not seriously hamper the exercise of fundamental constitutional rights."[22]

III. ECtHR General Principles Regarding Special Investigation Techniques

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, however, 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.[23]

---

[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] Venice Commission Report, *supra* note 2, at 6.

For all Member States, the ECHR, in Article 8, provides that everyone has the right to respect for his private and family life, his home, and his correspondence.[24] Any interference by a public authority with the exercise of this right is prohibited:

> [E]xcept 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.[25]

Furthermore, in the words of the European Court of Human Rights:

> [T]his 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.[26]

Once an interference with a fundamental right is established (*infra* Part A), it can only be considered legitimate if the measure is in accordance with the law (*infra* Part B), serves a legitimate goal and is necessary in a democratic society (*infra* Part C).

A. The Existence of an Interference

In general, the Court interprets the notion of "interference" in the context of privacy rather widely. The Court in *Klass v. Germany* determined that an individual could submit an application concerning secret surveillance measures, without being able to point to any concrete measure specifically affecting him. The Court held that:

> [I]f 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

---

[24] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8 ¶ 1, Nov. 1, 1998, 213 U.N.T.S. 222, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm.

[25] *Id.* ¶ 2.

[26] Klass v. Germany, App. No. 5029/71, 2 Eur. H.R. Rep. 214 ¶ 42 (1980).

> 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.[27]

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 in itself amounts to an interference with Article 8.[28] As will be shown with more detail in *infra* Part IV, however, some government actions do not self-evidently amount to an interference.

B. Measure in Accordance with the Law

In the analysis of the Court, for a measure to be in accordance with the law, it should be foreseeable (*infra* Part 1), it should be accompanied by safeguards against abuse (*infra* Part 2), and control tools should be provided (*infra* Part 3).

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 domestic law, but that it also refer to the quality of the law in question. Referring to the quality of the law requires that a measure should be compatible with the rule of law, accessible to the person concerned, and foreseeable as to its effects.[29]

---

[27] *Klass*, 2 Eur. Ct. H.R. ¶ 34; *see, e.g.*, Liberty v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. ¶ 56 (2008); Iordachi v. Moldova, App. No. 25198/02, Eur. Ct. H.R. ¶ 30 (2009).

[28] *See, e.g.*, Ass'n for Eur. Integration and Human Rights v. Bulgaria, App. No. 62540/00, Eur. Ct. H.R. ¶ 69 (2007).

[29] *See* Malone v. United Kingdom, App. No. 8691/79, 7 Eur. H.R. Rep. 14 ¶¶ 66-67 (1984); Leander v. Sweden, App. No. 9248/81, 9 Eur. H.R. Rep. 433 ¶¶ 50-51 (1987); Huvig v. France, App. No. 11105/84, Eur. H.R. Rep. ¶ 29 (1990); Kruslin v. France, App. No. 11801/85, Eur. H.R. Rep. ¶ 30 (1990); Kopp v. Switzerland, App. No. 23224/94, Eur. H.R. Rep. ¶¶ 63-64 (1998); Valenzuela Contreras v. Spain, App. No. 27671/95, Eur. H.R. Rep. ¶ 46 (1998); Amann v. Switzerland, App. No. 27798/95, Eur. Ct. H.R. ¶¶ 50-56 (2000); Rotaru v. Romania, App. No. 28341/95, Eur. Ct. H.R. ¶ 55 (2000); Doerga v. Netherlands, App. No. 51210/99, Eur. Ct. H.R. ¶ 45 (2004); Antunes Rocha v. Portugal, App. No. 64330/01, Eur. Ct. H.R. ¶¶ 66-67; Van der Velden v. Netherlands, App. No. 29514/05, Eur. Ct. H.R. ¶ 2 (2006); Weber v. Germany, App. No. 54934/00, Eur. Ct. H.R. ¶ 93 (2006); Dumitru Popescu v. Romania, App. No. 71525/01, Eur. Ct. H.R. ¶ 61

In the jurisprudence of the Court, "foreseeable" means that a rule is formulated with sufficient precision to enable any individual to regulate his conduct, if necessary after taking advice. In addition, the phrase implies that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities. The Court has noted in various cases that the risk of arbitrariness is especially evident when a power of the executive is exercised in secret.[30] Obviously, in the context of secret surveillance measures, the requirement of foreseeability cannot mean that an individual know 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."[31]

2. Safeguards Against Abuse

In addition, adequate and effective safeguards against abuse must exist. 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."[32] In the *Klass* case of 1978, which was the earliest landmark judgment, the Court noted that it:

> [M]ust 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 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.[33]

(2007); Ass'n for Eur. Integration and Human Rights v. Bulgaria, App. No. 62540/00, Eur. Ct. H.R. ¶ 71 (2007); Liberty v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. ¶¶ 59-62 (2008); S. v. United Kingdom, App. No. 30562/04, Eur. Ct. H.R. ¶ 95 (2008); Bykov v. Russia, App. No. 4378/02, Eur. Ct. H.R. ¶ 76 (2009); Iordachi v. Moldova, App. No. 25198/02, Eur. Ct. H.R. ¶¶ 37-39 (2009).

[30] *See* cases cited *supra* note 29.

[31] Khan v. United Kingdom, App. No. 35394/97, Eur. Ct. H.R. ¶ 26 (2000) (quoting Malone v. United Kingdom, App. No. 8691/79, 7 Eur. H.R. Rep. 14 ¶ 67 (1984)).

[32] *Klass*, 2 Eur. Ct. H.R. 214 ¶ 49.

[33] *Id.* ¶ 50.

