CEPS Paper in
LIBERTY and SECURITY in Europe

National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges

Didier Bigo, Sergio Carrera, Nicholas Hernanz and Amandine Scherrer

No. 78/ January 2015

Abstract

This study provides a comparative analysis of the national legal regimes and practices governing the use of intelligence information as evidence in the United Kingdom, France, Germany, Spain, Italy, the Netherlands and Sweden. It explores notably how national security can be invoked to determine the classification of information and evidence as 'state secrets' in court proceedings and whether such laws and practices are fundamental rights- and rule of law-compliant. The study finds that, in the majority of Member States under investigation, the judiciary is significantly hindered in effectively adjudicating justice and guaranteeing the rights of the defence in 'national security' cases. The research also illustrates that the very term 'national security' is nebulously defined across the Member States analysed, with no national definition meeting legal certainty and "in accordance with the law" standards and a clear risk that the executive and secret services may act arbitrarily. The study argues that national and transnational intelligence community practices and cooperation need to be subject to more independent and effective judicial accountability and be brought into line with EU 'rule of law' standards.

This document was originally commissioned by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and published in December 2014. It is available for free downloading on the European Parliament's website (www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf) and is republished by CEPS with the kind permission of the Parliament.

ISBN 978-94-6138-440-9
Available for free downloading from the CEPS website (www.ceps.eu)

Contents

List of Abbreviations

AIVD	Algemene Inlichtingen- en Veiligheidsdienst (General Intelligence and Security Service, The Netherlands)
AFSJ	Area of Freedom, Security and Justice
BKA	Bundeskriminalamt (Federal Criminal Police Office, Germany)
CCSDN	Commission consultative sur le secret de la défense nationale (Consultative commission on national defence secrets, France)
CIA	Central Intelligence Agency (United States)
CoE	Council of Europe
COPASIR	Comitato Parlamentare per la Sicurezza della Repubblica (Parliamentary Committee for the Security of the Republic, Italy)
CMPs	Closed Material Procedures
CNI	Centro Nacional de Inteligencia (National Intelligence Centre, Spain)
COREPER	Permanent Representatives Committee (Council of the European Union configuration)
CJEU	Court of Justice of the European Union
ECHR	European Convention on Human Rights 1950
ECtHR	European Court of Human Rights
EU	European Union
EUCFR	Charter of Fundamental Rights of the European Union
EUMS	European Union Member State(s)
FRA	European Union Agency for Fundamental Rights
GCHQ	Government Communications Headquarters (United Kingdom)
ISC	Intelligence and Security Committee (United Kingdom)
JSA	Justice and Security Act (United Kingdom)
JTRIG	Joint Threat Research Intelligence Group (United Kingdom)
LIBE	Civil Liberties, Justice and Home Affairs Committee (European Parliament)
MI5 & MI6	Military Intelligence, Sections 5 and 6 (United Kingdom)
NCND	"Neither confirm nor deny"
NGO(s)	Non-governmental organisation(s)
NSA	National Security Agency (United States)
RIPA	Regulation of Investigatory Powers Act (United Kingdom)
SIS	Schengen Information System
SISMI	Servizio per le Informazioni e la Sicurezza Militare (Military Intelligence and Security Service, Italy)
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UN	United Nations

National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges

Didier Bigo, Sergio Carrera, Nicholas Hernanz and Amandine Scherrer

CEPS Paper in Liberty and Security in Europe No. 78 / January 2015

Executive Summary

This study examines the way in which justice systems across a selection of EU Member States use and rely on intelligence information that is kept secret and not disclosed to the defendants and judicial authorities in the name of national security. It analyses the laws and practices in place from the perspective of their multifaceted impact on the EU Charter of Fundamental Rights (in particular its provisions related to the rights of the defence and freedom of information and expression), as well as on wider 'rule of law' principles. The analysis is based **on a comparative study of the legal regimes, interpretations by domestic and European tribunals as well as key developments and contemporary practices concerning the use of intelligence information as 'evidence' and the classification of information as 'state secrets' during trials in the name of 'national security' in the following seven EU Member States** (EUMS): United Kingdom, France, Germany, Spain, Italy, the Netherlands and Sweden.

The examination has highlighted a number of **key research findings**. It first shows **a wide variety of national legal systems and judicial practices embedded in domestic historical, political and constitutional trajectories characterising each Member State jurisdiction** (see Section 1 of the study and Annex 5 with detailed Country Fiches). The United Kingdom and the Netherlands are the only two Member States examined with official legislation allowing for the formal use of classified intelligence information in judicial proceedings. The United Kingdom constitutes an 'exception' in the broader EU landscape due to the existence of the much-contested 'Closed Material Procedures' (CMPs) – secret court hearings where only the judge and security-cleared special advocates are given access to sensitive intelligence material. The Netherlands operates a system of 'shielded witnesses' in courts, allowing intelligence officials to be heard before a special examining magistrate (Sections 1.1. and 1.2 of this study). Other EUMS analysed (Germany, Spain and Sweden) present indirect judicial practices in which certain evidence may be hidden from a party during trials under a number of conditions (Section 1.3).

Nevertheless, the study demonstrates that **secret evidence is not always legal evidence**. In countries such as Germany, Italy or Spain the rights of the defence and the right to a fair trial cannot be 'balanced' against national security or state interests as this would directly contravene their respective constitutional frameworks (Section 1.4). Yet, all EUMS under examination face a number of challenges as regards **the difficult and often controversial declassification or disclosure of intelligence materials**, which too often lacks proper independent judicial oversight and allows for a disproportionate margin of appreciation by state authorities (Section 1.5 of this study).

Another issue resulting from the comparative investigation relates to **the fuzziness and legal uncertainties inherent to the very term 'national security'** (as evidenced in Section 1.6 and Annex 3). While this notion is quite regularly part of political and legal debates in EU and national arenas, the study reveals that a proper definition of what national security actually means is lacking across a majority of EUMS under investigation. The few definitional features that appear in EUMS' legal regimes and doctrinal practices fail to meet legal certainty and 'rule of law' standards, such as the "in accordance with the law" test (see below). This too often leads to a disproportionate degree of appreciation for the executive and over-protection from independent judicial oversight, which is further exacerbated in a context where some EUMS have bilateral systems of mutual respect of state secrets with third countries such as the US. Moreover, the **disparities and heterogeneous legal protection regimes** among EUMS also mean that EU citizens who are suspects in judicial procedures are protected differently or to divergent degrees across the EU. There are **variable 'areas of justice' in the EU** when it comes to the rights of defence of suspects in cases dealing with national

security and state secrets. This diversity is at odds with the ambition of developing a common AFSJ and achieving non-discrimination between EU nationals when it comes to the delivery of fundamental rights.

A second key finding of the study relates to **a growing transnational exchange of intelligence and use of these intelligence materials before courts** (as developed in Section 2 and Annex 1 of this study). The 2013 Snowden revelations provide the general context within which EUMS' regimes and practices need to be analysed. There has been a growing expansion of intelligence cooperation across the world, which is mainly transatlantic and asymmetrical in nature due to the more prominent role played by the US. This has strengthened the view that transnational threats require a more extensive sharing of raw data on individuals collected by Internet or mobile devices. This trend poses a number of dilemmas from the perspective of judicial accountably and the rule of law (Section 2.1 of this study). One relates to the difficulties in assessing the quality, lawfulness and accuracy of the information, and the extent to which this very information can be considered 'evidence' in trials (Section 2.2). The current reliance on intelligence information is, moreover, problematic in light of insufficient or deferential judicial oversight of executive decisions taken 'in the name of national security'. This is particularly also the case in respect of the ways in which the use of state secrets can disrupt government officials' accountability in cases of alleged 'wrongdoing' (Section 2.3).

A third finding concerns an emerging set of **European judicial standards** from the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) on issues related to intelligence information, national security and state secrets, in particular when these affect the rights of the defence (refer to Section 3, Annex 1 and Annex 2 of this study). One of the most important legal standards when assessing national security and intelligence information is **the "in accordance with the law" principle**. The ECtHR has outlined three main conditions composing this test: first, the measure under judicial scrutiny needs to have its basis in domestic law; second, the law needs to be accessible and sufficiently clear to the individual involved; and third, the consequences must be foreseeable. The ECtHR has repeatedly called for domestic laws to afford sufficient legal protections, with sufficient clarity, to prevent the exercise of arbitrariness and unfettered powers by the executive (as evidenced in Section 3.1).

Obscure laws, or laws allowing the use of secrecy, are therefore not laws, as they fail to respect European judicial standards. This has been confirmed by the CJEU in several rulings dealing with the legality of executive interferences on the rights of the defence in the context of EU antiterrorism policies and national security. Here the Luxembourg Court has recalled **the essential nature of the principle of effective judicial protection** by the Community judicature even in cases related to national security. The CJEU has further clarified that for the rights of the defence to be respected, the evidence available against an individual needs to be disclosed to him/her and include at least a summary of the reasons upon which the case rests (see Section 3.2).

The freedom of the press (information and expression) and the protection of journalists and their sources are considered as vital for the functioning of modern liberal democracies (Section 4 of this study). A third cross-cutting finding of this study is that the freedom of the press is **still systematically jeopardised when national security is invoked** in a majority of EUMS under examination. A number of legal restrictions to the rights of journalists and whistle-blowers on grounds of national security are often found across EUMS. In the United Kingdom, the debate over press freedom and national security is particularly vivid in the context of Snowden's revelations and their reporting by investigative journalists, as demonstrated in the Miranda case. In the Netherlands, a judgment by a national court compromising the sources of journalists was challenged by the ECtHR. This study has found that the legal protection granted to whistle-blowers in national security cases in the Member States examined is far from sufficient.

The study ultimately shows that there are **significant barriers to the judiciary's role of effectively adjudicating justice and guaranteeing the rights of the defence** in the majority of EUMS under examination. Claims of secrecy obstruct judicial scrutiny, and judicial authorities too often have to trust the quality and lawfulness of the information provided by the intelligence services and the legitimacy of state secrets claims. The resulting picture is that **judicial authorities across the EUMS under examination have a high degree of trust in claims made by governments and intelligence communities in judicial proceedings that national security is under threat**, that EUMS readily accept the 'state secrets' arguments which prevent judicial and legal oversight on the lawfulness of the information used in trials and that they accept the legitimacy of executive claims on secrecy. That notwithstanding, various court cases presented in this study and Snowden's revelations on unlawful practices of large-scale mass surveillance illustrate the

ways in which **the trust-based relationship between independent judicial authorities and intelligence services' practices has been increasingly under pressure**.

In view of all these challenges, the study concludes that there is a risk that practical transnational arrangements prevail over efforts to use new mechanisms led by the spirit of the Lisbon Treaty that could improve respect for fundamental rights and the rule of law across the Union, while not interfering with Member States' national sovereignty in questions related to national security. The recommendations outlined hereafter seek to avoid this risk. It is necessary **to strengthen the ways in which the courts and judicial actors fulfil their duty to uphold the rule of law with increased vigilance**. The EU can play a role in **consolidating, promoting and ensuring a more effective implementation of supranational fundamental and human rights principles developed by European Courts and the rule of law**. In the light of this, the following policy recommendations are put forward in this study:

- **The new EU Framework to strengthen the Rule of Law should be used to encourage concerned EU Member States to modify their current legislation concerning the use of national security, state secrets and intelligence information in judicial proceedings.** The growing reliance of certain Member States on the use of secret evidence in courts constitutes a direct challenge to judicial scrutiny, as well as to the rights of the defence and freedom of the press laid down in the EU Charter of Fundamental Rights. The European Parliament could call on the new European Commission to use this case as a test bed for making operational the EU Rule of Law Framework. Concerned EUMS would need to put in place the necessary national reforms in order to fully ensure respect for the rights of the defence as provided for in Articles 47 and 48 of the EU Charter.
- **A professional code for the transnational management and accountability of data in the EU should be adopted.** The European Parliament could call for the elaboration and inter-institutional adoption of an EU Code for the Transnational Management and Accountability of Information addressed to the intelligence communities in the Member States. The goal should be to ensure that the practices of intelligence services are in accordance with fundamental rights and 'rule of law' principles and European judicial and legal 'rule of law' standards. The Code would provide EU guidelines for invoking national security and secrecy in the EU. Most important, it would present a common EU understanding of the basis on which national security should not be invoked by EUMS authorities (what national security is not).
- An '**EU Observatory'** should be established to map and follow up EUMS' uses and evolving interpretations of national security and state secrets. The EU Observatory would additionally facilitate a better understanding of when the 'national security' justification should not be used by EUMS.
- **The EU should better streamline the promotion and effective implementation of fundamental rights and 'rule of law' standards** laid down in relevant international and regional instruments. The European Parliament should call for a consolidated partnership with supranational human rights actors such as the Council of Europe and the United Nations.
- **An EU level framework for the protection of whistle-blowers in cases related to national security should be adopted.** The systematic protection of whistle-blowers should include strong guarantees of immunity and asylum.

National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges

Didier Bigo, Sergio Carrera, Nicholas Hernanz and Amandine Scherrer*

CEPS Paper in Liberty and Security in Europe No. 78 / January 2015

1. Introduction

1.1 The scope of the challenge

This study examines from a comparative perspective the complex legal issues inherent to the interface between national security, state secrets, judicial accountability of intelligence, as well as the legal and practical arrangements which have been implemented to address these contested issues in a selection of EU Member States (EUMS). Of course, the framing of debates on the relationship between intelligence and the rule of law and judicial scrutiny differs considerably across EUMS. **The approaches and solutions chosen to resolve the tensions between the national security argument and the concomitant use of secrecy and the need for judicial oversight to ensure public and democratic accountability are the result of long historical trajectories and different legal systems in EUMS**. Each State presents different ways of dealing with the management of political violence, implementing its criminal justice system and engaging in the collection, storage and transfer of data on individuals on a large scale.

On all these topics, **EUMS do not share the same underlying assumptions concerning the role of secrecy and its legitimacy in liberal democratic regimes**. For some, secrecy is a right derived from national sovereignty that the executive can decide to balance against the fundamental rights of individuals when necessary to defend its foreign affairs or/and other state interests. In other EUMS, however, fundamental rights of the defence cannot be balanced against national security, as this would pose a direct challenge to their constitutional traditions and frameworks. The mechanisms of control may also differ, giving more or less power to the executive. The difference of views over secrecy creates divisions in each state jurisdiction and generates considerable controversy, often creating opposition among civil and law enforcement service actors, the judiciary and civil society organisations.

This study analyses the legal regimes and key debates at stake in seven EUMS: the United Kingdom, France, Germany, Spain, Italy, the Netherlands and Sweden. The choice of these EUMS was informed by a previous report submitted to the European Parliament on "National Programmes for Mass Surveillance of Personal

---

* Didier Bigo is Director of the Centre d'Etudes sur les Conflits, Liberté et Sécurité (CCLS) and Professor at Sciences-Po Paris and King's College London. Sergio Carrera is Senior Research Fellow and Head of the Justice and Home Affairs Section, Centre for European Policy Studies, CEPS. Nicholas Hernanz is Researcher, Justice and Home Affairs Section, CEPS. Amandine Scherrer is European Studies Coordinator and Associate Researcher at CCLS.

The authors would like to express their gratitude to Prof. Elspeth Guild (CEPS) and all the participants in the civil society organisations and practitioners Focus Groups which were organised for the purposes of this study for their comments on an earlier draft. Any errors or omissions are the sole responsibility of the authors.

Contributions in the annexed Country Fiches were made by:

- Mar Jimeno Bulnes, Professor in the Law Faculty of the University of Burgos, Spain
- Emmy Eklundh, Doctoral Researcher at the University of Manchester
- Roseline Letteron, Professor of Public Law at the Université Paris-Sorbonne
- Nikolaus Marsch, Lecturer at the Law Faculty of the University of Freiburg in Breisgau
- Daniel Squires, Lawyer specialised in public law and human rights, Matrix Chambers, London
- Arianna Vedaschi, Professor of Law at Bocconi University, Milan
- Gabriele Marino, Doctoral Researcher at the University of Exeter
- Anja Wiesbrock, Postdoctoral Researcher, Institute for Private Law, University of Oslo

Data in EU Member States and Their Compatibility with EU Law",[1] and the European Parliament Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and transatlantic cooperation in Justice and Home Affairs (Moraes Report),[2] which examined surveillance programmes and practices in EU countries such as the UK, France, Sweden, Germany and the Netherlands. The research illustrates that there is no real agreement regarding the role and legitimacy of secrecy across several Member States of the EU. **There is, however, substantial common ground on the role and necessity of the secret services, as well as their legal and judicial oversight from a 'rule of law' perspective**.

Few contest that secret services play a fundamental role in democracies to secure the country against transnational challenges. The very existence of intelligence services inside the institutions of representative democracies, and their necessity, is by and large uncontested. By their nature, actors which are often called secret or intelligence services can be ordered to do non-disclosable things, and for a long time it has not been widely accepted that they could be prosecuted or brought to justice for these actions or alleged wrongdoings. Intelligence communities share a particular culture of secrecy, as well as a strong sense of loyalty, and they are often respected by citizens. The acceptance of their practices has been shaped in liberal democracies by the recognition of a sharp distinction between what they could do 'internally' and 'externally', and particularly a distinction between their practices regarding citizens and foreigners. Nevertheless, as rightly recalled in the above-mentioned Moraes Report,[3] this sharp distinction is losing ground to the rapid emergence of new technologies related to internet and mobile devices. There has been much controversy involving the intelligence and law enforcement communities, NGOs defending civil liberties, internet companies and users surrounding the nature of the targets and the scale of the surveillance. Similar debates have focused on the duration of personal data retention and their use as intelligence material to build profiles of suspects before these persons have even committed any specific crime.

Conversely, there is also substantial common ground on **the need for efficient oversight of these services**, even if the proposed solutions are very different across the EUMS and may vary from limited oversight (often performed by actors who were previously members of these same services) to more in-depth oversight mechanisms operated by members of parliaments or independent judges. Intelligence oversight has been a recurrent challenge addressed in various scholarly research and previous policy-relevant studies.[4] The services have been nonetheless condemned when they have crossed the line.[5] By the late 1990s, acceptance of the need for oversight of intelligence activities by parliamentary or judicial authorities had progressively grown.

Yet the attacks of 9/11 in New York, followed by the Madrid and London bombings, somehow shocked the fragile consensus according to which intelligence communities cannot operate 'above or outside the law'. **These developments reinforced official justifications for more involvement of intelligence services in policing and the politics of terrorism prevention** that most governments and their services have favoured. They facilitated a general trend of intelligence services not revealing sources that allegedly incriminate individuals as 'suspects' in judicial proceedings, especially when this information was acquired abroad

---

[1] See: D. Bigo et al. (2013), "National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law", Study for the European Parliament, PE 493.032, November.

[2] European Parliament (2014), Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, 2013/2188/INI, 21 February.

[3] Paragraph 14 of the Moraes Report points out that the 'internal'-'external' distinction "is exacerbated by rapid technological and societal developments, since internet and mobile devices are everywhere in modern daily life ('ubiquitous computing') and the business model of most internet companies is based on the processing of personal data…that the scale of this problem is unprecedented…that this may create a situation where infrastructure for the mass collection and processing of data could be misused in cases of change of political regime".

[4] P. Gill (2012), 'Intelligence, Threat, Risk and the Challenge of Oversight', *Intelligence and National Security*, 27:2, pp. 206-22; Venice Commission (2007), Report on the democratic oversight of the security services, June; A. Wills, M. Vermeulen (2011), Parliamentary Oversight of Security and Intelligence Agencies in the European Union, European Parliament.

[5] For example on civil rights movements or recently with undercover practices in animal rights and ecologist movements or complicity in extraordinary renditions.

and/or shared with transnational networks or foreign actors. In that context, and as this study illustrates in the selected EUMS, this has opened up possibilities for the admissibility of secret information as 'evidence' in judicial proceedings, which in turn seriously impairs the rights of the defence and fair trial principles integral to the rule of law foundations of the EU.

Despite the common ground, there is not universal agreement and the tensions between the various schools of thought have been exacerbated. **Discussions are particularly contentious when the use of intelligence information and state secrets challenges effective judicial scrutiny,** and when state secrets are invoked to check investigations into unlawful practices by the executive and/or its intelligence services with significant consequences for fundamental rights. More generally, the above-mentioned **'politics of prevention'** has moved the axis of criminal justice from the an individual committing a criminal act, and the existence of objective and sound evidence backing the charge against him, towards the elaboration of lists of suspects, on the basis of 'information', and the temptation to preventively detain or deprive suspects of liberty and security. **It is relative to these new challenges that the present study tries to shed light on contemporary practices across the EUMS**.

This study examines how some EUMS have adapted their own legal approaches and systems in the field of national security and secrecy, especially in the context of a policy for preventing terrorism. It starts by acknowledging that each of these systems is the result of a unique domestic constitutional and criminal justice background. It may come as no surprise that the EUMS under investigation present distinct legal arrangements, different approaches to the principle of separation of powers, and varying ranges of 'privileges' that may be granted to the executive – such as the right to invoke state secrets in the name of national security or state interests.

The research presented in this study shows very different ways in which the tensions between secret materials presented in court and the principle of open justice have been debated and dealt with. We have also found disparate approaches to judicial scrutiny and officials' accountability. As the study shows, current debates regarding secret court hearings in the UK, where only the judge and security-cleared special advocates are given access to sensitive intelligence material (in what are called 'closed material procedures', or CMPs), are illustrative of the distinct legal and political philosophies involved and indicate that **it is far from straightforward to talk about a process of convergence.** Therefore, the study does not seek to identify 'best' or 'promising practices' or 'common trends' on state secrets and democracy, as such an exercise would make very little sense given the legal and political specificities we have encountered in each domestic arena under investigation. Instead, special focus is paid to assessing **the compatibility of the legal regimes and practical arrangements identified across the selected EUMS with the EU Charter of Fundamental Rights and recent developments on 'rule of law' monitoring as a central feature of the EU**.

We argue that the separation of powers, the independence of the judiciary and respect for the **'democratic rule of law with fundamental rights'**[6] are key principles in any liberal democracy,[7] and that the issues at stake – the use of secrecy and secret evidence in courts – must be assessed in light of these principles. The study also starts from the premise that a pure legal approach, while indispensable, is not enough when dealing with the use of intelligence information, state secrets and national security in courts. Our research has adopted a broader disciplinary perspective by taking into account wider debates on social practices and public confidence in institutions. **The following four specific themes** are at the heart of the analysis:

- the use of secret information, legal certainty, judicial scrutiny and legal safeguards;
- the growing transnational exchange of intelligence and the use of these intelligence materials in courts;
- trust, mistrust and the balance of powers in liberal democracies; and
- the freedom of the press and the protection of whistle-blowers.

---

[6] S. Carrera, E. Guild and N. Hernanz (2013), "The Triangular Relationship between Fundamental Rights, Democracy and the Rule of Law in the EU: Towards an EU Copenhagen Mechanism", Study for the European Parliament, DG IPOL, Brussels.

[7] Charles Louis de Secondat, Baron de Montesquieu, *Complete Works, vol. 1 (The Spirit of Laws)* [1748]; M. Vatter (2008), "The Idea of Public Reason and the Reason of State. Schmitt and Rawls on the Political", *Political Theory* 36:239-71.

The use of secret information, legal certainty, judicial scrutiny and legal safeguards

Special procedures have been adopted and implemented in some EUMS allowing for the use of secret information as evidence in judicial proceedings (the UK and the Netherlands). In other EU legal systems, there is an indirect use of intelligence materials in practice by national courts and law enforcement authorities (Spain, Sweden and Germany). In France and Italy, the judicial authorities can only access declassified or open materials, while 'secret' information cannot be used in court. In these cases, the challenge instead lies in the powers granted to the executive to determine the 'classification' of information. The UK is an exception among the countries under examination. At the forefront of intelligence-led policing and preventive law enforcement (detailed hereafter), successive UK governments have proactively submitted bills, such as the Special Immigration Appeal Commission Act (SIAC), the Regulation of Investigatory Powers Act (RIPA), and the Justice and Security Act (JSA), that have transformed the criminal justice system's traditional approach. In the UK there has been intense controversy and heated debate. The study attempts to drill down into these discussions in order to address the quality and effectiveness of specific safeguards to ensure a fair trial and the rights of the defence. In comparison, the other EUMS under consideration have encountered far fewer controversies and challenges, but none of them have gone as far as the UK in the systematic use of secret evidence in trials.

In examining legal certainty, judicial scrutiny and fundamental rights safeguards, the study focuses on the following research questions: To what extent are intelligence materials properly scrutinised by judicial authorities? What are the legal safeguards for ensuring a fair trial? Are there sufficient guarantees in place to prevent misuse and abuse of secrecy? To what extent is the use of secrecy in courts compatible with the rule of law? These questions are addressed by analysing the national legislation and procedures in place and how they are enacted in judicial practices or doctrine. Taking into consideration how legal texts are implemented in courtroom practice helps identify gaps, legal uncertainties and inadequate safeguards, which are in turn tested against European judiciary standards developed by the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU).

The growing transnational exchange of intelligence and the use of these intelligence materials in courts

The second theme covered by this study relates to the general context in which it was undertaken – the 2013 Snowden revelations. As explored by Richard Aldrich, **the most important development within intelligence and security services in recent years has been the growing expansion of intelligence cooperation across the world.**[8] This cooperation is at present mainly transatlantic and asymmetrical in nature. The US has played a prominent role and has insisted on the absolute protection of its sources. The national security of each EUMS may therefore be dependent on transnational shared data and on a degree of collaboration between the Western intelligence services in order 'to connect the dots' of traces left by small, hostile groups acting globally. The role of NATO and of bilateral agreements on the exchange of information is increasingly central. Strong cooperation and ties can be found among the Five Eyes[9] and to a lesser degree with its allies (Sweden, the Netherlands, Germany and France). If tighter cooperation agreements and greater mutual understanding have not entirely suppressed competition between intelligence communities at both national and international levels, they have strengthened the view that transnational and global threats require extensive sharing of raw data collected on various platforms such as the internet or smart phones. Such collection involves not only state authorities, but also private partners.

The growing transnational exchange of intelligence raises specific challenges in relation to the use of intelligence materials in courts. One such challenge is distinguishing between 'information' and 'intelligence' when they are shared across domestic intelligence and law enforcement services that have their own views, priorities, and data-processing systems. Another challenge relates to one of the arguments in favour of the use of Closed Material Procedures (CMPs) as practised in the UK: **the protection of mutual agreements between intelligence services that prevent disclosure of information**. The study asks: When intelligence materials are presented to courts, how are they scrutinised if the context in which they were collected is not known? As trust gained through cooperation is central to intelligence communities' work, to what extent does it build mutual secrecy that affects a fair trial?

---

[8] R. Aldrich (2009), "Global Intelligence Co-operation versus Accountability: New Facets to an Old Problem", *Intelligence and National Security* Vol. 24, No. 1, 26-56, February.

[9] The 'Five Eyes' designates the intelligence alliance comprising Australia, Canada, New Zealand, the UK and the US.

Thus the study acknowledges alleged unlawful practices of intelligence communities in collecting data. **The use of intelligence information in courts needs to be assessed in the context of surveillance scandals prompted by Snowden's revelations**. The claims of secrecy and its interference in judicial procedures cannot be disconnected from the practices of antiterrorist and (police-military) intelligence services. If the EUMS can organise freely the structure and tasks of their intelligence services, as well as the way in which the information they provide is used for national security purposes, they must also respect the rule of law and fundamental rights integral to the very foundations of EU constitutional principles as enshrined in the EU Treaties.

Effective judicial scrutiny plays a key role. The study examines how the use of intelligence materials in judicial proceedings interferes with accountability in cases where officials are suspected of wrongdoing and unlawfulness, and how the validity of the materials is assessed. It addresses the extent to which the use of intelligence materials and information affects the notion of 'evidence' itself. **The extent to which 'information' can be considered accurate, reliable and lawful 'evidence'** is crucial, owing to the potential consequences for the rights of the defence. The study thus asks: When secret information is used in judicial proceedings, are there any cross-examination mechanisms in place? Are the procedural rules and judicial practices deferential towards the executive and intelligence communities? The answers to these questions are of fundamental importance to ascertaining the validity and quality of materials and information presented before courts, as they have a great impact on the outcomes of a trial and can potentially breach fair trial standards.

Trust, mistrust and the balance of powers in liberal democracies

A third theme under analysis relates to the way in which EUMS judicial authorities in many instances have to presume or trust the legitimacy of national security and state secrets claims, and the validity (both in terms of accuracy, quality and lawfulness) of information provided by intelligence communities. The study presents court cases that illustrate how independent judicial authorities' trust in or deference to intelligence services is challenged by revelations of unlawful intelligence practices.

Snowden's revelations confirm the need for proper scrutiny of intelligence materials presented before courts. In fact, 'mistrust' may be crucial to implementing the principle of the separation of powers, which is at the heart of 'rule of law' standards. As described in a previous study on large-scale surveillance in Europe,[10] Snowden's revelations concerning bulk interception operations in the UK and the US prompted the central question of the scale of surveillance that is acceptable and proportionate in our democracies. Thus the legitimacy crisis sparked by the revelations is directly relevant to this study. It's a crisis not only of the legitimacy of intelligence communities but also of the efficiency of oversight mechanisms. In any case, the Snowden scandal has undoubtedly led to public distrust. This was one aspect underlined in the above-mentioned European Parliament Report on the US NSA and various Member State surveillance programmes and their impact on EU citizens' fundamental rights and transatlantic cooperation in Justice and Home Affairs, which declared that

> …trust has been profoundly shaken: trust between the two transatlantic partners, trust between citizens and their governments, trust in the functioning of democratic institutions on both sides of the Atlantic, trust in the respect of the rule of law, and trust in the security of IT services and communication…in order to rebuild trust in all these dimensions, an immediate and comprehensive response plan comprising a series of actions which are subject to public scrutiny is needed.

The use of intelligence materials in legal proceedings has led to various reactions and attitudes in EUMS judiciary systems. In some cases, judges have taken this opportunity to challenge the discretionary powers of the executive to use secrecy. In other cases, there is evidence that exceptional, secrecy-driven practices contaminate judicial procedures. The study assesses the extent to which this contamination destabilises the key principle of "equality of arms" that is at the basis of a fair trial, effective remedies and more generally the rights of the defence enshrined in Articles 47 and 48 of the EU Charter of Fundamental Rights.

[10] D. Bigo et al., op. cit.

Freedom of the press and protection of whistle-blowers

A fourth central issue raised by the use of secret materials before courts and the national security argument is **the pivotal role played by investigative journalism and whistle-blowers in disclosing matters of public interest and concern**. What happens when journalists disclose sensitive or classified information? To what extent does the use of the national security argument affect the work of investigative journalists and the disclosure of matters that are of public interest? The study examines several worrying examples where freedom of information has been restricted or where the protection of journalists' sources has been compromised in the name of national security.

1.2 Study methodology, terminology and structure

1.2.1 Methodology

This study conducts a comparative analysis of the legal regimes, interpretations by domestic and European tribunals as well as key developments and contemporary practices concerning the use – or non-use – of intelligence information as evidence during trials in the following EU Member States: the United Kingdom, France, Germany, Spain, Italy, the Netherlands and Sweden. The choice of these seven Member States is meant to provide a selection of national historical, constitutional and legal backgrounds and experiences of allowing (or not allowing) the use of intelligence information and state secrets in courts. It is also designed to illustrate different conceptualisations of 'state secret' or 'national security' in national legislation. Five of these EUMS were included in the previous study conducted jointly between the Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS) and the Centre d'Etudes sur les Conflits, Liberté et Sécurité (CCLS): the UK, Sweden, France, Germany and the Netherlands.[11]

Findings are based mainly on consultation with a new network of independent scholars and experts established specifically for this study. Consultation culminated in the 'Country Fiches' in Annex 5, most of which were drafted by the leading national scholar on the basis of questionnaires completed by academics, practitioners and civil society actors. The national scholar summarised questionnaire findings, thus ensuring independent analysis. Research of primary and secondary sources rounded out overall study objectives and scope.