The Court then found a number of legal limitations to be in accordance with Article 8 of the ECHR. 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. Among other requirements, 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. Exploratory or general surveillance was not permitted by the contested legislation. Under the same legislation, the Court found that 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.[34] Accordingly, "there exist[ed] an administrative procedure designed to ensure that measures were not ordered haphazardly, irregularly or without due and proper consideration."[35]

Starting with *Klass* at the end of the 1970s, the Court has steadily outlined a number of general principles regarding State responsibility regarding secret surveillance measures. In recent cases, the Court has grown more exigent on the quality of the law, emphasizing its effectiveness in practice, rather than its theoretical merits. For example, the Court determined in the 2000 *Rotaru* case against Romania that although data on citizens may be gathered, recorded and archived, the kind of information gathered has to be defined, as well as the categories of people that may be subjected to it, the circumstances that warrant surveillance, and the procedure that needs to be followed.[36] The framework in existence and its application at the time was deemed largely incomplete.[37]

Overall, the Court, through its case-law on secret measures of surveillance, has developed a set of minimum safeguards that should be statutorily introduced in order to avoid abuses of power. The safeguards should include: the nature of the offenses that may give rise to a surveillance order; categories of people liable to be subject 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 destroyed.[38] Finally, "the body is-

---

[34] *Id.* ¶ 51.
[35] *Id.*
[36] *See* Rotaru v. Romania, App. No. 28341/95, 8 Eur. Ct. H.R. 449 ¶¶ 57-58 (2000).
[37] *Id.* ¶¶ 62-63.
[38] Iordachi v. Moldova, App. No. 25198/02, Eur. Ct. H.R. ¶ 39 (2009) (quoting *We-*

suing 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."[39]

With regard to who should design that 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.[40]

The Venice Commission reached the same conclusion, stating:

> [T]he 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.[41]

3. Control of Surveillance

The Venice Commission concluded that legislative control over the

---

ber, Eur. Ct. H.R. ¶ 95). *See* Huvig v. France, App. No. 11105/84, Eur. H.R. Rep. ¶ 34 (1990); Kruslin v. France, App. No. 11801/85, Eur. H.R. Rep. ¶ 35 (1990).

[39] *Iordachi*, App. No. 25198/02, Eur. Ct. H.R. ¶ 40 (quoting *Dumitru Popescu*, Eur. Ct. H.R. ¶¶ 70-73); *see* Valenzuela Contreras v. Spain, App. No. 27671/95, 28 Eur. H.R. Rep. 483 ¶ 46 (1998); Ass'n for Eur. Integration and Human Rights v. Bulgaria, App. No. 62540/00, Eur. Ct. H.R. ¶¶ 76-77 (2007); Liberty v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. ¶ 62 (2008).

[40] Malone v. United Kingdom, App. No. 8691/79, 7 Eur. Ct. H.R. ¶ 68 (1984); Leander v. Sweden, App. No. 9248/81, 9 Eur. H.R. Rep. ¶ 51 (1987); Amann v. Switzerland, App. No. 27798/95, Eur. Ct. H.R. ¶ 56 (2000); *Rotaru*, App. No. 28341/95, Eur. Ct. H.R. ¶ 55 (2000); Liberty v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. ¶ 62 (2008). The Court pointed out the same for delegation to the judiciary. *See* Huvig v. France, App. No. 11105/84, Eur. H.R. Rep. ¶ 29 (1990); Kruslin v. France, App. No. 11801/85, Eur. H.R. Rep. ¶ 30 (1990); Weber v. Germany, App. No. 54934/00, Eur. Ct. H.R. ¶ 93 (2006); Bykov v. Russia, App. No. 4378/02, Eur. Ct. H.R. ¶ 78 (2009); Iordachi, App. No. 25198/02, Eur. Ct. H.R. ¶¶ 39 (quoting *Weber*, Eur. Ct. H.R. ¶ 94).

[41] Venice Commission Report, *supra* note 2, at 20.

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.[42] Important issues are: an actor's competence to exercise that control (*Infra* Part a); the way the control process should be conducted before and during the surveillance measure (*Infra* Part b); and possibilities of a citizen to question the legality of a surveillance measure afterwards (*Infra* Part c).

a. Control Actors

In general, the European Court considers that in a field where abuse is potentially so easy and could have such harmful consequences for democratic society, it is in principle desirable to entrust supervisory control to a judge.[43] The Venice Commission equally promotes judicial control.[44] The rights of individuals cannot be adequately protected if the acts of such institutions are not made susceptible to judicial review.

> [W]hereas 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.[45]

Nevertheless, the European Court admitted that 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," are acceptable as well. The Court emphasized its democratic character, "which can be reflected in a balanced membership of the parliamentary board." In those circumstances, such supervisory bodies may "be regarded as enjoying sufficient independence to give an objective ruling."[46] In the *Leander* case of 1987, the Court repeated that it:

> [A]ttaches particular importance to the presence of parliamentarians on the

---

[42] *Id.* at 6.
[43] Klass v. Germany, App. No. 5029/71, 2 Eur. H.R. Rep. 214 ¶ 56 (1980).
[44] Venice Commission Report, *supra* note 2, at 11-13.
[45] *Id.* at 25.
[46] *Klass*, 2 Eur. Ct. H.R. ¶ 56.

> 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.[47]

The Venice Commission on its turn noticed the existence of supplemental parliamentary supervision.[48]

An overall control over the system of secret surveillance being entrusted to the executive, such as the Minister of Internal Affairs, and not to independent bodies, is not acceptable to the Court.[49] 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."[50] Nevertheless, fundamental freedoms can never be properly guaranteed if domestic security surveillances are 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.[51]

b. A Priori and Ad Hoc Control

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

---

[47] Leander v. Sweden, App. No. 9248/81, 9 Eur. H.R. Rep. 433 ¶ 65 (1987).

[48] Venice Commission Report, *supra* note 2, at 14.

[49] Ass'n for Eur. Integration and Human Rights v. Bulgaria, App. No. 62540/00, Eur. Ct. H.R. ¶ 87 (2007).

[50] Venice Commission Report, *supra* note 2, at 14.

[51] Venice Commission Report, *supra* note 2, at 20.

terminated. The Court stated that in the first two stages, the very nature and logic of secret surveillance dictate that the surveillance and the accompanying review should take place 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(2), are not to be exceeded.[52]

According to the Court, the rule of law implies that an interference with an individual's rights by the executive authorities should be subject to an effective control, assured by the judiciary – at least in the last resort. Judicial control offers the best guarantee of independence, impartiality, and a proper procedure.[53] In the analysis of the Venice Commission, the fact that many intelligence gathering actions are carried out clandestinely, makes it impractical to rely on judicial control at the initiative of the person who has been the target of an operation of the security services.[54] The Venice Commission stated further:

> 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.[55]

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. As an overriding principle:

> [T]he courts should have jurisdiction to determine whether the actions complained of were within the powers and functions of the internal security

---

[52] *Klass*, 2 Eur. Ct. H.R. ¶ 55.

[53] Rotaru v. Romania, App. No. 28341/95, 8 Eur. H.R. Rep. 449 ¶ 59 (2000). In the *Antunes Rocha* case, the Court reiterated this idea, omitting however the reference to the judiciary as key player. Antunes Rocha v. Portugal, App. No. 64330/01, Eur. Ct. H.R. ¶ 76 (2005).

[54] Venice Commission Report, *supra* note 2, at 13.

[55] *Id.*

> 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.[56]

In the view of the ECtHR:

> [A]s 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.[57]

One of the questions the Court already had to answer is whether it is feasible in practice to require subsequent notification in all cases. Obviously, the activity or danger against which a particular series of surveillance measures is directed may continue after the suspension of those measures. In the opinion of the Court, subsequent notification to each individual affected might well jeopardize the long-term purpose that originally prompted the surveillance.[58] 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 in *Klass* was that not informing the individual once surveillance has ceased cannot itself be incompatible with Article 8 of the ECHR.[59] However, in the 2008 *Ekimdzhiev* case the Court ruled that legislation excluding such notification in any case and at any time (for reasons of classification of information), is intolerable.[60] Legislation excluding notification would mean that a target of surveillance may be unable to seek redress for unlawful interferences with the Article 8 rights; the person would not know that they had been monitored unless there was a leak of information or the person was subsequently prosecuted

---

[56] *Id.*

[57] *Klass*, 2 Eur. Ct. H.R. ¶ 57.

[58] *Id.* ¶ 58.

[59] *Id.*

[60] Ass'n for Eur. Integration and Human Rights v. Bulgaria, App. No. 62540/00, Eur. Ct. H.R. ¶ 93 (2007).

based on the gathered information.[61]

C. Measures 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.[62] The measures, however, must also be necessary in today's democratic society. The Court emphasized that, "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."[63]

In accordance to settled case-law, 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."[64] The Venice Commission, having accepted that the unorthodox means by which internal security services must be allowed to operate can have a negative effect, [65] stated:

> [I]t is imperative that these extraordinary measures and restrictions of fundamental rights and liberties should be proportionate to the danger involved. 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

---

[61] *Id.* ¶ 91.

[62] Article 8 ¶ 2 of the ECHR provides the possibility to restrict privacy in the interest 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. European Convention on Human Rights, art. 8 ¶ 2, Sept. 3, 1953, 213 U.N.T.S. 222, *available at* http://actrav.itcilo.org/actrav-english/telearn/glo-bal/ilo/law/coeprot.htm#Article%208.

[63] *Klass*, 2 Eur. Ct. H.R. ¶ 42; *see also* Rotaru v. Romania, App. No. 28341/95, 8 Eur. Ct. H.R. 449 ¶ 47; Antunes Rocha v. Portugal, App. No. 64330/01, Eur. Ct. H.R. ¶ 66 (2005).

[64] *See, e.g.*, Observer and Guardian v. United Kingdom, App. No. 13585/88, Eur. Ct. H.R. ¶59 (1991); Sunday Times v. United Kingdom, App. No. 13166/87, Eur. Ct. H.R. ¶ 50 (1991); Jersild v. Denmark, App. No. 15890/89, Eur. Ct. H.R. ¶ 31 (1994). In relation to Article 8, *see, e.g.*, Hertel v. Switzerland, App. No. 25181/94), Eur. Ct. H.R. ¶ 46 (1998); S. v. United Kingdom, App. No. 30562/04, Eur. Ct. H.R. ¶ 101 (2008).

[65] Venice Commission Report, *supra* note 2, at 26.

> manner as long as the danger their action is meant to prevent persists and with the minimum involvement for a definite and determinate purpose.[66]

While the national authorities 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, either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider."[67]

Occasionally, the Court considers not only the qualitative aspects of legislation, but also statistical evidence, such as 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 actions were used in criminal proceedings afterwards, and so on. For example, the Court noted in the *Ekimdzhiev* case that:

> [M]ore 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 Minster 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

---

[66] *Id.*

[67] S., App. No. 30562/04, Eur. Ct. H.R. ¶ 102.

> 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.[68]

As mentioned above, the Court previously held with regard to secret surveillance that national authorities enjoyed a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security.[69] The criteria concerning foreseeability, safeguards and control seem to indicate, however, that today this margin has become limited. In some national security cases not relating to Article 8, the Court considers that there is no margin of appreciation at all.[70]

IV. SPECIAL INVESTIGATION TECHNIQUES INTERFERING WITH THE RIGHT TO PRIVACY

When it comes to privacy, it is inherent to the nature of the privacy reducing measures that national security may not have been affected yet. 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, or at least made credible, by facts. In what follows, a number of investigation techniques are examined in more detail. These involve systematic or intensified observations (*infra* Part A), the interception and opening of mail correspondence (*infra* Part B), the identification, tracking and wiretapping of telecommunication (*infra* Part C), and the keeping of data (*infra* Part D). The last two techniques, to the application of which governments seem to be increasingly inclined, will be discussed with more attention. As explained above, every State has its own legal framework to organize the competences of the actors concerned.

A. Systematic or Intensified Observations

Within the ECHR framework, the justifiability of intensified observations depends on what particular actions have been undertaken. The

---

[68] Ass'n for European Integration and Human Rights v. Bulgaria, App. No. 62540/00, Eur. Ct. H.R. ¶ 92 (2008).

[69] *See* Leander v. Sweden, App. No. 9248/81, 9 Eur. H.R. Rep. 433 ¶ 59 (1987). *See also* Malone v. United Kingdom, App. No. 8691/79, 7 Eur. H.R. Rep. 14 ¶ 81 (1984).

[70] The Court has found, for example, that even when confronted with alleged terrorist activities, there is no margin of appreciation in the application of the principle of non-refoulement under Article 3 ECHR. *See* Chahal v. United Kingdom, App. No. 22414/93, 23 Eur. H.R. Rep. 413 (1996); *see also* Saadi v. Italy, App. No. 37201/06, Eur. Ct. H.R. (2008).

systematic retention of information regarding a person's whereabouts and doings must 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 (*infra* Parts C and D). Obviously, physically searching private dwellings or property constitutes a serious interference with a person's private life, and *a fortiori* when the person concerned is unaware. As always, the European Court attaches great importance to preceding judicial control.[71] In the *Murray* case, the Court found that:

> [I]t 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.[72]

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 offenses.[73] It opined that "[t]hese 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."[74]

Since there existed evidence resulting in a genuine and honest suspicion that the applicant committed a terrorist linked crime, the Court in *Murray* accepted that it was reasonable under the circumstances to search the target's house.[75] In general, the existence of specific legislation dealing with situations in which officers enter

---

[71] *See, e.g.*, Chappell v. United Kingdom, App. No. 10461/83, 12 Eur. H.R. Rep. 1 ¶ 59 (1989).