In addition, two focus groups were organised in order to present the key findings of a first draft of the study and to receive comments and inputs: a focus group of civil society organisations active in the debates over the use of CMPs and intelligence information in courts and counterterrorism, and a focus group of practitioners from the private, legal and public sectors. Two focus group meetings took place on 30 October 2014 at CEPS in order to allow for comments on a draft outline of the study. The Proceedings Report of these meetings is included in Annex 4. Results from these discussions were taken into consideration when drafting the final version of the study.

1.2.2 Terminology and concepts

The analysis of the use of intelligence materials in courts requires clarifying beforehand concepts and terminology used in the study.

The study uses the concept of **'intelligence materials'**. In doing so, it includes information gathered, exchanged or stored by 'intelligence communities' (police, secret services, military or other law enforcement authorities). Each of the EUMS under scrutiny has its own specificities regarding intelligence-gathering. The study thus deals with both 'human intelligence' (gathered from a person on the ground) and 'signals intelligence' (gathered from interception of signals), which, depending on the institutional structures of the EUMS, can be operated by the police, dedicated special services and/or the military.

Reference is also made to **'information'** and **'intelligence'**, while taking into account the blurring of the distinction between these two terms in practice. In principle, the distinction between information and intelligence is well-established. Information consists of bits of data that, when combined and viewed together with relevant background knowledge, may be used to produce intelligence, which informs the actions and decisions of policing organisations. However, as previous scholarly contributions have rightly suggested,

[11] Ibid.

there is increasing confusion between 'information' and 'intelligence' in contexts where there is strong reliance on intelligence in policing activities.[12] Peter Gill provided insights on how intelligence-led policing, specifically in the UK, grew considerably in the 1990s due to public rejection of traditional methods such as interrogations and confessions.[13] Previous reports for the LIBE Committee of the European Parliament have underlined the more recent drive for intelligence policies in EU internal security strategies.[14]

Intelligence-led policing is a law enforcement practice and strategy that focuses on the reduction of crime through the use of criminal (predictive) analysis and intelligence. In this context, the distinction between 'information' and 'intelligence' is increasingly blurred. As the work of Gary Marx has amply demonstrated, it is not uncommon to refer to any information that comes into police hands by covert means as intelligence. Innes and Sheptycki have highlighted that this elasticity of terminology should serve as a warning: "As the practices of intelligence-led policing have spread internationally and across a variety of policing-type institutions, the terms associated with it have become subject to some looseness of definition".[15] This has important consequences for this study, as such 'looseness' can lead to **ambiguity in the nature and validity of secret materials when presented as 'evidence' in court**.

Indeed, this raises a subsequent challenge: **the distinction between 'intelligence' and 'evidence'.** As noted by Kent Roach, "[T]he ideal types of intelligence and evidence are rooted in a Cold War consensus in which intelligence could be collected to inform government about security risks with the expectation that it would never be publicly disclosed beyond the narrow range of those who 'need to know' and alas the occasional mole. In contrast, evidence was collected after a crime was committed. It could be subject to cross-examination and adversarial challenge and it would be used in a public trial to prove guilt beyond a reasonable doubt". Roach argued that "although there have always been departures from the ideal types, the creation of sweeping new terrorism offences after 9/11 has blurred the traditional distinctions between intelligence and evidence. Such new offences reflect an intelligence mind-set that focuses on threats, risk, associations and suspicion as opposed to an evidence or criminal law mind-set that focuses on acts, accomplices and guilt. One implication of the blurring of the distinction between intelligence and evidence is a convergence between the work of police forces and security intelligence agencies in terrorism investigations. This convergence is driven in part by the demands of prevention".[16]

Therefore, **this study takes into account the effects and consequences of preventive logic in policing, which affects both the status of the suspect and the nature of the evidence used against him**. Special attention is therefore given to the challenges posed by the use of the concept of 'secret evidence' and, in particular, the extent to which the quality and the robustness of 'secret evidence' can be properly scrutinised.

The study often refers to the concepts of **'national security'** and **'state interest'**. These concepts encompass many different meanings and conceptual features across the EUMS under examination, and these specificities are detailed in Section 1.6. Our research thus addresses the risk of secrecy being used in the interests of state authorities. While the use of secrecy may be legitimate, it can neither be entirely discretionary nor arbitrary or unfettered, nor can it be used to the detriment of accountability and the democratic rule of law with fundamental rights. Fundamental questions concern the role of the executive in a liberal-democratic State and its discretionary flexibility over 'what' constitutes an issue of national security that would require secrecy, and the power of oversight and room for manoeuvre left to parliaments and the judiciary.

1.2.3 Structure

While addressing the issues and challenges raised above, Section 1 of the study provides a comparative assessment across the Member States under examination of the ways in which their national regimes and

---

[12] M. Innes and J. Sheptycki (2004), "From detection to disruption: intelligence and the changing logic of police control", *International Criminal Justice Review*, Volume 14.

[13] P. Gill (2000), *Rounding up the usual suspects: developments in contemporary law enforcement intelligence*, Aldershot, Hants, England; Burlington, VT: Ashgate.

[14] J. Jeandesboz, E-P. Guittet and A. Scherrer (2011), "Developing an EU Internal Security Strategy, fighting terrorism and organised crime", Report for the LIBE Committee.

[15] Innes and Sheptycki, op. cit.

[16] K. Roach (2010), "The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations", in N. McGarrity, A. Lynch and G. Williams (eds), *Counter-Terrorism and Beyond,* London: Routledge, pp. 48-68.

judicial practices allow or do not allow for the use of intelligence information as secret evidence. It also analyses how the notions of 'state secrets' and 'national security' are understood and implemented in their relevant legislation, as well as how these concepts have been used, interpreted or dealt with by competent courts. In particular, the analysis covers how the lack of scrutiny by the judiciary over processes of classification/declassification of information prevents independent judicial scrutiny and effective remedies for suspects.

Section 2 examines the extent to which the judiciary is prevented from accessing information of the utmost relevance for delivering justice and safeguarding the interests at stake, or information that may constitute incriminating evidence when the State is engaged in alleged unlawful practices infringing human rights. This raises the question of the deferential or minimal degree of scrutiny exercised by some judicial authorities towards the executive in cases where national security and state secrets are invoked. Section 3 thus analyses the role played by supranational legal principles and standards developed by the European Court and Human Rights and the Court of Justice of the European Union and how they limit States' actions and decisions that interfere with fundamental rights.

Our analysis of EUMS laws and practices concerning intelligence materials introduced in legal proceedings, and of EU standards in the field, sheds an interesting light on two connected challenges: freedom of the press and protection of 'whistle-blowers'. Section 4 describes the ways in which these rights and freedoms are often compromised and jeopardised when national security issues are raised. This Section argues that derogations from freedom of the press and protection of 'whistle-blowers' in the name of national security not only obstruct public awareness as regards the functioning of their institutions, but also weigh heavily on the reliability of intelligence materials introduced in judicial proceedings.

2. National regimes and practices in EU Member States on the use of intelligence information by courts

KEY FINDINGS

- The United Kingdom stands as an exception in the European landscape when examining the use of secrecy during trials. The use of 'closed material procedures' (CMPs) in judicial proceedings is provided for in national legislation. CMPs allow sensitive intelligence material to be introduced in secret hearings in which only the judge and special advocates have access to the material.
- Since the introduction of the 2006 Act on Shielded Witnesses, the Netherlands has also been able to 'shield' witnesses from intelligence communities in the interest of national security at an "in camera" (closed proceedings/hearings) pre-trial stage.
- Germany, Spain and Sweden have a range of judicial practices through which certain evidence may be hidden from a party during trials.
- In the majority of these cases, the principle of "equality of arms" in a trial is compromised, as at least one party does not have full access to the evidence admissible in court.
- The use of secret evidence is categorically not permitted in France and Italy. However, judges face challenges linked to the very difficult process of declassification of intelligence materials and where the executive exercises great power over the use of secrecy.
- In the context of transnational exchanges of intelligence, the question of 'mutual secrecy' arises. International security agreements with foreign States can mandate a system of 'mutual respect' of protected secrets. In the UK, for example, the main rationale behind the introduction of CMPs in civil courts is to avoid classified intelligence provided by foreign allies (mainly the United States) from being disclosed during court proceedings.
- The disparate practices in the Member States examined also mean that claimants and defendants may be protected differently across the EU due to a patchwork of practices and standards of protection.

This Section examines relevant national legal regimes governing the use of intelligence information during trials and the extent to which these allow for secret evidence and closed material procedures. The examination also covers the existence of indirect judicial practices allowing for the use of intelligence information or materials as secret evidence during a trial or court sessions held in camera. The various ways in which the notion of 'national security' is framed and understood as grounds for classifying or declassifying information or keeping a trial 'secret' is also included.

The analysis of the seven EU Member States under investigation shows the diversity of constitutional and organisational settings when it comes to the relationship between judicial accountability, state secrets and intelligence. Particular attention is given to the situation in the United Kingdom. Its legal regime constitutes an exception in comparison to other EUMS when it comes to the use and acceptance of secret evidence by competent courts. The UK regime includes an enlarged system of 'closed material procedures' (CMPs) covering criminal, administrative and civil proceedings. During a CMP, the judge has the power to decide, upon request by the government, whether to present evidence to the court in secret without the defendant being granted access to that information. By their very nature, **CMPs pose particular challenges to fundamental rights and the open justice and adversarial principles in judicial proceedings**.

The other EU Member State where the use of intelligence information as secret evidence is provided for by law is the Netherlands, where the 2006 Act on Shielded Witnesses lays down a special procedure allowing for anonymous testimonies by intelligence officials.

The other EU Member States under analysis – Germany, Sweden, Spain, France and Italy – do not have such procedures. They instead show divergent legal regimes and judicial practices covering the interface between intelligence, state secrets and the rights of the defence on the one hand and intelligence community accountability on the other. These are deeply rooted in their respective constitutional, political and legal

structures. In some of these EU Member States the constitutional framework and practices have formally forbidden the use of secret evidence in trials, yet they still present indirect uses of intelligence materials and accept state secrets practices. What are the features characterising these regimes and judicial practices, and how do they differ when compared to CMPs in the UK? When secret information is introduced in judicial proceedings, or when information is classified as state secrets, are there any mechanisms of cross-examination and oversight in place?

The following subsections examine the features characterising the use of intelligence information in judicial proceedings in the selected group of EUMS. **Two situations are covered: cases in which intelligence services seek to use information/materials against an individual, and cases in which the executive/intelligence communities are accused and evidence cannot be used due to state secrets**. First, we start by looking at the context in the United Kingdom and its use of CMPs (1.1). Second, we present the case of the Netherlands, which allows anonymisation of testimonies for national security reasons (1.2). Third, we will present those Member States where judicial practice has shown various degrees of acceptance of classified intelligence as evidence in court despite not having any formal legislation providing for it (1.3). Fourth, we will look at those Member States where the use of secret evidence in trials is formally forbidden under their constitutional regimes (1.4). This raises questions of classification and declassification of documents by the government, which are explored in detail (1.5). Finally, we present the ways in which the EU Member States under analysis justify the use of secrecy in judicial proceedings (1.6).

2.1 The United Kingdom and the use of closed material procedures (CMPs)

The United Kingdom has a specific piece of legislation allowing for the use of classified intelligence information as evidence in court.

The adoption in 2013 of the Justice and Security Act (JSA)[17] in the UK opened up important debates over the use of intelligence information and so-called 'closed material procedures' (CMPs) in courts and in judicial proceedings. CMPs are secret court hearings where only the judge and security-cleared special advocates are given access to sensitive intelligence material.

While the JSA codified the use of CMPs in any civil case in which it is argued that disclosure of material would harm national security, the use of CMPs was first introduced by the Special Immigration Appeal Commission Act 1997, which permitted the government to rely on closed material in seeking to justify deportation on national security grounds. Further pieces of legislation have extended the use of CMPs to other areas of law:

- the Anti-Terrorism, Crime and Security Act 2001,[18] no longer in force, which permitted the permanent detention of foreign nationals suspected of being terrorists;
- the Prevention of Terrorism Act 2005[19] and the Terrorism Prevention and Investigation Measures Acts 2011,[20] which permitted restrictive measures to be imposed on those suspected of involvement in terrorism;
- the Counter-Terrorism Act 2008,[21] which grants the UK Treasury the opportunity not to disclose material if contrary to the public interest;
- the Justice and Security Act of 2013 mentioned above, which extends the use of CMPs to the main civil courts, for example, for claims for damages in relation to extraordinary rendition and alleged torture cases.

The main rationale behind the introduction of CMPs to civil courts is to avoid threats to national security and disclosure of classified intelligence provided by foreign allies of the United Kingdom (mainly the United States) during court proceedings. The Binyam Mohammed case of 2010, presented below in Section 2,

[17] See the full text of the Act at www.legislation.gov.uk/ukpga/2013/18/contents/enacted/data.htm.

[18] See the full text of the Act at www.legislation.gov.uk/ukpga/2001/24/contents.

[19] See the full text of the Act at www.legislation.gov.uk/ukpga/2005/2/contents.

[20] See the full text of the Act at www.legislation.gov.uk/ukpga/2011/23/contents/enacted.

[21] See the full text of the Act at www.legislation.gov.uk/ukpga/2008/28/pdfs/ukpga_20080028_en.pdf.

allowed former Guantanamo Bay detainees to obtain compensation from the British government for having been subject to cruel, inhuman and degrading treatment – the case relied on evidence from the US Central Intelligence Agency, which proved the UK's knowledge of the detainees' mistreatment. While the UK government insisted on keeping this evidence as closed material, the Supreme Court forced the government to disclose the documents during an open trial. As a direct result of this case, UK legislators introduced the Justice and Security Act in 2013 to allow the use of CMPs during civil trials, and therefore prevent effective judicial scrutiny of its mutual state secrets cooperation with the US.[22]

CMPs introduced in the JSA extend the use of "special advocates" to any civil case. Special advocates are security-vetted lawyers who are permitted to participate in CMPs and represent claimants. Special advocates differ from normal lawyers who represent claimants. Special advocates are permitted to disclose to clients a simplified summary or 'gist' of intelligence material used in secret hearings, while withholding specific details. The special advocates are instructed to protect the appellant's interests and may argue against admitting material on the grounds that it would prevent a fair trial, but they may not communicate with the appellant without the government's permission and they can never communicate about the secret evidence. The court then considers this secret material during a closed session in the absence of the appellant and his/her legal advisers, but with the assistance of the special advocate. The special advocates examine the relevance of the secret intelligence information to the case, its admissibility (would it prevent a fair trial?) and the legitimacy of its classification (would disclosure really harm national security?). The intended significance of having special advocates to rebalance the rights of the accused has been criticised by scholars:

> Special advocates serve both a 'disclosure' and 'representative' function...However, once closed material is disclosed to the special advocate he or she may not take instructions from or speak to the affected person. The inability to consult with the affected party is the chief subject of complaints regarding the use of special advocates. In addition, special advocates object to the lack of access to independent experts or evidence and the practical inability to call witnesses[23]

The House of Lords has also criticised the serious limitations on the ability of special advocates to challenge the government's use of closed materials:

> The special advocates felt that more could be disclosed than the Government was prepared to permit, but they are not really in a position to challenge such objections to disclosure, because they do not have access to any independent expert evidence. The special advocates have no means of gainsaying the Government's assessment that disclosure would cause harm to the public interest…In addition to this…, their evidence to us identified another significant limitation in practice: the problem of late disclosure of closed material…The effect of late disclosure of the closed material to the special advocates is seriously to compromise their ability to discharge their important function, because it leaves them with insufficient time to scrutinise the closed material and to challenge the Government's reasons for the material being closed."[24]

The use of this procedure under the Special Immigration Appeal Commission Act was and remains highly controversial. The JSA has further emphasised the controversy. **The use of CMPs might prevent claimants from being aware of all the allegations made against them, which has been criticised on the grounds that parties are no longer on an equal footing.**[25]

For its supporters, CMPs as introduced by the JSA aim to provide solutions to the challenges posed by the increasing number of civil court proceedings in which sensitive information is relevant. In a green paper

---

[22] Summary based on the answers of one of the UK experts in the questionnaire.