[72] Murray v. United Kingdom, App. No. 14310/88, 19 Eur. H.R. Rep. 193 ¶ 90 (1994).

[73] *Id.* ¶ 91.

[74] *Id.*

[75] *Id.* ¶ 92.

private places without conducting a normal house search is appropriate. With regard to cases involving 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 to gather information about serious crime and terrorism, they do not exceed their powers.[76]

In any case, authorities will have to be careful, even when conducting observations in a public environment. According to the ECtHR, 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 ignored that a person's private life may extend outside a person's home or private premises.[77] In the case of *P.G. and J.H. v. United Kingdom*, the Court added, however, 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.[78]

B. The Interception and Opening of Mail Correspondence

Obviously, the Court has dealt with protection of correspondence problems. In a national security context, it paid particular attention to the mail traffic between a prisoner and his attorney. In *Campbell*, the Court found that the prison authorities may open a letter:

> [W]hen 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

---

[76] Venice Commission Report, *supra* note 2, at 21.
[77] Perry v. United Kingdom, App. No. 63737/00, Eur. Ct. H.R. ¶ 36 (2003).
[78] P.G. v. United Kingdom, App. No. 44787/98, Eur. Ct. H.R. ¶ 57 (2001).

> 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.[79]

In the *Erdem* case, the Court accepted that it is necessary in a democratic society, for reasons of national security, to monitor the correspondence of prisoners specifically suspected of belonging to a terrorist organization. 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 obtained confidential."[80] For these reasons, the interference was considered falling in the margin of appreciation of the State.[81] 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.[82]

C. Identification, Tracking and Wiretapping of Telecommunication

Wiretapping is a very invasive investigation method because it allows police officers to listen to citizens' private conversations. It is no surprise that the issue has provoked a large number of applications to the Court, resulting in a rather differentiated analysis. In the *Klass* case mentioned above, the Court noted the technical advances made in the field of espionage and, correspondingly, of surveillance.[83] Most importantly, 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."[84]

For that reason, the Court accepted that the existence of legislation granting powers of secret surveillance of telecommunications is, under

---

[79] Campbell v. United Kingdom, Eur. Ct. H.R. (ser. A) 233 ¶ 48 (1992).
[80] Erdem v. Germany, App. No. 38321/97, Eur. Ct. H.R. ¶ 67 (2001).
[81] *Id.* ¶ 69.
[82] Venice Commission Report, *supra* note 2, at 21.
[83] *Klass*, 2 Eur. Ct. H.R. ¶ 48.
[84] *Id.*

exceptional conditions, a necessary evil.[85] The domestic legislature enjoys certain discretion; the Court does not consider itself to be a substitute for the assessment by the national authorities of what might be the best policy. Nevertheless the Court stressed that:

> [T]his 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.[86]

The principles regulating telephone tapping apply equally to the use of radio-transmitting devices, which are, in terms of the nature and degree of the intrusion involved, virtually identical to that of telephone tapping.[87] Not all telecom follow-ups, however, amount to such wiretapping. In the *Malone* case of 1984, the Court found that the registering of numbers dialed on a particular telephone, and the time and duration of each call by its very nature to be distinguished from the interception of communications, which is undesirable and illegitimate in a democratic society unless justified.[88] Hence, the measures taken in order to prevent arbitrariness are not under the same scrutiny as in cases of the 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."[89] The retention and use of data will be further discussed below (cf. *infra* Part D).

As a matter of principle, in the *Huvig* and *Kruslin* judgments of 1990, the Court considered that "[t]apping and other forms of interception of telephone conversations . . . must . . . be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated."[90] The domestic law must be sufficiently

---

[85] *Id.* ¶ 49.

[86] *Id.*

[87] Bykov v. Russia, App. No. 4378/02, Eur. Ct. H.R. ¶ 79 (2009).

[88] Malone v. United Kingdom, App. No. 8691/79, 7 Eur. H.R. Rep. 14 ¶ 84 (1985)

[89] *Id.*; *see, e.g.*, P.G. and J.H. v. United Kingdom, App. No. 44787/98, Eur. Ct. H.R. 550 ¶¶ 42-47 (2001).

[90] Huvig v. France, App. No. 11105/84, 12 Eur. H.R. Rep. 528 ¶ 32 (1990); Kruslin v. France, App. No. 11801/85, 12 Eur. H.R. Rep. 547 ¶ 33 (1990); Kopp v. Switzerland, App. No. 23224/94, 27 Eur. H.R. Rep. 91 ¶ 72 (1999); *See* Valenzuela Contreras v. Spain, App. No. 27671/95, 28 Eur. H.R. Rep. 483 ¶ 46 (1999); Liberty v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. ¶ 62 (2008) (quoting Weber v. Germany, App. No. 54934/00, Eur. Ct. H.R. ¶ 93 (2006)); Iordachi v. Moldova, App. No. 25198/02, Eur.

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 measures.[91] Nevertheless, and contrary to the legislation of some Member States, the proactive ordering of a telephone tap (before any crime is committed) is not necessarily a violation of Article 8 of the ECHR.[92] The Court noted in the *Lüdi* case that the tap was "aimed at the 'prevention of crime,'" and it had "no doubt as to its necessity in a democratic society."[93] According to the Court, to assess the legitimacy of a wiretap, a distinction has to be made between two stages of interception: the authorization of the measure (*infra* Part 1) and the control during the surveillance process (*infra* Part 2).[94]

1. Wiretap authorization

In the first stage, the following general conditions to justify secret surveillance must be fulfilled: (1) the applicable legislation should provide the nature of the offenses which may give rise to the tapping; (2) a definition of the categories of people possibly subject to the measure; (3) limits on its duration; (4) the procedure to be followed for examining, using and storing the data; (5) the precautions to be taken when communicating the data to others; and (6) the circumstances in which recordings or tapes are erased or destroyed.[95] 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 offenses which

---

Ct. H.R. ¶ 39 (2009) (quoting Weber v. Germany, App. No. 54934/00, Eur. Ct. H.R. ¶ 93 (2006)).

[91] *Iordachi*, App. No. 25198/02, Eur. Ct. H.R. ¶ 39 (quoting *Weber*, App. No. 54934/00, Eur. Ct. H.R. ¶ 93); *See Huvig*, 12 Eur. H.R. Rep. 528 ¶ 29; *Kruslin*, 12 Eur. H.R. Rep. 547 ¶ 30; *Kopp*, 27 Eur. H.R. Rep. 91 ¶ 64; Khan v. United Kingdom, App. No. 35394/97, Eur. Ct. H.R. ¶ 26 (2000) (quoting *Malone*, 7 Eur. H.R. Rep. 14 ¶ 67).

[92] The Belgian Code of Criminal Procedure, for example, does not allow it. Article 53 of the ECHR provides that nothing in the Convention "shall be construed as limiting or derogating from any of the human rights and fundamental freedoms which may be ensured under the laws of any High Contracting Party . . . ." As a consequence of this maximization clause, in principle, the more protective framework will be applied.

[93] Lüdi v. Switzerland, App. No. 12433/86, 15 Eur. H.R. Rep. 173 ¶ 39 (1992).

[94] *Iordachi*, App. No. 25198/02, Eur. Ct. H.R. ¶ 41; *see also* Ass'n for Eur. Integration & Human Rights v. Bulgaria, App. No. 62540/00, Eur. Ct. H.R. ¶ 84 (2007).

[95] *Huvig*, 12 Eur. H.R. Rep. 528 ¶ 34; *Kruslin*, 12 Eur. H.R. Rep. 547 ¶ 35; *Valenzuela Contreras*, 28 Eur. H.R. Rep. 483 ¶ 46; *see also Iordachi*, App. No. 25198/02, Eur. Ct. H.R. ¶ 39; Bugallo v. Spain, App. No. 58496/00, Eur. Ct. H.R. ¶ 30 (2003).

may give rise to such an order. The absence of an obligation to set a limit on the duration of telephone tapping, specifications of the procedure for creating 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 defence," is considered problematic.[96] According to the Court, "[t]he requirement that the effects of the 'law' [should] 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."[97]

Indeed, the Court stresses the value of a decision by an investigating judge or, for example, by the president of the indictment division of the court, who is an independent judicial authority.[98] Interceptions ordered only by the public prosecution, without any *a priori* control possibility by a judge, do not meet the required standards of independence.[99] "[T]he 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 authorising it."[100] The Venice Commission advised the same stating that a wiretap should only be installed when the judge is satisfied that there is imminent danger of a serious crime and that more routine methods of investigation would be unlikely to succeed.[101] Provisions should be made for the transcripts to be handed first to the judge, who then releases to the investigating services the portions that he deems relevant to the investigations being carried out.[102] As it appears, the so-called *"John Doe"* taps provided for in section 206 of the U.S. Patriot Act (expired in principle in 2009), being anonymous regarding either the person or the place monitored, would 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.

---

[96] *Id.*

[97] *Valenzuela Contreras*, 28 Eur. H.R. Rep. 483 ¶ 60.

[98] *See Huvig*, 12 Eur. H.R. Rep. 528 ¶ 33; *Kruslin*, 12 Eur. H.R. Rep. 547 ¶ 34; *Kopp* v. Switzerland, App. No. 23224/94, 27 Eur. H.R. Rep. 91 ¶ 72 (1999), 27 Eur. H.R. Rep. 91 ¶ 72; Amann v. Switzerland, App. No. 27798/95, Eur. Ct. H.R. ¶ 60 (2000).

[99] *Dumitru Popescu*, Popescu v. Romania, App. No. 71525/01, Eur. Ct. H.R. ¶¶ 70-73 (2007).

[100] *Iordachi*, App. No. 25198/02, Eur. Ct. H.R. ¶ 51.

[101] Venice Commission Report, *supra* note 2, at 21.

[102] *Id.*

2. Wiretap Control

With regard to the second stage, control over the surveillance should be put under control of a judge or another independent body.[103] In the total absence of any effective judicial control policies, the Court is not impressed by a (theoretical) resort to Parliament.[104] An investigating judge whose role is limited to issuing interception warrants and deciding on the storage of the tapes and transcripts is not enough if the law fails to make a provision for acquainting him with the results of the surveillance, and does not require him to determine if the requirements of the law have been complied with. Leaving that competence to the prosecutor's office is not sufficient, certainly not considering that the situations protected would then only be those attached to criminal proceedings, neglecting any surveillance outside of that scope.[105] Delegating the task to draft the reports of the monitored conversations to a judicial clerk is equally insufficient.[106] The Court noted that, with regard to the "thoroughness," that:

> [D]ans 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.[107]

---

[103] Bugallo v. Spain, App. No. 58496/00, Eur. Ct. H.R. ¶ 30 (2003); *Dumitru Popescu*, App. No. 71525/01, Eur. Ct. H.R. ¶ 70-73; *see Iordachi*, App. No. 25198/02, Eur. Ct. H.R. ¶ 30.

[104] *Dumitru Popescu*, App. No. 71525/01, Eur. Ct. H.R. ¶ 77 (only available in French).

[105] *Iordachi*, App. No. 25198/02, Eur. Ct. H.R. ¶ 47.

[106] *Bugallo*, App. No. 58496/00, Eur. Ct. H.R. ¶ 30.

[107] *Dumitru Popescu*, App. No. 71525/01, Eur. Ct. H.R. ¶ 78. "[U]nder certain circumstances, it would be excessive, for one thing from a practical point of view, to transcribe and include the totality of intercepted conversations operated from a telephone set into the preliminary investigation file of a case. That could indeed be contrary to other rights, like, for example, the right to respect for the private lives of other people who have made calls from the monitored set. If that is the case, the person concerned should nevertheless be offered the opportunity to listen to the recordings or to challenge their truthfulness, hence the necessity to keep them intact until the end of the criminal proceed-

The Court has also given attention to the circumstances in which recordings may or must be erased or destroyed, in particular, where an accused has been discharged by an investigating judge or acquitted by a court.[108]

D. The Keeping of Data

In the *Leander* judgment, the ECtHR 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.[109]

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. Other than the techniques discussed above, it is not always self-evident whether the keeping of data amounts to a privacy interference (*infra* Part 1). Once an interference is established, the question is whether it can be justified under Article 8 of the ECHR (*infra* Part 2).