[23] A. Lynch, T. Tulich and R. Welsh (2014), "Secrecy and Control Orders: The role and vulnerability of constitutional values in the United Kingdom and Australia", in D. Cole, F. Fabbrini and A. Vedaschi, *Secrecy, National Security and the Vindication of Constitutional Law,* Cheltenham: Edward Elgar, p. 159.

[24] See: House of Lords and House of Commons Counter-Terrorism Policy and Human Rights (2010), Annual Renewal of Control Orders Legislation 2010 - Human Rights Joint Committee, Sixteenth Report, HL 64/HC 395, p. 21.

[25] J. Jackson (2013), "Justice, Security and the Right to a Fair Trial: Is the Use of Secret Evidence Ever Fair?", *Public Law*, 720-736.

presented to the UK Parliament in October 2011,[26] the Secretary of State for Justice Ken Clarke provided the following supporting arguments for the extension of the use of CMPs to civil cases:

- The very nature of intelligence information makes its disclosure in an open courtroom impossible, as this disclosure would endanger national security and/or breach international cooperation and agreements in the field of intelligence sharing.
- The existing concept of Public Interest Immunity (PII) in the UK, which allows for one litigant to refrain from disclosing evidence to the other litigants where disclosure would be damaging to the public interest, is not satisfactory, as it excludes key material from judicial proceedings. Too often, judges have to deliver judgments without being able to take into account key information.
- The introduction of the JSA makes CMPs more widely available in civil proceedings for use in instances in which sensitive material is relevant to the case.

In his Green Paper, Ken Clarke insisted:

> [T]he legislation seeks to find solutions that improve the current arrangements while upholding the Government's commitment to the rule of law. We urgently need a framework which will enable the courts to consider material which is too sensitive to be disclosed in open court, but which will also protect the fundamental elements that make up a fair hearing.[27]

The UK security services publicly supported the bill, arguing that it would make it possible to bring to justice cases that had previously been denied on security grounds. Another argument put forward by intelligence officials has been that such procedures would improve accountability of the intelligence communities. MI5 Director Jonathan Evans declared:

> At present our ability to account for our actions in the courts is constrained by the fact that sensitive national security related material relevant to civil proceedings can only be considered in open court. This means that such material cannot in practice go into court at all. This situation is bad for us, bad for the other party to proceedings and bad for the administration of justice.[28]

However, and despite these official statements, it is precisely on this question that the proposal was attacked by its opponents, who argued that **secret justice was not compatible with a fair trial, could prevent accountability, and could further damage public confidence.**

Special advocates who already operate in CMPs under the Special Immigration Appeal Commission Act declared:

> CMPs represent a departure from the foundational principle of natural justice that all parties are entitled to see and challenge all the evidence relied upon before the court and to combat that evidence by calling evidence of their own. They also undermine the principle that public justice should be dispensed in public.[29]

Civil liberties and human rights representatives have publicly criticised the bill[30] for the following reasons:

- The use of the special advocate procedure excludes non-state parties from a hearing or any knowledge of the secret evidence given in CMPs. The use of CMPs means that the person affected is unlikely to know the case against him or her, which is a breach of the right to a fair trial.

---

[26] Green paper presented to the UK Parliament in October 2011 by the Secretary of State for Justice Ken Clarke. Available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/228860/8194.pdf.

[27] Ibid.

[28] Address at the Lord Mayor's Annual Defence and Security Lecture by the Director General of the Security Service, Jonathan Evans, 25 June 2012. Available at www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html.

[29] Justice and Security Green Paper: Response to consultation from special advocates, 16 December 2011. Available at: http://consultation.cabinetoffice.gov.uk/justiceandsecurity/wp-content/uploads/2012/09_Special%20Advocates.pdf.

[30] See among others the JUSTICE briefing of 5 July 2013 on "Justice and Security Act 2013: Civil Procedure (Amendment No 5) Rules 2013", available at www.justice.org.uk/data/files/resources/354/JUSTICE-Civil-Procedure-_Am-No5_-Rules-Briefing-July-2013.pdf.

- The use of special advocates in closed hearings does not provide sufficient protection against the risk of an unfair trial.
- The executive has discretionary powers over which materials are presented.
- Evidence derived from secret intelligence sources may not be as robust as that used in an open court process.

David Anderson QC, Independent Reviewer of Terrorism Legislation, conceded that the bill did not treat parties to civil litigation on an equal basis and that the use of CMPs provided an impetus for the government to choose not to put material into a CMP where it would assist the claimant.[31]

During the focus group discussions on 30 October 2014, summarised in Annex 4, some participants noted that the UK is a common law system, in which the adversarial principle predominates in judicial proceedings, while the rest of continental Europe uses the civil law system and the inquisitorial system for the most part. The notion of the separation of powers in the UK implies the idea of 'balancing' the powers rather than strictly respecting the separation of powers, which is somewhat different from the other EU Member States. **It is thus very difficult to conceive that the use of CMPs might be exported from the common law/adversarial context of the UK to EU Member States that use the civil law/inquisitorial system**.

The UK debates over CMPs offer much food for thought in our study. As we have seen above, the UK has introduced exceptional procedures regarding the use of secret evidence in courts. The use of information and materials provided by intelligence communities, which are kept secret and not disclosed to the defendants in the name of national security, **not only sparks debate in terms of respect for fair trials, equality of arms and fundamental rights**. It also poses important questions linked to **the changing practices of the intelligence communities and the extent to which materials provided by these services in courts is properly scrutinised by judicial authorities**. Furthermore, the use of CMPs not only raises specific legal challenges; it also raises questions about the separations of powers, democratic control and the principle of open justice.

2.2 The use of secrecy in the Netherlands – the Act on Shielded Witnesses

In **the Netherlands**, the Act on Shielded Witnesses (*Wet afgeschermde getuigen*) introduced in 2006[32] aims to improve the use of information collected by the intelligence and security services as evidence in criminal proceedings. It creates a special procedure in which members of the two principal Dutch intelligence services (AIVD and MIVD) may be heard before a special examining magistrate (located in Rotterdam) at a pre-trial stage. The examining magistrate decides whether, in the interests of national security, particular information must remain secret and whether the witness should be 'shielded' (i.e. remain anonymous). In most cases the procedure is in camera and ex parte, and the report of the hearing will only be submitted to the parties with the consent of the shielded witness. During the in camera procedure, a list of questions for the witness is handed to the special magistrate by the counsel representing the suspect and the trial judge, for whom the hearing is shielded.[33] It is possible, but not common, for the trial participants to be present when the examining magistrate assesses the value of the intelligence, but the witness is always shielded. Since 2006, not only AIVD information, but also information from foreign intelligence services, has been accepted as evidence.

The Piranha case is a key example of the admission of intelligence evidence in court. In this case, which started in 2005, six individuals of Dutch-Moroccan descent were charged with constituting a terrorist network. The case is particularly interesting for the way in which intelligence information constituted the central component of the evidence presented by the public prosecutor, which included a CD-ROM collected by the AIVD containing the video of a farewell message by one of the main suspects. During the Piranha

---

[31] Evidence given by David Anderson QC, Joint Committee on Human Rights, 19 June 2012. Available at www.parliament.uk/documents/joint-committees/human-rights/Uncorrected_Transcript_Justice_and_Security_Bill_David_Anderson_19062012.pdf.

[32] See the full text of the Act (in Dutch) at www.eerstekamer.nl/behandeling/20061024/publicatie_wet_14/document3/f=/w29743st.pdf.

[33] Refer to the Netherlands Country Fiche in Annex 5.

case, the defence counsel was unable to receive the full transcripts of AIVD evidence or question all intelligence officers.[34]

Intelligence in general has been used in administrative, civil and criminal court cases for decades, as well as in immigration law. It is – by and large – up to the judge to consider whether intelligence is admitted in a case, but there is very limited scope for assessing the legitimacy of the intelligence information provided (the judge or public prosecutor is supposed to presume the legitimacy of the information). In administrative procedures, administrative law makes it possible to give the judge permission to see the closed material. This is not so clear-cut in criminal cases as courts differ in their opinion.[35] The procedural guarantees and the protection standards for the rights of the defence under the Shielded Witnesses Act are limited because **the witness's reliability cannot be tested by the defendant** due to the duty of secrecy and the fact that the procedure is ex parte and in camera, and because there is no right of appeal to challenge the decision to grant anonymity. As Coster van Voorhout (2007) has rightly highlighted:

> As the defence remains unaware of the identity of the adverse witness, and cannot observe his demeanour or perform oral adverse-questioning in the presence of the accused, the defence is restricted in its efforts to challenge the case. The examining magistrate, who generally has to act as if he were acting for both parties, could, in principle, compensate for this...However, the examining magistrate cannot fully examine the witness either, given that the officer's duty of secrecy precludes him from answering any questions besides questions concerning (i) being an intelligence officer, and (ii) his willingness to testify.[36]

It was also argued that, in the Netherlands, "the right to anonymity as a safeguard of state security seems to prevail over the right of the defendant to a fair trial."[37] It should also be noted that the shielded witness procedure in the Netherlands has mainly been discussed in the light of Article 6 ECHR rather than the Dutch constitution, as the constitution does not contain an article on the right to a fair trial. A proposal by the Dutch government to include a provision on the right to a fair trial in Article 17 of the constitution is currently being discussed.[38]

2.3 Member States where the use of classified intelligence information as evidence is practised by national courts

A number of EUMS, in particular Germany, Spain and Sweden, do not formally allow the use of classified intelligence information as evidence in court in their national laws. The use of intelligence information might, however, still occur in some judicial practices or may be allowed under very specific circumstances. Certain safeguards have been put in place (in Germany) as regards the rights of the defence. Our analysis shows a tendency in Sweden and Germany to use so-called "second-hand" evidence, or "hearsay" evidence, which is obtained indirectly through another witness or report but has not been seen or heard directly. Another feature of the use of intelligence information in some EUMS covered by our analysis is the organisation of a separate, closed, in camera session in which the classified information is shown to a carefully selected audience, **but kept hidden from the claimant or defendant**. This is the case in the United Kingdom and in the Netherlands (as presented above), but also in Germany.

By way of illustration, in **Germany,** secret evidence is forbidden in trials. However, certain testimonies or anonymous information based on secret evidence might be accepted by the court under certain conditions.

---

[34] For more on the *Piranha* case, see, among others, Q. Eijkman, D. Lettinga and G. Verbossen (2012), "Impact of Counter-Terrorism on Communities: Netherlands Background Report", Open Society Foundations, Institute of Strategic Dialogue, London; as well as de Goede, M. and de Graaf, B. (2013), Sentencing Risk: Temporality and Precaution in Terrorism Trials, *International Political Sociology*, 7(3), 313-331.

[35] Answers provided by one of the Dutch experts in the questionnaires.

[36] J. Coster van Voorhout (2007), "Intelligence as Legal Evidence: Comparative Criminal Research into the Viability of the Proposed Dutch Scheme of Shielded Intelligence Witnesses in England and Wales, and Legislative Compliance with Article 6 (3) (d) ECHR", *Utrecht Law Review*, 2, 2, p. 129.

[37] S. Van der Hof, E. J. Koops and R. E. Leenes (2009), "Anonymity and the Law in the Netherlands", in V. Steeves, C. Lucock and I. Kerr (eds), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, New York: Oxford University Press, p. 507.

[38] See www.liberties.eu/en/news/right-to-a-fair-trial-the-netherlands.

As a general principle, and unlike the above-described situations in the UK and the Netherlands, German courts cannot base their judgments on secret information. This was confirmed by the Federal Constitutional Court in 1981.[39] Article 103 of the German Constitution (*Grundgesetz*) guarantees to anyone the right to be heard, from which the Federal Constitutional Court deduced the right of all parties to a court procedure to know all evidence on which the court envisages basing its judgment, and the right to comment on all such evidence. As Nikolaus Marsch puts it:

> As a consequence of the constitutional enshrinement of a right to be heard and the jurisprudence of Federal Constitutional Court with regard to this fundamental right, closed material court procedures are not allowed in Germany and an introduction by the legislator would be unconstitutional.[40]

"Second-hand" (or "hearsay") evidence based on classified intelligence information might still be used in court, in the form of anonymous informer testimony or an intelligence officer describing a classified document, for example.

The Friedrich Cremer case in 1980 constitutes a good example of such indirect use of intelligence information. Mr Cremer was convicted based on the interrogation of a former East German spy, but this spy was never summoned to the court due to the refusal by the German intelligence service to reveal his location for national security reasons. The court accepted the use of the minutes of the spy's interrogation as evidence against Mr Cremer.[41] The Federal Constitutional Court accepted the use of second-hand evidence on the condition that the lower probative force of this evidence be taken into account by the court.[42] Essentially, the Federal Constitutional Court held that "a concrete threat is required to justify any intrusion into basic rights".[43]

An intermediate in camera procedure is possible when intelligence services or the Ministry of Interior refuse to submit intelligence information to the courts on grounds of the "protection of state interests". This refusal can be challenged before an administrative court, which will assess the legality of the administrative decision not to disclose the documents in an intermediate closed session.[44] This procedure is meant to strengthen the constitutional right to a judicial remedy and to balance the interests of the claimant with the "protection of state interests" argument to keep evidence secret. This in camera procedure was introduced into German legislation to comply with a decision of the Federal Constitutional Court in 1999.[45]

In **Spain**, articles 9 and 24 of the Spanish Constitution prevent any kind of conviction of a person without knowing the rationale or the grounds behind this conviction. The use of closed material procedures in Spain would be deemed unconstitutional. However, since 2000, judicial practice has allowed intelligence information to be introduced during trials through second-hand evidence based on testimonies of officials who have not had direct access to the intelligence documents. Such information is deemed 'confidential' and accepted as valid evidence without being properly presented in court. Confidential testimonies have sometimes been accepted by the jurisprudence;[46] for instance, extradition requests for suspected terrorists by United States courts have been approved by Spanish courts on the basis of secret evidence.[47] During our 30 October focus groups, summarised in Annex 4, participants also noted that courts in Spain accept intelligence information from foreign police agencies, such as the Serious and Organised Crime Agency (SOCA) in the UK. Some of the evidence might be cross-examined when the judge allows it, but the judges in national and regional jurisdictions in Spain have differing views on whether to allow cross-examination.

---

[39] See Federal Constitutional Court, 26.5.1981, 2 BvR 215/81.

[40] See Annex 5: Germany's Country Fiche, p. 1.

[41] See the Germany Country Fiche in Annex 5.

[42] See Federal Constitutional Court, 26.5.1981, 2 BvR 215/81.

[43] For an examination of the German Federal Constitutional Court case law, see: M. Vashakmadze (2014), "Secrecy vs. Openness: Counterterrorism and the role of the German Federal Constitutional Court", in Cole, Fabbrini and Vedaschi (eds), op. cit., pp. 44-56.

[44] See Section 99 of the Code of Administrative Court Procedure.

[45] See Bundesverfassungsgericht, 27.10.1999, 1 BvR 385/90 as well as Germany's Country Fiche in Annex 5 for a more detailed analysis of the case law.

[46] Answers by one of the Spanish experts in the questionnaire.

[47] Ibid.

Judicial practice has shown that classified materials have been used or accepted by courts to convict suspected terrorists in **Sweden**. The case of Ali Berzengi and Ferman Abdullah in 2005 demonstrated that classified material from US intelligence services was accepted as evidence to rule against two individuals accused of preparing terror crimes.[48] The evidence was presented orally by an FBI representative and not in written form, which is contrary to standard legal practice in Sweden. The rationale behind the court's reliance on secret information was that the court could trust sources coming from "international legal assistance".[49]

2.4 Member States where there is no use of secret evidence in trials

In some of the EUMS covered by this study, the use of 'secret evidence' in trials or CMPs is refused by courts. No legislation or judicial practice allows for the use of secret documents or classified information from intelligence agencies during a trial. As we will see in the next subsection, however, this raises other challenges when it comes to the use of 'state secrets' as a way to prevent or limit judicial oversight of executive and intelligence communities' practices.