1. 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. The question is whether the gathering of data on a person amounts to an interference with Article 8 of the ECHR in all circumstances.

In the *Friedl* case, which involved the use of photographs taken by the authorities during a public demonstration, the European Commission for Human Rights[110] noted that there was no intrusion into the inner cir-

---

ings, and, more in general, to include the pieces that look suitable to him for the defense of his interests into the preliminary investigation file." *Id.* (translated by author).

[108] Huvig v. France, App. No. 11105/84, 12 Eur. H.R. Rep. 528 ¶ 34 (1990); Kruslin v. France, App. No. 11801/85, 12 Eur. H.R. Rep. 547 ¶ 35 (1990); Valenzuela Contreras v. Spain, App. No. 27671/95, 28 Eur. H.R. Rep. 483 ¶ 46 (1999); *Iordachi*, App. No. 25198/02, Eur. Ct. H.R. ¶ 39 (quoting Weber v. Germany, App. No. 54934/00, Eur. Ct. H.R. ¶ 95 (2006)).

[109] Leander v. Sweden, App. No. 9248/81, 9 Eur. H.R. Rep. 433 ¶ 59 (1987).

[110] 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.

cle of the applicant's private life.[111] The photographs were taken of a public demonstration and they had been used solely as an aid to police the demonstration on the relevant day.[112] In this context, the Commission gave weight to the fact that the photographs taken remained anonymous, the personal data recorded and the photographs 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.[113] In *Lupker*, equally concerning photographs, the Commission observed first that they were not taken in a way which constituted an intrusion upon the applicants' privacy; second, that the photographs were kept in police archives since they had been either provided voluntarily or taken by police in connection with a previous arrest; and third, 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."[114]

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.[115] In those cases, the question whether privacy was violated was not even asked – government action did not amount to a privacy issue.

The storing and releasing of information from a secret police file without opportunity to refute it is, however, considered an interference.[116] Furthermore, the Court was not persuaded that recordings taken for use as voice samples could 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."[117] 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 case, the Court pointed out that it was not its job

---

[111] Friedl v. Austria, App. No. 15225/89, 21 Eur. H.R. Rep. 83 (1995).
[112] *Id.* ¶ 49.
[113] *Id.* ¶ 50.
[114] Lupker v. Netherlands, App. No. 18395/91, Eur. H.R. Rep. (1992).
[115] Herbecq v. Belgium, App No. 32200/96, 4 Eur. H.R. Rep. 504 (1998).
[116] Leander v. Sweden, App. No. 9248/81, 9 Eur. H.R. Rep. 433 ¶ 48 (1987).
[117] P.G. v. United Kingdom, App. No. 44787/98, Eur. Ct. H.R. 550 ¶ 59 (2001).

to speculate as to whether the information gathered is sensitive or not, nor as to whether the individual has been inconvenienced in any way. It is sufficient to conclude that where data relating to the private life of an individual is stored by a public authority, the measure amounted to an interference with Article 8 protection.[118]

With regard to fingerprints, the Court reassessed existing case-law established in the 2008 landmark case *S. and Marper*. In the past, the Commission concluded that fingerprints were 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.[119] The Court now concluded that the general approach with respect to photographs and voice samples should also be followed with respect to fingerprints. Fingerprints objectively contain unique information about the individual concerned, allowing for 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. Accordingly, the Court considered that the retention of fingerprints in 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.[120]

Today, in a time when many States across the world tend to systematically keep biometrical data on people, the question of what status should be given to cellular and DNA material is highly important. With regard to the keeping of that type of information, the *S. and Marper* judgment declared that this amounts to an interference with the right to privacy.[121]

> [A]n 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

---

[118] Amann v. Switzerland, App. No. 27798/95, Eur. Ct. H.R. ¶ 70 (2000).

[119] Kinnunen v. Finland, App. No. 24950/94, Eur. Comm'n H.R. (1996) [PLEASE NOTE – WE COULD NOT FIND THIS CITE].

[120] S. v. United Kingdom, App. No. 30562/04, Eur. Ct. H.R. ¶ 85 (2008).

[121] *Id.* ¶ 77.

> with precision today.[122]

The Court noted, however, that a legitimate concern about the conceivable use of cellular material in the future is not the only element to be taken into account. In addition to the highly personal nature of cellular samples, they contain sensitive information about an individual, including information about his or her health, and, moreover, samples contain a unique genetic code of great relevance to both the individual and his relatives.[123]

DNA profiles contain a more limited amount of personal information in a coded form. Nonetheless, the profiles contain substantial amounts of unique personal data. While that information may be considered objective and irrefutable, processing the data 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 lives of the individuals concerned."[124] The frequency of familial searches, the safeguards attached thereto, and the likelihood of detriment in a particular case were found immaterial in this respect. The conclusion was similarly not affected because the information is in coded form. The Court concluded that "[t]he 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."[125]

2. Justifiability of an Interference

In order to maintain such databases, 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 in the *Rotaru* case (*supra*), for the measures to be in accordance with the law, the Court reiterated:

> [T]hat 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 safe-

---

[122] *Id.* ¶ 71.
[123] *Id.* ¶ 72.
[124] *Id.* ¶¶ 74-75.
[125] *Id.* ¶ 76.