In **France**, the notion of 'secret evidence' does not exist in the context of a trial: a confidential document or information is not accepted by judges. In criminal law, evidence has to be openly debated and cannot be obtained illegally. A French expert summarised the context in an answer to our questionnaire:

> French law is based on an absolute prohibition of the communication of classified materials protected by the '*secret défense*', including to judicial authorities. This means that any transmission of classified information to the judge, who is not authorised to have access to classified materials because of the rule of separation of powers, is a direct violation of the secrecy of national defence, which is punishable by criminal law. The judiciary can only have access to a record if it has previously been declassified, following a procedure established by law.[50]

The principle of equality of arms in France stems from Articles 1 and 6 of the Declaration of the Rights of the Man and of the Citizen of 1789, but was only established in law in 2000 as an addition to the Penal Procedures' Code, directly influenced by Article 6 of the European Convention on Human Rights.[51]

Similarly, in **Italy**, the use of secret evidence in trials is excluded by the Italian legal system. As Arianna Vedaschi puts it:

> As a general principle, in Italian criminal law, each and every piece of evidence which the Public Prosecutor or judge uses during a trial must be disclosed to the defendant and his/her defence counsel. No evidence can ground a judgment in a criminal court, unless it was disclosed to the defendant, for his/her perusal, in the course of the trial.[52]

Evidence that is not disclosed to the defendant is not allowed in the Italian criminal law system. This is based on the protection of the rights of the defence and the right to a fair trial in Articles 24 and 111 of the Italian Constitution. Italy – together with Germany and Spain – is another example of a Member State where using closed materials during judicial proceedings would be unconstitutional. In addition, when a public servant is requested to testify on matters deemed to be covered by the so-called "state secrets privilege", he/she is obliged to refrain from answering the questions or otherwise revealing the information at stake.[53]

---

[48] See the Ali Berzengi and Ferman Abdullah case (Svea High Court), 2005, presented in Sweden's Country Fiche.

[49] Stockholms tingsrätt (2005), "Dom i mål B 2965-04".

[50] Answer by one of the French experts in the questionnaire.

[51] J.P. Dintilhac (2003), "L'égalité des armes dans les enceintes judiciaires", in the 2003 Annual Report of the Cour de Cassation, available at:

www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2003_37/deuxieme_partie_tudes_documents_40/tudes_theme_egalite_42/enceinte_judiciaires_6255.html.

[52] Refer to the Italy Country Fiche in Annex 5.

[53] According to Article 202 of the Italian Code of Criminal Procedure as well as Article 41 of Law 124/2007. This duty is reinforced by the provisions (Articles 261-262) of the Italian Penal Code that severely punish those who reveal state secrets or other classified information.

In both Member States where the use of secret evidence in trials is categorically refused by courts, the very existence of a case rests on the willingness of the government to declassify the evidence and make it available to the parties and the courts involved. This is what the next subsection explores.

2.5 Classification and declassification of secret intelligence information

Questions related to the executive's power to classify or declassify information and to the system of accountability applicable to that power are of central importance to our analysis. This is especially the case in those instances where it is the executive or its intelligence services that are being charged with wrongdoing or abuses and the information needed by courts to prove their unlawful activities is classified as 'state secrets'. "Declassification" is the process of making certain documents available to the public after a period in which these documents were classified as secret and restricted. In other EUMS, such as the UK, other terminological references, such as "disclosure", are also used, though the terms are not entirely interchangeable.

In **France**, as examined above, confidential information is not accepted by courts. The principle of equality of arms in trials means that all parties must have the right to openly debate and contradict the evidence used against them. If a document is classified as secret due to national security concerns, it has to be declassified before it can be accepted as evidence in judicial proceedings. This has caused a number of challenges, notably in the case of the 2002 Karachi attacks where judges have repeatedly asked for certain documents to be declassified, with limited success.[54] The Parliamentary investigation into this case was also limited due to declassification issues. Declassification of secret intelligence information rests exclusively in the hands of the executive, with very limited oversight by Parliament and absolutely no involvement of the judicial authorities. The *Commission consultative sur le secret de la défense nationale* (CCSDN) is an independent administrative authority, which delivers opinions on declassification issues that are non-binding on the government. Parliamentary oversight, established by 2007 legislation,[55] allows a small number of members of Parliament in the "Parliamentary delegation for intelligence" to have access to a limited amount of intelligence information. Their activity remains restricted to intelligence and they cannot obtain all classified evidence.[56]

In addition, **international agreements may also prevent the declassification of intelligence information**. Security agreements binding France to foreign States, for example, can be used to organise a system of **mutual respect of protected secrets**. Such agreements ensure that each State will protect the other State's classified information in the same way as its own classified information. As Brodeur and Dupeyron (2003) have pointed out, the French system completely lacks public transparency and parliamentary control. In their view:

> All operations of the [French security and intelligence services] are covered by unimpeachable state secrets and, occasional revelations brought about by investigative journalism or media leaks excepted, very little information on the activities of the French [security and intelligence services] ever reaches the public…In sum, the control of the French [security and intelligence services] is not firmly grounded in law.[57]

The use of classified materials is not allowed in courts in **Spain**. If a classified document is introduced in a courtroom as evidence, it must observe the common judicial rules on evidence as laid down in the Spanish legal order.[58] In this context, lawyers of all the parties must be able to examine such evidence. However, as we have described above, cases in which evidence has been kept confidential have taken place in judicial practice. "Classified materials" in Spain can take two forms: either "secret" or "confidential", according to

---

[54] See France's Country Fiche for a detailed analysis of the investigation on the circumstances of the attack on 8 May 2002 in Karachi, in which 14 people lost their lives.

[55] Law No. 2007-1443 of 9 October 2007, available (in French) at: http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000252177.

[56] The *Conseil constitutionnel* has confirmed this prohibition in its decision No. 2001-456 DC on 27 December 2001.

[57] J.P. Brodeur and N. Dupeyron (2003), "Democracy and Secrecy: The French Intelligence Community", in J.P. Brodeur, P. Gill and D. Töllborg (eds), *Democracy, Law and Security*, Aldershot: Ashgate, pp. 22-23.

[58] Fair trial rules are underlined in the Act on Criminal Procedure and in Article 24 of the Spanish Constitution (with the evolving constitutional jurisprudence interpreting it).

their relevance and their need for protection. The power to qualify a document as classified – or to declassify the document – is left exclusively to the executive (Council of Ministers and Assembly of State Chiefs).[59] The activities carried out by the Spanish National Centre of Intelligence (CNI) are considered, as a whole, to be "classified materials" on the grounds of national security.[60] Oversight of the CNI's activities is left to the Parliament and the judiciary.[61] However, the institutions that have access to classified documents are limited in their powers of oversight:

> [I]nstitutions that may have access to the classified documents are the Parliament and the Ombudsman...the Ombudsman is the only institution with limited access to secret information, although the Council of Ministers may forbid such access.[62]

As highlighted above, there is no possibility to use secret evidence in trials in **Italy**. When evidence is protected under the so-called "state secrets privilege", it will either be declared inadmissible by the judge or the public prosecutor and not taken into account during the trial, or accepted (after a review of the state secrets privilege) as ordinary evidence and disclosed to all parties. The rules on state secrecy have raised a number of problematic issues with respect to criminal prosecutions, embodied in the now famous Abu Omar case (see Section 2 below).[63] Articles 24 and 111 of the Italian Constitution protect the rights of the defence and the right to a fair trial respectively. This has been interpreted strictly by the courts in the sense of prohibiting the use of secret evidence in trials. Evidence that is deemed to be covered by the state secrets privilege will be declared either inadmissible or admissible, but no longer covered by the privilege.[64]

The decision on whether evidence is protected by the state secrets privilege ultimately rests with the Prime Minister's office: the hearing of the evidence is suspended by the judge while the Prime Minister confirms – or denies – the existence of the state secrets privilege.[65] The Prime Minister's decision can be challenged before the Constitutional Court by a judge or a public prosecutor. Another oversight mechanism exists in the form of a Joint Parliamentary Committee (COPASIR),[66] which must be informed every time the Prime Minister's office confirms the classification of state secrets. However, in the most recent judgments, the Constitutional Court oversight mechanism has proven quite ineffective in restricting the wide discretion granted to the Prime Minister's office. In the Abu Omar case, the Constitutional Court ruled in favour of the Prime Minister's office on the grounds that the state secrets privilege protected the integrity of the Italian Republic and its foreign relations.[67] This decision by the Constitutional Court has been criticised by some scholars who have argued that it failed to exercise its oversight role in deference to the executive (as detailed hereafter in section 2.1).[68]

2.6 Justifications for the use of state secrets – what is national security?

Governments often invoke an argument based on the common interest to keep certain documents or witnesses confidential or to exclude them during a trial. This argument is often based on concepts such as **'national security'**, **'*secret défense*'** and **'state interest'**, which encompass many different meanings across

---

[59] Articles 3 and 4 of Law 9/1968, 5 April, on Official Secrecy.

[60] See Article 5(1) of Law 11/2002, 6 May, creating the CNI.

[61] Ibid., articles 11 and 12.

[62] See A. Giménez-Salinas (2003), "The Spanish Intelligence Services", in Brodeur, Gill and Töllborg (eds), op. cit., p. 76.

[63] Decision 106/2009 of the Italian Constitutional Court of 11 March 2009. More details on the case can be found in Italy Country Fiche in Annex 5.

[64] Article 256 of the Italian Code of Criminal Procedure.

[65] Article 202 of the Italian Code of Criminal Procedure and Article 41 of Law 124/2007.

[66] *Comitato Parlamentare per la Sicurezza della Repubblica*, composed of five members of the House of Deputies and five members of the Senate.

[67] See Constitutional Court Decision n. 106/2009 of 11 March 2009.

[68] See, for example, C. Danisi (2011), "State Secrets, Impunity and Human Rights Violations: Restriction of Evidence in the Abu Omar Case", *Essex Human Rights Review* 8, 1, October; F. Messineo (2009), "'Extraordinary Renditions' and State Obligations to Criminalize and Prosecute Torture in the Light of the Abu Omar Case in Italy", *Journal of International Criminal Justice* 7, 5, 1023-1044; A. Vedaschi, "Arcana Imperii and Salus Rei Publicae: state secrets privilege and the Italian legal framework", in Cole, Fabbrini and Vedaschi (eds), op. cit., Chapter 7.

the EU Member States examined in our case-studies. The terms encountered during our research include "national security", "public interest", "legitimate state security", "very pressing interests of national security", "threat to security", or "national defence secret". The argument can be traced back to the concept of *raison d'Etat* or "reason of State".[69]

The essential notion is that States may interfere with certain individual rights in exceptional circumstances, when their independence, sovereignty, territorial integrity, constitutional order and/or public safety are threatened. While the origins of the term "national security" in the United States in the 1950s were framed by the threat of war by a foreign enemy,[70] the concept has broadened to include criminal activities, terrorism and migration. Bigo (1994) has shown in the "security continuum" model that there have been shifts away from the one-dimensional Cold War security concept and towards fears of population movements and, more specifically, transnational organised crime, which is cited in political rhetoric as a way to justify new surveillance powers.[71] What are the different understandings and conceptualisations of national security in the seven EUMS examined in this study? The following paragraphs examine how they are understood or framed; a summary of this analysis is provided in the form of a table in Annex 3.

While the concept of national security is not defined in any piece of legislation in the **United Kingdom**, its meaning has been considered by the courts. The House of Lords, SSHD v. Rehman, defined 'national security' as the "security of the United Kingdom and its people", which encompasses the protection of democracy and the legal and constitutional systems of the state, military defence and actions against a foreign state.[72] Other terms may also be employed: the "international relations of the UK", the "detection and prevention of crime", or any other "national" or "public interest".[73]

In **France,** "*secret défense*" ('top-secret defence matter') and "*sécurité nationale*" ('national security') are two different concepts linked together in a defence-security continuum asserting a unity of threat, whether foreign or domestic.[74] The national security concept in France is influenced by the English-speaking world and has only recently been introduced. Several pieces of legislation refer to it, including a decree which states that "the protection of secrecy concerns all fields of activity related to defence and national security: political, military, diplomatic, scientific, economic, industrial".[75] However, the notion of *sécurité nationale* is used more in a doctrinal manner in France. Its definition remains by and large uncertain as it is used either as motivation for adopting measures to ensure security, or, more simply, as a synonym for national defence when qualifying intelligence activities.

In **Germany**, there is no concept of 'national security' per se, but the notion of the protection of state interests of the Federation or the federal states comes closest to it. This stems from the consciousness of German lawmakers after the Second World War of the Nazi regime's misuse of the 'national security' concept.[76] The protection of state interests is defined in Section 99 of the Administrative Court Procedure Act, which provides that access to certain files may be refused if the knowledge of their content "would prove disadvantageous to the interests of the Federation or of a Land".[77] German courts and their case law

---

[69] See N. Machiavelli (1512), *The Prince*, as well as G. Botero (1589), *The Reason of State*.

[70] See, for example, Walter Lippmann's definition in 1943: "a nation has security when it does not have to sacrifice its legitimate interests to avoid war, and is able, if challenged, to maintain them by war", in W. Lippmann (1943), *U.S. Foreign Policy: Shield of the Republic*, Boston: Little, p. 5.

[71] D. Bigo (1994), "The European internal security field: stakes and rivalries in a newly developing area of police intervention", in M. Anderson and M. den Boer (eds), *Policing Across National Boundaries*, London: Pinter, pp. 161-173.

[72] See *SSHD v. Rehman* [2003] 1 AC 153, paragraphs 16, 17 and 50.

[73] See UK Country Fiche in Annex 5.

[74] See France Country Fiche in Annex 5.

[75] See the "*Arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale*", Titre Ier, as well as "*loi n° 91-646 du 10 juillet 1991*".

[76] The orchestrated burning of the Reichstag in February 1933 allowed Hitler to abolish key basic rights and all constitutional guarantees in Germany on the grounds of protecting the people and the State. See R. A. Miller (2010), "Balancing Security and Liberty in Germany", *Journal of National Security Law & Policy*, Vol. 4, p. 369, in particular Section 1.

[77] See Section 99(1) of the Code of Administrative Court Procedure (English translation may be found at www.gesetze-im-internet.de/englisch_vwgo/englisch_vwgo.html).

have interpreted this reason for refusal narrowly by limiting its application to knowledge that could be disadvantageous to important interests only. These may include the external and internal security of Germany, or the existence and functioning of the Federation or a federal state as such. Furthermore, the courts have insisted that it has to be sufficiently likely that the disadvantages will materialise.[78]

There is no common concept or definition of national security in the legislation in **Spain.** Only indirect references are contained in certain pieces of legislation, and these are more related to home affairs than to justice. The threat or damage to "the security and defence of the state" is mentioned in a 1968 law.[79] More recent legislation specifies that the threat could be to "the independence or territorial integrity of Spain, national interests and the stability of the rule of law and its institutions".[80] These concepts are used when the government determines that a document must be classified.

The legal system in **Italy** also lacks a proper definition of national security. Nevertheless, with regard to the state secrets privilege, mention is made of the protection of the "security of the Republic" when dealing with non-disclosure of documents.[81] This includes "the integrity of the Republic (including in relation to international agreements, the defence of its underlying institutions as established by the Constitution, the State's independence vis à vis other states and its relations with them, as well as its military preparation and defence)".[82] The concept of "security of the Republic" is not explicitly limited to the purposes of the intelligence services but can be generally applied within the whole legal system. The Italian Constitutional Court has interpreted the state secrets privilege as a legitimate tool for protecting the supreme interests of the State as a democratic community of individuals.[83] However, as outlined above, the recent judgments of the Constitutional Court regarding the Abu Omar case have taken a controversial approach to granting broader discretionary power to the executive branch.[84]

The concept of national security plays a major role in justifying the use of secret information in criminal procedures under the Act on Shielded Witnesses in **the Netherlands**. The concept of national security is not specifically defined in Dutch legislation, but the case law has recognised the discretion of the main intelligence agency (AIVD) in deciding what constitutes a threat to national security.[85] Annual reports of the AIVD include, for example, terrorist violence, the proliferation of weapons of mass destruction or espionage activities as issues that are considered to pose a threat to national security.[86] The Dutch National Security Strategy in 2007 foresees that "national security is at stake when one or more of the country's and/or society's vital interests are threatened to such an extent that potential societal disruption could occur".[87] Such interests may include territorial, economic, ecological or physical security, and social and political stability.[88]

In **Sweden**, the 2009 Public Access to Information and Secrecy Act defines national security as "any sort of information which can harm the country".[89] The 1949 Freedom of the Press Act lists the interests that may be protected by keeping official documents secret:

1. national security or Sweden's relations with a foreign state or an international organisation;
2. the central financial policy, the monetary policy, or the national foreign exchange policy;
3. the inspection, control or other supervisory activities of a public authority;

---

[78] See R. Rudisile, in F. Schoch, J. Schneider and W. Bier (eds), *Verwaltungsgerichtsordnung*, Sect. 99 par. 16; Posser, in: Posser/Wolff (eds), *BeckOK VwGO*, Sect. 99 par. 20.1.

[79] Art. 2 of Law 9/1968 on Official Secrecy.

[80] Art. 1 Law 11/2002, 6 May 2002, on regulation of the National Centre of Intelligence (CNI).

[81] See Article 39.1 of Law 124/2007, available in English at www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html.

[82] Ibid.

[83] See Italian Constitutional Court, judgments 82/1976 and 86/1977.

[84] Ibid., judgments 106/2009, 40/2012 and 24/2014.

[85] See Raad van State, 04-07-2006, 200602107/1.

[86] See the AIVD Jaarverslag 2013: www.aivd.nl/publicaties?ActLbl=jaarverslag-2013&ActItmIdt=3097.

[87] See the Netherlands Country Fiche in Annex 5. The 2007 National Security Strategy (*Strategie Nationale Veiligheid*) is available at www.nctv.nl/onderwerpen/nv/strategie-nationale-veiligheid/.

[88] Ibid.

[89] See Sweden's Public Access to Information and Secrecy Act (Offentlighets- och sekretesslagen [2009:400]).

4. the interest of preventing or prosecuting crime;
5. the public economic interest;
6. the protection of the personal or economic circumstances of private subjects; or
7. the preservation of animal or plant species.[90]

A more precise hint can be found in the role of the Swedish Security Service, whose mission is to "protect the democratic system, the rights and freedoms of our citizens and national security".[91] No information has been found on the way national courts have interpreted this concept.

In light of the above, **the concept of 'national security' seems to be either absent from, or very loosely defined by, EUMS' national legal systems**. The table in Annex 3 shows that **the conceptual features attributed to this term remain 'open-ended' even in those Member States with legal frameworks**. There are several concepts which are often used or prescribed in EU Member States, yet there is no commonly held legal definition in any of the countries under examination that meets the legal certainty and "in accordance with the law" test (see Section 3 below). The changing notion of national security is fought over in the supranational judicial context and on the basis of 'rule of law' and 'division of powers' principles. This conceptual fuzziness leads **to accountability deficits of the executive and intelligence communities** described in the following section.

The notion of national security becomes more complex in the context of systems of 'mutual respect' of protected secrets with third countries such as the US. The Snowden revelations have posed an interesting question in relation to the concept of 'national security': **'Whose' security? Is the national security of third countries part of the national security of EUMS?** The possible violations of the rule of law and fundamental rights linked to large-scale surveillance affect the security of the Union, its Member States, and EU citizens and residents. They also bypass the use of established channels of mutual legal assistance between the EU and third countries such as the US. A key issue is therefore the way in which these **mutual respect regimes actually undermine notions of national security and the common internal security of the Union as a whole**.

[90] See Regeringskansliet (2009) Public Access to Information and Secrecy Act: Information concerning public access to information and secrecy legislation etc., available in English at www.government.se/content/1/c6/13/13/97/aa5c1d4c.pdf.

[91] See www.sakerhetspolisen.se/en/swedish-security-service/about-us.html.

3. Assessing the reliance of the EU Member States' justice systems on intelligence information in courts: The issue of scrutiny

KEY FINDINGS

- In EUMS that allow classified information to be used in legal proceedings (UK, the Netherlands, Germany, Spain and Sweden), there are significant practical challenges in exercising proper scrutiny over the information.
- The current reliance on intelligence materials found in the majority of the EUMS under examination is highly problematic given the insufficient judicial oversight and in the context of the recent digital surveillance revelations.
- In cases where officials are suspected of wrongdoing and unlawful practices, our cross-examination of EUMS legal practices reveals a number of challenges to official accountability, either in the use of closed material procedures (in the UK) or in the practical barriers to accessing classified materials (Italy, France).
- Claims of secrecy clearly obstruct judicial scrutiny across the EUMS under examination. The use of secrecy makes it very difficult to assess the quality of the intelligence materials provided, and makes it impossible both for the public to know whether serious allegations of misconduct are true and for those affected to hold to account those responsible.

This section will assess the reliance of the EUMS' justice systems on intelligence information in courts. To what extent can intelligence information be used in courts, and in particular, as evidence? Intelligence information becomes 'secret evidence' when it is used and accepted as such in judicial proceedings without being disclosed to interested parties. It may be heard in camera or in the form of documentary information, which is partly or fully classified. This, of course, raises the question of the nature of the materials presented: Have they been carefully assessed and have they been gathered with due respect for the law? Section 2.1 examines how, in practice, judicial scrutiny operates when intelligence materials are presented to courts. Arguing that the mechanisms in place in the EUMS under investigation are not adequate to guarantee the quality of the materials provided by intelligence services in courts, Section 2.2 analyses this aspect in the specific context of digital surveillance. Section 2.3 examines cases where judicial authorities request information classified as 'secret' from executive/intelligence authorities to determine whether the government and/or its officials acted unlawfully.

3.1 Assessing the quality of information used to convict an individual before the courts

As described in Section 1, intelligence information is used directly via CMPs and indirectly via second-hand evidence. This subsection aims to demonstrate that **the judicial authorities too often presume the quality of the information provided by the intelligence services**. In other words, the courts rely on and 'validate' intelligence information based on a presumption of good faith.

The Venice Commission stated in its 2007 Report on the Democratic Oversight of the Security Services:

> Where the parliament is not in a position to hold the executive accountable, it becomes even more important that the national courts are able to perform this function effectively. But, for a variety of reasons the ordinary courts are often in a poor position to perform adequately this task

> in the area of national security. Unlike other government authorizations to limit human rights, powers granted to governments in this area are often wholly discretionary.[92]

All the EUMS under examination have **mechanisms of judicial oversight** of the materials presented to courts, but most of them are **limited**.

In the UK, the existing system of special advocates (as described in Section 1) is limited to ensuring proper scrutiny of the closed materials presented to courts. The deficiencies of the special advocates system have been identified by Justice UK[93] and underlined by many special advocates themselves. Among these deficiencies is the **lack of formal rules for evidence**, allowing second- or third-hand hearsay or even more remote evidence to be admitted, frequently with the primary source unattributed and unidentifiable. In the Netherlands, the Shielded Witnesses Act described in Section 1 provides for the possibility of hearing AIVD officers as shielded witnesses. **In practice, there is very little oversight of intelligence services providing evidence to be used in court**. After having received an official report from the AIVD with the relevant information, the Public Prosecutor on Counterterrorism is charged with analysing all relevant information before a criminal investigation is initiated. Yet it appears from case law that the extent to which the public prosecutor has to check the information collected by the AIVD is very limited. Since the AIVD is already monitored in other ways, the public prosecutor is supposed to presume the legitimacy of the information provided by the intelligence services. **There are thus real difficulties for the judge to assess the reliability of the official written reports provided by AIVD**. The Act on Shielded Witnesses forbids defence counsels to know who collected the evidence or question witnesses. In Germany, the admission of second-hand witnesses, as described in Section 1, has important consequences for the intelligence materials produced for the courts. Even if the German Federal Constitutional Court held that the courts have to accept the lower probative force of second-hand evidence, **neither the courts nor the parties have the possibility of assessing the reliability of the first-hand evidence (for example, through a cross-examination of a witness)**.

Judicial oversight of the materials presented to courts can be also **weakened by the discretionary powers granted to the executive**.

The Abu Omar case in Italy is an interesting case study. In a 2003 joint operation, the CIA and the Italian Military Intelligence and Security Service (SISMI) abducted and transferred to Egypt the Imam of Milan, Hassan Mustafa Osama Nasr, also known as Abu Omar.[94] There, according to his account, he was tortured and harshly questioned with respect to his alleged connections to al-Qaeda and jihadist groups. Criminal investigations, led by the Office of the Public Prosecutor of Milan, resulted in a first judgment by the Criminal Court of Milan that convicted CIA agents (directly or indirectly involved in the case) of kidnapping and two SISMI agents for abetment. The then head of SISMI and another high-ranking officer of the Italian secret service were acquitted due to the existence of state secrets in the documents and other information. In fact, during the criminal procedure and court hearings, Italian officers had claimed the state secrets privilege. As pointed out by the study's national expert for Italy, **while the state secrets privilege in Italy can in practice be subject to judicial review (via the Constitutional Court) and to political oversight (via the Joint Parliamentary Committee for the Intelligence and Security Services), both kinds of oversight provided by the law have proven quite ineffective in restricting the wide discretion granted to the executive**. Only the Prime Minister is entitled to decide what constitutes national security and shall be classified as a state secret, and the Abu Omar case shows a substantial lack of power to overrule the Prime Minister's decision. **Similarly, in France, the classification of *'secret défense'* ('top-secret defence matter') remains solely within the power of the executive, with very restricted oversight.**[95] *Secret défense* can only be opposed by the judiciary and the Parliament. This constitutes a significant challenge in

---

[92] See Report on the Democratic oversight of the security services, adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007), Paragraph 85. Available at www.statewatch.org/news/2007/jun/venice-com-control-of-security-services.pdf.

[93] See JUSTICE UK, Justice and Security Act 2013: Civil Procedure (Amendment No 5) Rules 2013, 5 July 2013. Available at www.justice.org.uk/data/files/resources/354/JUSTICE-Civil-Procedure-_Am-No5_-Rules-Briefing-July-2013.pdf.

[94] The case is presented in details in the Italy Country Fiche in Annex 5.

[95] See France Country Fiche in Annex 5.

cases where classified information obstructs judicial scrutiny of government officials suspected of wrongdoing, as described below in subsection 2.3.

It should be noted that **effective judicial scrutiny of the quality of information provided by intelligence communities is further undermined when presented in CMPs or relayed in judicial proceedings as second-hand evidence or as an intelligence report**. In these cases, the quality and reliability of the information are even more difficult to assess.

In light of these limits and challenges to judicial scrutiny, reliance on intelligence materials appears highly problematic. Intelligence oversight is key to ensuring the legitimacy and lawfulness of materials presented to courts and used in judicial procedures. It is also key to restoring public confidence, which has been heavily undermined in the wake of Snowden's revelations.

3.2 Digital surveillance and scrutiny in a post-Snowden era

The practices of intelligence services have been challenged and contested in the past on legitimate grounds. The Snowden revelations have unveiled further alleged unlawful practices in the form of large-scale surveillance programmes carried out by law enforcement agencies across the EUMS. In a recent study prepared and presented for the LIBE Committee Inquiry,[96] we showed that the distinction between targeted surveillance for criminal investigation purposes, which can be legitimate if framed according to the rule of law, and large-scale surveillance with unclear objectives is increasingly blurred. The Moraes Report underlined that Snowden's revelations showed "compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication and location data and metadata of all citizens around the world on an unprecedented scale and in an indiscriminate and non-suspicion-based manner."[97]

As addressed by the Council of Europe in a recent issue paper,

> There is a lack of clear treaty rules governing the actions of national security and intelligence agencies, and the basis on which they operate and exchange data. In many countries, there are few clear, published laws regulating the work of these agencies. In some, there are no published rules at all. Until the rules are known under which these agencies and services operate – domestically, extraterritorially or in co-operation with each other – their activities cannot be said to be in accordance with the rule of law. Another matter of serious concern is the manifest ineffectiveness of many supervisory systems.
>
> In other words, in relation to national security, there is as yet no real cornerstone to uphold the rule of law – although there are at least basic principles that could form the foundation of such an essential part of the universal human rights edifice.[98]

Intelligence service digital surveillance information used in courts represents a significant challenge to judicial scrutiny. This issue is even more important given the use of CMPs in the UK where **information obtained through interceptions of communications is now allowed in legal proceedings**. CMP processes have specific statutory exceptions permitting intercept material. Section 18(1) of the Regulation of Investigatory Powers Act 2000 (RIPA) lists the proceedings to which the exclusion of intercept material does not apply. In the 2013 Justice and Security Act's Explanatory Notes, courts are explicitly asked to ignore the exclusion of intercept material set out in RIPA, meaning that intercept evidence can be used to support an application for a declaration.[99]

---

[96] See D. Bigo et al., op. cit.

[97] C. Moraes (2014), "Draft Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs", LIBE Committee.

[98] See Council of Europe (2014), "The rule of law on the Internet and in the wider digital world", Issue paper published by the Council of Europe Commissioner for Human Rights, December, p. 19.

[99] Justice and Security Act 2013 Explanatory Notes, Paragraph 72. Available at www.legislation.gov.uk/ukpga/2013/18/notes/division/5/2?view=plain.

The use of intelligence materials obtained through digital surveillance is highly problematic, as it has been widely reported that intelligence agencies in some EUMS (especially GCHQ in the UK) seemed to have considered themselves 'above the law' in their data collection activities.

In his 2013 Annual Report, UK Interception of Communications Commissioner Sir Anthony May addressed the public concerns raised in the wake of Snowden's revelations. The report concluded that the Secretaries of State and the agencies that undertake interception operations "do so lawfully, conscientiously, effectively and in the national interest".[100] Furthermore, Sir Anthony May concluded that the Intelligence Services were not receiving from US agencies intercept material that could not lawfully be acquired by intercept within the UK and thereby circumventing domestic regimes. However, it has been noted that May's Report did not test intercept cases against the legal regime meeting the criteria set out by the jurisprudence of the ECtHR. The only statute that May referred to as directly applicable is the 1994 Intelligence Services Act. As reiterated in a 'skeleton argument' presented on behalf of Privacy International and Bytes for All submitted in July 2014 to the Investigatory Power Tribunals (IPT),[101] the Strasbourg Court has ruled four times on bulk surveillance and related data collection and retention issues. These cases each confirm that any kind of bulk data collection and analysis, especially if automated, pose grave risks and must be very narrowly confined.[102] According to the legal arguments presented to the IPT, the ways in which intercept materials are gathered and acquired from foreign intelligence services fail to pass the "in accordance with the law" test pursuant to ECHR Art 8.

In its opinion on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows", released in February 2014, the European Data Protection Supervisor (EDPS) reiterated that rights to privacy and data protection are enshrined in primary law in Article 8 of the Council of Europe Convention on Human Rights and Fundamental Freedoms, Articles 7 and 8 of the EU Charter of Fundamental Rights and Article 16 TFEU. Even if the EDPS acknowledged that these provisions of EU law do not apply to the national security of EUMS (according to Article 4(2) of the Treaty of the European Union), the EDPS stated, "[T]his does not mean that national **security remains an unregulated area**, in particular as regards the protection of fundamental rights: the Council of Europe instruments mentioned above and national laws are in most situations fully applicable to this field" (emphasis added).[103]

This study does not aim to examine the allegations against intelligence services in the field of digital surveillance. However, **the use in courts of intelligence information obtained through extensive surveillance raises more than mere concern**, since such evidence relies on covert investigation activities, carried out by intelligence agencies, without any of the guarantees provided by ordinary evidentiary rules within criminal investigations. As previously underlined, an essential precondition to admitting the use of secret evidence in national security cases is the good faith of governmental agencies involved in data collection and analysis, in terms of compliance with laws and fundamental rights. Snowden's revelations have shown that such compliance was not sufficiently safeguarded. The use of intelligence materials in courts appears to be particularly worrying, since **no real scrutiny and no effective review of the procedures used to collect such evidence is provided before it is 'packaged' for the judge's perusal**. How can we consider a trial based on secret evidence 'fair' if we cannot be sure that evidence was fairly collected (i.e. in a manner that respects the law and fundamental rights)?