> guards 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.126

The fact 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."[127]

The question remains as to whether it is necessary in a democratic society to use DNA collection 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 have made rapid and marked progress in using DNA information in the determination of innocence or guilt.[128] Furthermore, 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.[129] 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.[130]

According to the Court, the core principles of data protection require the

---

[126] *Id.* ¶ 99 (internal citation omitted).
[127] Van der Velden v. Netherlands, App. No. 29514/05, Eur. Ct. H.R. 1174 (2006).
[128] *S.*, App. No. 30562/04, Eur. Ct. H.R. ¶ 105.
[129] *Van der Velden*, App. No. 29514/05, Eur. Ct. H.R. 1174 (2006).
[130] *S.*, App. No. 30562/04, Eur. Ct. H.R. ¶ 106.

retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage.[131] More particularly, most of the Member States allow cellular samples to be taken in criminal proceedings only from individuals suspected of having committed offenses of a certain minimum gravity. The Court noted that in the great majority of the 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, although a restricted number of exceptions to this principle is allowed by some States.[132]

The Court remarked that the protection afforded by Article 8 of the ECHR would be unacceptably weakened if the use of modern scientific techniques in the criminal justice system were allowed at any cost. "In the Court's view, the strong consensus existing among the [Member] 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."[133] This leads one to ask: can there 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*, the Court accepted that the extension of the database had contributed to the detection and prevention of crime, despite the fact that there was no evidence at that time establishing 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."[134] 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 rejects a blanket and indiscriminate 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

---

[131] *Id.* ¶ 107.
[132] *Id.* ¶ 108.
[133] *Id.* ¶ 112.
[134] *Id.* ¶ 117.

> 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.[135]

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. For example, 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.[136] The risk of stigmatization, as the Court emphasized, is of particular concern. The perception that persons involved are not being treated as innocent is heightened by the fact that 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 offense are required to be destroyed.[137] 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 into society.[138] It concluded that "[a]ccordingly, 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."[139]

V. SPECIAL INVESTIGATION TECHNIQUES INTERFERING WITH THE RIGHT TO A FAIR TRIAL

It is clear that the application of certain special investigation techniques cannot only give cause to violations of an individual's privacy, but it may also touch upon other fundamental rights, including the right to a fair trial. The European Court does not accept that Article 6, which guarantees due process, has no application to pre-trial proceedings. Its requirements may be relevant before a case is sent for trial, because the

---

[135] *S.*, App. No. 30562/04, Eur. Ct. H.R. ¶ 119 (internal citation omitted).
[136] *Id.* ¶ 120.
[137] *Id.* ¶ 122.
[138] *Id.* ¶ 124.
[139] *Id.* ¶ 125.

fairness of the trial is likely to be seriously prejudiced by an initial failure to afford such rights.[140] Often, the question about the admissibility during trial of the information previously obtained, 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 of the ECHR. It holds that the admissibility of evidence is primarily a matter to be regulated 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."[141] Overall, as it will appear, there is a certain leniency towards due process restrictions when national security is at stake. But it is limited, and including within the Court, not uncontroversial. Below, the technique of infiltration (*infra* Part A), and the keeping of observation and infiltration data in confidential records (*infra* Part B), will be discussed more profoundly.

A. Infiltration

For police to perform their task, they are increasingly required to make use of undercover agents, informers, and covert practices, particularly in tackling organized crime and corruption. That special investigation technique is essentially of a deceptive nature. The European Court noted in this regard that the use of special investigative methods – in particular, undercover techniques – cannot in itself infringe the right to a fair trial.[142] However, on account of the risk of police incitement entailed by such techniques, their use must be kept within clear limits, as will be shown below.

In the *Lüdi* case, the Court found, first of all, that the sending of an undercover agent into what was thought to be a large criminal network did 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

---

[140] Imbrioscia v. Switzerland, App. No. 13972/88, Eur. H.R. Rep. 56 ¶ 36 (1993) (internal citation omitted).

[141] *See, e.g.*, Ramanauskas v. Lithuania, App. No. 74420/01, Eur. Ct. H.R. 119 ¶ 52 (2008) (citing Van Mechelen v. Netherlands, App. No. 21363/93, 25 Eur. H.R. Rep. 647 ¶ 50 (1997)); Teixeira de Castro v. Portugal, App. No. 25829/94, 28 Eur. H.R. Rep. 101 ¶ 34 (1998)); Eurofinacom v. France, App. No. 58753/00, Eur. Ct. H.R. (2004); Rowe & Davis v. United Kingdom, App. No. 28901/95, Eur. Ct. H.R. 91 ¶ 62 (2000).

[142] *Ramanauskas*, App. No. 74420/01, Eur. Ct. H.R. 119 ¶ 51.

he is consequently running the risk of encountering an undercover police officer whose task, is in fact, to expose him.[143] Regarding fair trial rights however, the use of undercover agents must be restricted and safeguards put in place. Crucial in *Lüdi* was the determination that the police officer concerned had been sworn in, the investigating judge had not been unaware of his mission, and the authorities had opened a preliminary investigation.[144]

By doing so, the police officers' role is confined to acting as an undercover agent. The fact that the authorities have "good reason to suspect" the defendant of having a propensity to commit an offense would tend to suggest that an operation is more akin to "infiltration" than "instigation." That was not the case in the case of *Teixeira de Castro*. As there was no government evidence to support that the applicant was predisposed to commit offenses, 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."145 In the Court's opinion, the right to a fair administration of justice holds such a prominent place that it cannot be sacrificed for the sake of expedience.146 Following the principles established in Teixeira, the Ramanauskas case, for example, held 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."147

In that circumstance, suspicion must be based on concrete evidence showing that initial steps have been taken to commit the acts constituting the offense for which the defendant is subsequently prosecuted. The Court holds that police officers act only as undercover agents if significant steps preparatory to the commission of the offense had been taken before their participation in the investigation.[148] The Court also checks "whether there is evidence indicating that, without such intervention, the

---

[143] *See* Lüdi v. Switzerland, App. No. 12433/86, 15 Eur. H.R. Rep. ¶ 40 (1992).

[144] *Id.* ¶ 49. The Court observed nevertheless a violation of Article 6, because the defense could not question the undercover agent during trial. *Id.*

[145] Eurofinacom v. France, App. No. 58753/00, Eur. Ct. H.R. (2004) (citing *Teixeira de Castro,* App. No. 25829/94, 28 Eur, H.R. Rep. 101 ¶ 38)).

[146] *Ramanauskas*, App. No. 74420/01, Eur. Ct. H.R. 119 ¶ 54; Vanyan v. Russia, App. No. 53203/99, Eur. Ct. H.R. 877 ¶ 46 (2005); *see Teixeira de Castro*, App. No. 25829/94, 28 Eur, H.R. Rep. 101 ¶¶ 35-36 (1998).

[147] *Ramanauskas*, App. No. 74420/01, Eur. Ct. H.R. 119 ¶ 54.