The extent to which the debates raised in the context of Snowden's revelations have affected the use of secret evidence in courts is difficult to assess. In the UK, where GCHQ practices were heavily criticised, the

---

[100] See 2013 Annual Report of the Interception of Communications Commissioner Rt Hon. Sir Anthony May, p. 24. Full report available at http://iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf.

[101] Skeleton argument served on behalf of Privacy International and Bytes for all for preliminary issues hearing, 14 July 2014.

[102] Cases referred to are: *Weber & Saravia v. Germany* (2008); *Liberty v. UK* (2009); *S v. UK* (2009) and *MK v. France* (2013).

[103] See EDPS (2014) Opinion on the Communication from the Commission to the European Parliament and the Council on 'Rebuilding Trust in EU-US Data Flows', February 2014. Available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-02-20_EU_US_rebuliding_trust_EN.pdf.

government's practice in "open" hearings is to "neither confirm nor deny" ("NCND") that it engages in any form of digital surveillance and it has not confirmed or denied the truth of any of the Snowden revelations insofar as they concern the UK engaging in interception of communications. That NCND policy has been accepted by the courts. While in "closed" hearings special advocates may have argued that recent revelations of digital surveillance practices demand that certain evidence not be admitted, their attempts to do so would not be made public. In any case, as the legality of the government's digital surveillance programme is still being considered, such arguments would not succeed. Nevertheless, these legal arguments should not obscure the fact that the Snowden revelations have eroded trust in intelligence service practices and the presumption that materials they present to courts have been lawfully obtained.

In assessing the reliance of EU Member States' justice systems on intelligence information presented in courts, a related issue concerns the use of secrecy and how this affects government officials' accountability.

3.3 Secrecy and government officials' accountability

Assessing to what extent the use of secrecy can disrupt government officials' accountability is of paramount importance. In this subsection, three case studies will be highlighted: UK Al Rawi and Others v. The Security Service and Binyam Mohammed v. FCO, which shed an interesting light on the current Belhaj rendition case; the Abu Omar case in Italy; and the French 'Karachi case'. These cases show how the use of CMPs in the UK, the state secrets privilege in Italy and the 'secret défense' (top-secret defence matter) in France can result in unanswered questions about officials' accountability.

In the UK, Al Rawi and Others v. The Security Service and Binyam Mohammed v. FCO were two cases brought by former Guantanamo Bay detainees who sued the UK government, alleging the UK's complicity in their detention, rendition and mistreatment by foreign authorities. In the case of Binyam Mohammed, the UK was forced to disclose documents, which showed the UK's knowledge of Mr Mohammed's mistreatment.

Binyam Mohammed, a British resident, had brought an action against the UK government for being complicit in his torture in 2011 in a now well-documented extraordinary rendition case. During the proceedings, evidence came to light that British intelligence officials, in collaboration with US security officials, were directly implicated. Binyam Mohammed and a number of other ex-Guantanamo Bay detainees brought a civil claim against the UK government for its involvement in their ill treatment and unlawful detention by the US authorities. The UK government applied to the High Court for it to adopt a CMP, which would see Mr Mohammed and the other claimants and their lawyers excluded from the hearing of the case and the issuing of a 'closed judgment' that they would not be entitled to see. In May 2010 the Court of Appeal ruled that an ordinary civil claim must be held in open court, as a litigant's right to know the case against him or her and to know the reasons why he or she has won or lost is fundamental to the right to a fair trial. In July 2010 the High Court ordered the release of some of the documents relating to the case. In November 2010 it was announced that Binyam Mohammed and some of the other former Guantanamo Bay detainees were to be awarded compensation by the British government for the treatment they received.[104]

The Binyam Mohammed case sheds an interesting light on the current Belhaj rendition case. Abdul Hakim Belhaj is a Libyan politician and a former Qaddafi opponent who claims the UK government was involved in his and his pregnant wife's illegal rendition, torture and mistreatment.[105] In particular, he claims British intelligence tipped off the Libyan authorities and helped the US arrange his rendition to Libya.[106] Belhaj is currently suing the Home Office, the Foreign Office, MI5, MI6, former Foreign Secretary Jack Straw, former MI6 agent Mark Allen and the Attorney General for their alleged role in his 2004 rendition. In December

---

[104] Liberty, Binyam Mohamed, available at www.liberty-human-rights.org.uk/human-rights/no-torture/uk-complicity-torture/binyam-mohamed.

[105] BBC report (2012), "Jack Straw faces legal action over 'rendition'", 18 April, www.bbc.co.uk/news/uk-17746561). Belhaj, who led an insurgency against Colonel Muammar Gaddafi before fleeing Libya in 1996, says that he and Moroccan Fatima Boudchar were abducted and detained by US secret agents with the help of British authorities. The couple was ultimately returned to Libya to be tortured and jailed by the dictator's government, Belhaj says, until the uprising in 2011 saw Belhaj emerge as a new political leader.

[106] BBC report (2013), "Government lawyers consider Belhaj rendition damages", 21 May, www.bbc.co.uk/news/uk-22614662.

2013 a High Court judge ruled that this claim was beyond the jurisdiction of the UK courts. The UK government argued that Belhaj's case cannot be heard at all on the grounds that the "act of State" doctrine means that UK Courts are precluded from judging the actions of foreign states in their own country.[107] In February 2014, the claimants were given permission to appeal the ruling on the act of State doctrine and the UK government cross-appealed contesting that, in addition to the act of State doctrine, state immunity also precluded the claims from being heard. Amnesty International, JUSTICE (the British affiliate of the International Commission of Jurists), and REDRESS have since joined the Belhaj case. The UN Special Rapporteurs on torture and arbitrary detention have also been granted permission to intervene on Belhaj's behalf. The above organisations stated in a written submission to the court that:

> The outcome of the [December appeal] has significant potential to determine the availability of an effective remedy to victims of gross violations of human rights both in the United Kingdom and other common law jurisdictions where officials act in concert with officials from other states.[108]

The NGOs publicly regretted that the High Court judgment in this case may immunise the UK government and its officials from judicial scrutiny in cases where they are alleged to have acted unlawfully, including in circumstances where they may have committed gross violations of human rights law.[109] They reiterated that the act of State doctrine must not be used to shield UK officials from accountability over their alleged complicity in the affair and that the act of State doctrine and the law of state immunity were two distinct sets of principles.[110] On 30 October 2014, Belhaj won the right to sue the UK government over his kidnapping. The Court of Appeal ruled that the case should go ahead despite government attempts to resist it on grounds of the act of State doctrine. The British government maintained that the UK's relations with the US would be seriously damaged if Belhaj was allowed to sue and make his case in a British court. The Foreign Office is currently considering whether to appeal. Under the Justice and Security Act, this rendition case will likely be heard in secret.

The Binyam Mohammed case detailed above is of particular relevance for our study and for the Belhaj case, as it can be argued that Binyam Mohammed would have been denied redress if the Justice and Security Act had been in force in 2010.[111] The disclosures made in that case about the activities of the Intelligence Services and the treatment and rendition of Mr Mohammed would not have been made if CMPs under the Justice and Security Act had applied. As underlined by an Amnesty International Report on CMPs, referring to the Belhaj case, "If these cases are heard using a closed material procedure, there is genuine concern that evidence concerning human rights violations could be withheld from the individuals, their lawyers and the wider public, potentially shrouding these cases in a cloak of secrecy that might never be fully lifted".[112]

In Italy, in the Abu Omar case described in Section 2.1, the High Court's decision to acquit two high-ranking officers of the Italian secret service due to the existence of state secrets ruled out any chance that Italian intelligence officials will ever be brought to justice. It appears that Italian courts no longer have any role in deciding what information is kept secret and why. Furthermore, in April 2013, Italian President Giorgio Napolitano pardoned Joseph Romano, the US military officer sentenced in absentia to seven years in prison for his involvement in the Abu Omar kidnapping. Robert Seldon Lady, Milan CIA Bureau Chief at the time of the kidnapping operation, is now actively seeking a pardon as well, after being sentenced in absentia to nine years for his role in the crime. As underlined by Julia Hall, Amnesty International's Expert on Counter-

---

[107] Amnesty International (2014), "UK government accused of 'scraping legal barrel' in Belhaj rendition case", Press release, July, www.amnesty.org/fr/node/48460.

[108] Redress (2014), "Submissions of the International Commission of Jurists, JUSTICE, Amnesty International and Redress", 30 June, available at www.redress.org/downloads/casework/belhadj---interveners-(ngo)---final---300614.pdf.

[109] JUSTICE (2014), "NGOs urge Court of Appeal to preserve access to justice in torture claims", 2 July, www.justice.org.uk/news.php/122/ngos-urge-court-of-appeal-to-preserve-access-to-justice-in-torture-claims; Amnesty International (2014), op. cit.

[110] Submissions of the International Commission of Jurists, JUSTICE, Amnesty International and Redress, www.justice.org.uk/data/files/BELHADJ_-_INTERVENERS_NGO_-_FINAL_-_300614.pdf.

[111] T. Hickman (2013), "Turning out the lights? The Justice and Security Act 2013", UK Const. L. Blog, 11 June, http://ukconstitutionallaw.org.

[112] Amnesty International (2012), *Left in the Dark: The Use of Secret Evidence in the UK*, London: AI Publications.

Terrorism and Human Rights, "the recent court decisions...could pave the way to impunity for virtually anyone involved in the Abu Omar affair".[113]

In France, the use of secrecy in the name of '*secret défense*' (top-secret defence matter) has obstructed several judicial inquiries into officials' accountability. The 'Karachi Affair' relates to alleged commissions and kickbacks paid by France when it sold submarines to Pakistan in the mid-1990s. Successive investigative judges in France have tried to explore the link between this arms deal and the 8 May 2002 terrorist attacks that resulted in the deaths of 11 French engineers working to assemble Agosta 90B class submarines for the Pakistani navy. Twelve years later, the investigation remains inconclusive. During their investigations, the judges considered a lead involving certain Pakistani groups acting in revenge after France decided to stop paying commissions related to these arms contracts. There are furthermore strong suspicions that these arms deals financed the campaign of former Prime Minister Edouard Balladur in the French presidential election in 1995 and that commissions obtained to ensure the deal enriched many military officers and political leaders in Pakistan.

As described in Section 1, in France '*secret défense*' cannot be communicated to or used by anyone – not even judges – other than those who have top-secret clearance. Since the investigations began in the Karachi Affair, antiterrorism judges have used the only procedure the law provides for: they have asked the Minister of Defence to declassify critical information for their investigations, and the *Commission consultative sur le secret de la défense nationale* (CCSDN) has been asked to advise on the declassification of crucial information for judicial inquiries. The CCSDN has provided some 15 advisory opinions since 2002, two-thirds of which are in favour of declassification and one-third completely or partially against it. Yet the required information has not been handed to the judges, since the Prime Minister is not bound by the Commission's opinion. In 2009, the French National Assembly set up a committee to investigate the circumstances of the 2002 attack in Karachi. In a report released in 2010, the members of this committee publicly regretted that the government did not provide them with first-hand documents that may have helped them in their task and allowed them to fully exercise their mission of parliamentary control. As a result, neither the Parliament nor the judges could access relevant information, and the case remains unsolved.

The cases outlined in this subsection demonstrate significant challenges to judicial scrutiny when officials' accountability is involved. Claims of secrecy clearly obstruct judicial scrutiny. The use of secrecy makes it very difficult if not impossible for the public to know whether serious allegations of misconduct are true and for those affected to hold to account those responsible. In the Karachi Affair, the families of the victims of the attacks are still awaiting information to understand how their relatives lost their lives.

Our cross-examination of EUMS' legal practices reveals a number of challenges to the intelligence services' accountability and oversight of their activities, as well as to the judicial scrutiny of the materials presented to courts. In what ways have European courts dealt with the tensions between national security, intelligence and the rights of the defence? Are there any common standards emerging from the jurisprudence of European courts to handle these tensions?

[113] J. Hall (2014), "Italy's Dirty Little (State) Secrets", 3 March.

4. When judicial scrutiny goes transnational: European judiciary standards

KEY FINDINGS

- There are a number of key European legal standards stemming from European judicial actors on the issues of intelligence information, national security and state secrets when these affect the rights of the defence. While EUMS authorities enjoy a considerable discretion when invoking 'national security', they are still subject to judicial scrutiny by domestic and European courts.
- The European courts have raised serious questions about the compatibility of some procedural rules on closed material with the ECHR and the EU Charter, stating specifically that evidence must always be available to the judge and the grounds justifying closed procedures given to the applicant/appellant..
- The most important legal standard when assessing national security and intelligence information is the "in accordance with the law" test, consolidated by both the ECtHR and the CJEU. This test requires national law to meet a number of essential quality standards; the law must thus be adequately accessible, clear and foreseeable.
- The executive is not free from effective control by national courts even in situations dealing with national security and matters of political violence. The principle of effective and independent judicial review constitutes a key European legal standard.
- The ECtHR has repeatedly called for domestic laws to afford sufficient legal protection, with sufficient clarity, to prevent the executive from acting arbitrarily and with unfettered powers. It has also held that 'surveillance in the name of national security' is only lawful as far as it is necessary in a democratic society.
- In A and Others v. UK, the ECtHR raised concerns about the practical challenges faced by special advocates in usefully fulfilling their function and set a number of conditions for UK practices to be ECHR-compliant, in particular that "non-disclosure" cannot deny a party knowledge of the very essence of the allegations against her/him.
- The CJEU has also considered the role of judicial accountability to be central in determining the legitimacy and legality of Member States' actions and the use of closed evidence in cases related to acts of political violence. It has identified clear legal standards for testing the legality of executive interference in defence rights. Effective judicial oversight before an impartial and independent court must go hand-in-hand with disclosing the evidence in order to ensure the rights of the defence enshrined in the EU Charter of Fundamental Rights. Moreover, EU Member States are required to provide effective judicial review and prescribe rules related to that review.

This section examines the role of supranational judicial accountability in delimiting the scope of action and margin of appreciation enjoyed by the executive on questions related to the use of intelligence information, national security and state secrets when these affect such fundamental rights as the rights of the defence. Are there any common European legal requirements or standards emerging from the jurisprudence of European courts against which to test the lawfulness of the use of intelligence information, national security and state secrets by States?

The commonly held position according to which national security remains within the exclusive confines of nation-state discretion sits uneasily with supranational fundamental and human rights instruments and judicial accountability. States' freedom to determine 'what' is national security, the lawfulness of interference with human rights 'in the name of national security' and the classification of intelligence information as 'state secrets' have been affected over the last 30 years as a consequence of European case law and principles. State authorities and intelligence communities no longer have 'the last word' when invoking national security and using intelligence data in their actions and decisions. In what ways have

European courts dealt with intelligence accountability and the tensions between national security, intelligence and the rights of defence?

This Section will examine the standards stemming from the ECHR (3.1) and from the "in accordance with the law" test developed by the Strasbourg Court's case-law, as well as the principles and standards developed by the Court of Justice of the EU (3.2).