[148] *See* Sequeira v. Portugal, App. No. 73557/01, Eur. Ct. H.R. (2003) (available in French only).

offence would not have been committed."[149] In any event, it is up 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. For the trial to be fair within the meaning of Article 6 of the ECHR, "all evidence obtained as a result of police incitement must be excluded."[150]

B. The Inaccessibility of a Confidential Record

The confidentiality of records holding information obtained through special investigation techniques is obviously a delicate matter. It is a fundamental aspect of the right to a fair trial that criminal proceedings are adversarial and that there is equality of arms between the prosecution and the defense. The right to an adversarial trial means, in a criminal case, that both parties must have the opportunity to know and comment on the evidence discovered. In addition, Article 6 of the ECHR 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 at risk of reprisals or to keep secret police methods of investigating crime, which must be weighed against the rights of the accused."[151]

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. "[I]n order to ensure that the accused receives a fair trial, any difficulties caused to the defence by a limitation on its rights must be sufficiently counterbalanced by the procedures fol-

---

[149] *Eurofinacom*, App. No. 58753/00, Eur. Ct. H.R. (2004) (internal citation omitted).

[150] *See, e.g.*, Khudobin v. Russia, App. No. 59696/00, Eur. Ct. H.R. ¶¶ 133-35 (2006); *Ramanauskas*, App. No. 74420/01, Eur. Ct. H.R. ¶ 60.

[151] Jasper v. United Kingdom, App. No. 27052/95, Eur. Ct. H.R. 90 ¶ 51 (2000) (internal citation omitted).

lowed by the judicial authorities."[152]

The European Court considers that a procedure whereby the prosecution itself attempts to assess the importance of concealed information for the defense and weighs this against the public interest in keeping the information secret, cannot comply with the requirements of Article 6 of the ECHR.[153] 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.[154] In the *Jasper* case, the Court found that it was sufficient that the trial judge, with full knowledge of the issues in the trial, 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. The Court was satisfied that the defending party was kept informed and permitted to make submissions and participate in the decision-making process, as far as was possible without revealing to them the material which the prosecution sought to keep secret on public interest grounds.[155]

Similarly, the Court determined in the *Rowe and Davis* case that a procedure before an appellate court about the disclosure of information was in itself not necessarily sufficient to remedy the unfairness during the trial by the absence of the scrutiny of information withheld by the trial judge.[156] Appellate judges' understanding of the possible relevance of the undisclosed material is sometimes dependent upon transcripts of hearings, and on the account of the issues given to them by prosecution. 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*."[157]

In the *Edwards and Lewis* case however, the Court drew the opposite conclusion with regard to the capacity of the trial judge. It appeared to the Court that the undisclosed evidence related, or might have related, to an issue of fact decided by the trial judge (the applicants alleged that

---

[152] *See, e.g.*, *id.* ¶ 51; Rowe & Davis v. United Kingdom, App. No. 28901/95, Eur. Ct. H.R. ¶¶ 60-61 (2000); Dowsett v. United Kingdom, App. No. 39482/98, Eur. Ct. H.R. 314 ¶ 42 (2003); Edwards & Lewis v. United Kingdom, App. Nos. 39647/98 and 40461/98, Eur. Ct. H.R. 381 ¶ 53 (2003).

[153] *Dowsett*, App. No. 39482/98, Eur. Ct. H.R. ¶ 44.

[154] *Id.* ¶ 50.

[155] *Jasper*, App. No. 27052/95, Eur. Ct. H.R. 90 ¶ 55.

[156] Rowe & Davis v. United Kingdom, App. No. 28901/95, Eur. Ct. H.R. ¶ 65.

[157] *Id.*

they had been the victim of police incitement).[158] As they were denied access, it was impossible for the defense representatives to argue the case in full. The judge 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. His appraisal of the evidence was essential to determine whether the prosecution could continue, and whether not disclosing it to the defense violated their right to a fair trial.[159]

VI. CONCLUDING REMARKS

Although it may be clear that striking a balance between national security and privacy interests of individual citizens is not an easy exercise, the European Court of Human Rights considers the efforts of Member States of the Council of Europe to live up to a number of principles particularly important. The Court's conclusions on the merits in all the above mentioned cases insisted on legal certainty; continuous control by independent (judicial) actors; a subsidiary deployment of very invasive measures for the benefit of others; less intrusive techniques; and proportionality of the interference with one's privacy or due process rights to the goals government seeks to defend. Particularly the latter condition may stay the pivotal point in the Court's decision-making for many years to come, as the proportionality requirement is a primary criterion in determining whether human rights interference can be considered "necessary in a democratic society." That is not all self-evident. Some of the junior Member States in Eastern Europe have had an authoritarian regime for decades. Many of the cases discussed above show that often, their legal system is still adapting to the democratic standards set out by the Council of Europe.[160] Nevertheless, no senior Member should assume that its intelligence framework is perfect as is.

It can be expected that in 21st century democracies, privacy issues

---

[158] Edwards & Lewis v. United Kingdom, App. Nos. 39647/98, 40461/98, Eur. Ct. H.R. 381 ¶ 57 (2003).

[159] *Id.* ¶ 58.

[160] On 31 December 2009, 28.1% of pending cases before the Court were cases against Russia, 8.4% against Ukraine, and 8.2% against Romania; 54.9% of all pending cases originated in only 6 of 46 Member States, all former dictatorships. *See* Analysis of Statistics 2009 of the Court (published January 2010), *available at* http://www.echr.coe.int/NR/rdonlyres/89A5AF7D-83D4-4A7B-8B91 6F4FA11AE51D/0/Analysis_of_statistics2009.pdf.

will remain a prominent legal issue. In contrast to questions of privacy concerning what we do while at work, on the internet or within our homes, when confronted with national security issues, it may be tempting to conclude that intrusive government measures should be allowed, since the greater good concerns our collective safety. Nevertheless, there is no reason why severe privacy deprivation should ever be considered self-evident. Even though the problem seems pre-eminently a matter of modern times, in 1759, in a time when nation-states were under full construction, Benjamin Franklin wrote a wisdom that has clearly passed the test of time: "Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety."[161] We may want to keep this in mind.

[161] Benjamin Franklin, *Remarks on the Proposition*, *in* 1 MEMOIRS OF THE LIFE AND WRITINGS OF BENJAMIN FRANKLIN 270 (1818).