4.1 European Convention on Human Rights Standards

The European Court of Human Rights (ECtHR) in Strasbourg has engaged with various issues affecting the relationship between national security, intelligence and human rights since the late 1970s. The Council of Europe and the Strasbourg Court are regional bodies scrutinising the lawfulness of Member States' intelligence activities from a human rights perspective. As a result, "States' margin of appreciation in cases connected with national security is no longer uniformly broad".[114]

States have often invoked national security in order to justify limitations on human rights. Controversially, the nebulous nature of the concept of national security, as described above in Section 1.6 and summarised in Annex 3, has not prevented the Strasbourg Court from giving it 'some substance' from the perspective of the European Convention on Human Rights (ECHR). According to the ECHR, national security includes subjects as broad as "the protection of state security and constitutional democracy from espionage, terrorism, support for terrorism, separatism and incident breach military discipline".[115] Authors like Cameron have been critical of the ECHR approach as not providing further conceptual clarity or definitional features of the term "national security". The conceptual obscurity surrounding the notion of "national security" limits scrutiny of intelligence agencies.[116]

The various rulings by the ECtHR have by and large dealt with the adequacy of the domestic legal regime regulating intelligence surveillance and the activities of the intelligence agencies, such as in cases covering secret surveillance, long-term storage of information in security files, deportations as well as extraordinary renditions and secret detentions. Strasbourg jurisprudence has paid particular attention to intelligence accountability in cases related to Articles 6 (Right to a Fair Trial) and 13 (Right to an Effective Remedy) of the ECHR, as well as the implications for Articles 3 (Prohibition of Torture), 5 (Right to Liberty and Security), 8 (Right to Respect for Private and Family Life) and 10 (Freedom of Expression) of the ECHR. A list of selected ECtHR case law of relevance for the purposes of this study is provided in Annex 1.[117] Specific attention will be paid to **rulings concerning the compatibility of national security, state secrets and intelligence information with Articles 6 and 13 ECHR**.

As a starting point it is important to clarify that, according to ECtHR jurisprudence, States are free to take measures they consider necessary for the protection of national security subject to human rights constraints. The system is not prescriptive of what must be done in the name of national security. ECHR standards rather prescribe **ex post checks of the compatibility between States' actions or decisions interfering with human rights on national security grounds and the ECHR**. The following three standards can be highlighted in this context: First, the "in accordance with the law" test; second, the "necessary in a democratic society" test; third, effective remedies and effective judicial control.

4.1.1 "In accordance with the law" test

The majority of ECtHR case law has assessed the lawfulness of national security-based actions by Member States from the perspective of their compliance with the "in accordance with the law" legal principle. This constitutes **the most important legal standard** when assessing national security, state secrets and

---

[114] European Court of Human Rights (2013), National Security and European case-law, Division de la Recherche/Research Division, Council of Europe, available at: www.echr.coe.int.

[115] Ibid., p. 4.

[116] I. Cameron (2005), "Beyond the Nation State: The Influence of the European Court of Human Rights on Intelligence Accountability", in H. Born, L.K. Johnson and I. Leigh (eds), *Who's Watching the Spies? Establishing Intelligence Accountability*, Dulles, VA: Potomac Books, Inc., pp. 34-53.

[117] National security is expressly referred to as one of the "legitimate aims" understood as necessary in limiting/restricting some of these same human rights. Refer to paragraphs 2 of Articles 8, 10 and 11 ECHR.

intelligence information. An Achilles' heel of much national security legislation and practice is that their opacity and imprecision make it impossible for individuals to adapt or adjust their behaviour accordingly.

The ECtHR has outlined three main conditions composing the "in accordance with the law" test: First, the measure under judicial scrutiny needs to have its basis in domestic law; second, the law needs to be accessible and sufficiently clear to the individual involved – the precision of the law plays a decisive role; and third, the consequences need to be foreseeable.[118] These three qualitative standards all allude to **the quality of the law at hand**, which States must guarantee, including (and especially) in issues related to national security and intelligence activities.

In the landmark ruling Gillan and Quinton v. the UK,[119] the ECtHR examined the lawfulness, from the perspective of the ECHR, of the powers of authorisation and confirmation as well as those of 'stop and search' under sections 44 and 45 of the 2000 Terrorism Act in the UK . Their compatibility with the "in accordance with the law test" played a particularly important role in this assessment. The court held that

> …the words 'in accordance with the law' require the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct[120]

For these requirements to be met the ECtHR called for the domestic law to afford **sufficient legal protection to prevent the executive from acting arbitrarily or with unfettered powers**. The law must indicate with **sufficient clarity the scope of any such discretion** conferred on the authorities and the ways in which it is exercised.[121] The ECtHR concluded that the broad room for manoeuvre granted to police officers by the UK Terrorism Act led to a clear risk of arbitrariness, with no need for the police officer to show any reasonable suspicion of the person involved.[122] The court held that the powers granted by the UK Act were neither sufficiently circumscribed nor subject to adequate legal safeguards against abuse, and therefore failed the "in accordance with the law" test. As we will see in Section 3.2 below, **this test is one of the examples where both the ECtHR and the Court of Justice of the European Union find national security legislation and practices to be failing**.

4.1.2 "Necessary in a democratic society" test

The second standard emerging from the Strasbourg jurisprudence concerns the necessity and proportionality principles. Are the States' measures or interferences with the Convention necessary in a democratic society? The court has examined the extent to which any interference with ECHR rights corresponds to a "pressing social need", whether they were proportionate to the legitimate aim pursued and whether the justifications provided by state authorities are relevant and sufficient.

One of the first landmark judgments where the court used this standard was Klass and Others v. Germany in 1978.[123] While accepting the legitimacy of national legislation on secret surveillance, the ECtHR

---

[118] *Kennedy v. United Kingdom*, no. 26839/05, 18 May 2010; *Rotaru v. Romania*, no. 28341/95, ECHR 2000-V; *Amann v. Switzerland*, no. 27798/95, ECHR 2000-II; *Iordachi and Others v. Moldova*, no. 25198/02, 10 February 2009; *Liberty and Others v. United Kingdom*, no. 58243/00, 1 July 2008.

[119] *Gillan and Quinton v. United Kingdom*, Application No. 4158/05, 12 January 2010.

[120] See §76. Reference was here also made to *S. and Marper v. United Kingdom* [GC], Application nos. 30562/04 and 30566/04, §§ 95 and 96, ECHR 2008.

[121] § 77. See also *Rotaru v. Romania* [GC], no. 28341/95, § 55, ECHR 2000-V; *Hasan and Chaush v. Bulgaria* [GC], no. 30985/96, § 4, ECHR 2000-XI; *Maestri v. Italy* [GC], no. 39748/98, § 30, ECHR 2004 I; see also, amongst other examples, *Silver and Others v. United Kingdom*, 25 March 1983, §§ 88-90, Series A no. 61; *Funke v. France*, §§ 56-57, judgment of 25 February 1993, Series A no. 256-A; *Al-Nashif v. Bulgaria*, no. 50963/99, § 119, 20 June 2002; *Ramazanova and Others v. Azerbaijan*, no. 44363/02, § 62, 1 February 2007; *Glas Nadezhda EOOD and Anatoliy Elenkov v. Bulgaria*, no. 14134/02, § 46, ECHR 2007 XI (extracts); *Vlasov v. Russia*, no. 78146/01, § 125, 12 June 2008; *Meltex Ltd and Movsesyan v. Armenia*, no. 32283/04, § 81, 17 June 2008).

[122] § 85. In particular as regards the disproportionate use against "black applicants or those of Asian origin", which in view of the court risked the discriminatory use of the powers against such persons.

[123] *Klass and Others v. Germany*, 6 September 1978, Series A no. 28.

acknowledged the danger that this kind of law poses to democracy and the rule of law.[124] The court held that **'surveillance in the name of national security' is only lawful as far as it is necessary in a democratic society**. This reasoning was later presented in a series of judgments assessing the lawfulness of interceptions of communications.[125]

The ECtHR has been clear in respect of interferences with the rights of the defence in national security cases: **any restriction has to be absolutely necessary**.[126] While national authorities enjoy a certain margin of appreciation when determining the 'necessity' of their actions, **this decision is subject to judicial oversight by the court**. The Strasbourg Court has laid down important requirements: the provision of adversarial proceedings, equality of arms and adequate safeguards protecting the suspect/accused.[127] An issue of particular relevance is that, in these cases, national authorities refuse to provide or disclose information classified as 'secret' or 'top secret'. This prevents the existence of any effective way to assess or challenge the authenticity or veracity and lawfulness of the information presented as 'evidence'.[128]

The decisive point used by the court when determining a breach of the ECHR in situations where the allegations are based on intelligence information has been **the existence of sufficiently detailed information allowing applicants to effectively challenge or contest them**. Some of the applicants in A and Others v. UK had been charged with being involved in fundraising for terrorist groups linked to al-Qaeda or with membership of al-Qaeda-linked extremist Islamist groups. The evidence allegedly linking the money raised and terrorism was not disclosed to either applicant. The court considered that this did not enable them to effectively challenge these serious allegations.[129] While the ECtHR did not directly challenge the actual legality of the use by the Special Immigration Appeals Commission (SIAC) of 'closed materials' and the system of special advocates in the UK Prevention of Terrorism Act,[130] it did raise concerns about the practical challenges faced by special advocates in usefully fulfilling their function[131] and set a number of conditions for UK practices to be ECHR-compliant.

In particular, a key message from the court was that "non-disclosure" cannot deny a party knowledge of the very essence of the allegations against her/him. While the court acknowledged that the question should be established on a case-by-case basis, it generally found that "where…the open material consisted purely of general assertions and SIAC's decision to uphold the certification and maintain the detention was based solely or to a decisive degree on closed material, the procedural requirements of Article 5 § 4 would

---

[124] Refer to paragraphs 46 and 49 of Klass judgment.

[125] For an assessment refer to Section 3.1 of: Bigo et al., op. cit.; see also *Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, § 80; *Liberty and Others v. the United Kingdom*, No. 58243/00, 1/10/2008. *Kennedy v. the United Kingdom*, No. 26839/05, 18.8.2010.

[126] *Van Mechelen and Others v. The Netherlands*; and *Leas v. Estonia*.

[127] *Fitt v. United Kingdom; Jasper v. United Kingdom; and Leas v. Estonia*.

[128] This was the issue in *Bucur and Toma v. Romania*, which dealt with a whistle-blower, where the ECtHR held that *"*...by refusing to verify whether the 'top secret' classification was justified and to answer the question of whether the interest in maintenance of the confidentiality of the information prevailed over the public interest in learning about the alleged unlawful telephone tapping, the domestic courts had not sought to examine the case from every angle, thereby depriving the applicant of the right to a fair trial" (see European Court of Human Rights, National Security and European case-law, op. cit., p. 34).

[129] §223.

[130] In paragraph 219 the ECtHR stated, "The Court considers that SIAC, which was a fully independent court (see paragraph 91 above) and which could examine all the relevant evidence, both closed and open, was best placed to ensure that no material was unnecessarily withheld from the detainee. In this connection, the special advocate could provide an important, additional safeguard through questioning the State's witnesses on the need for secrecy and through making submissions to the judge regarding the case for additional disclosure. On the material before it, the Court has no basis to find that excessive and unjustified secrecy was employed in respect of any of the applicants' appeals or that there were not compelling reasons for the lack of disclosure in each case."

[131] In paragraph 220, the Court stated that it "further considers that the special advocate could perform an important role in counterbalancing the lack of full disclosure and the lack of a full, open, adversarial hearing by testing the evidence and putting arguments on behalf of the detainee during the closed hearings. However, the special advocate could not perform this function in any useful way unless the detainee was provided with sufficient information about the allegations against him to enable him to give effective instructions to the special advocate".

not be satisfied." The information should therefore be sufficiently specific for the applicant not to be denied an opportunity to effectively challenge the accusation or the reasonableness of the Secretary of State's belief and suspicions about her/him. **On this basis, the court found the UK to be in violation of Article 5.4 ECHR.**[132] As we shall show in Section 3.2, this has also been developed as an **important CJEU standard when scrutinising intelligence accountability in the EU**.

The ECtHR has also been clear regarding the use and/or admission of 'torture evidence'. In Husayn v. Poland,[133] the court stated that if 'torture evidence' were admitted in a criminal trial, it would amount to a 'flagrant denial of justice' and violation of Article 6 ECHR. The ECtHR pursued a 'rule of law' argument and held:

> No legal system based upon the rule of law can countenance the admission of evidence – however reliable – which has been obtained by such a barbaric practice as torture. The trial process is a cornerstone of the rule of law. Torture evidence irreparably damages that process; it substitutes force for the rule of law and taints the reputation of any court that admits it…Statements obtained in violation of Article 3 are intrinsically unreliable…The admission of torture evidence is manifestly contrary, not just to the provisions of Article 6, but to the most basic international standards of a fair trial. It would make the whole trial not only immoral and illegal, but also entirely unreliable in its outcome.[134]

4.1.3 Effective remedies and effective judicial controls

The provision of effective and adequate safeguards against abuse has played a particularly important role for the ECtHR in determining the adequacy of the law and the legitimacy of interference with human rights.[135] Two of the most important provisions have been Article 6 ECHR, which stipulates the right to a fair trial, and Article 13 ECHR, which covers the right to an effective remedy (see Annex 2 of this study on Relevant Legal Fundamental Human Rights Provisions).

As regards Article 13 ECHR, and the notion of effective remedies, the Strasbourg Court has attached particular importance to **the existence and availability of a remedy to enforce effectively the substance of ECHR rights at the domestic level and grant appropriate relief in cases of alleged interferences by the State**.[136] A common thread in Strasbourg jurisprudence has been that **the more serious the alleged violation of a human right is, the higher the scrutiny standards attached to Article 13 ECHR**.[137] A remedy must be effective in nature. As provided in the 2014 case of Al Nashiri v. Poland,[138] "effective" means that **it must be possible to exercise the remedy without unjustifiable hindrance by the actions or inaction of state authorities.**[139] In the same judgment, and in relation to Article 3 ECHR, the court ruled that the notion of

---

[132] Paragraph 223 of the ruling states, "However, in each case the evidence which allegedly provided the link between the money raised and terrorism was not disclosed to either applicant. In these circumstances, the Court does not consider that these applicants were in a position effectively to challenge the allegations against them. There has therefore been a violation of Article 5 § 4 in respect of the first and tenth applicants."

[133] *Husayn (Abu Zubaydah) v. Poland*, Application no. 7511/13 of 24 July 2014.

[134] § 554.

[135] See European Court of Human Rights, National Security and European case-law, op. cit., page 9. See also *Kennedy v. United Kingdom*, no. 26839/05, 18 May 2010. "The assessment of this matter depended on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law". Pages 11 and 12 of ECtHR note on national security.

[136] In the above-mentioned case *Klass and others v. Germany* Application No. 5029/71 of 6 September 1978, the Court stated, "For the purposes of the present proceedings, an 'effective remedy' under Article 13 (art. 13) must mean a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance" (§69).

[137] Cameron, op. cit., pp. 34-35.

[138] *Al Nashiri v. Poland* (Application No. 28761/11) of 24 July 2014.

[139] The court stated, in § 546-547, "Where an individual has an arguable claim that he has been ill-treated by agents of the State, the notion of an 'effective remedy' entails, in addition to the payment of compensation where appropriate, a thorough and effective investigation capable of leading to the identification and punishment of those responsible and including effective access for the complainant to the investigatory procedure".

effective remedy under Article 13 ECHR requires **independent and rigorous scrutiny of the claim** and "this scrutiny must be carried out without regard to what the person may have done to warrant his expulsion or to any perceived threat to the national security of the State".[140]

The ECtHR has also consistently justified the need for scrutiny of intelligence activities with a clear 'rule of law' argument insofar as it should avoid the executive from acting arbitrarily or with unfettered powers.[141] The ECtHR has affirmed that **the executive is not free from effective control by national courts even in situations dealing with national security and matters of political violence**.[142] In the cases Klass and Kennedy v. the UK, the ECtHR found that it was essential for any interference by the executive in human rights to be subject to effective control, which should ordinarily (or rather preferably) be ensured by the judiciary.[143] This judicial control should offer the best guarantees of independence, impartiality and proper procedure.

It is true that, in the Klass case, the lack of judicial control was not deemed to be a violation of Article 13 ECHR, as the court considered that there were **other supervisory authorities conducting "effective and continuous controls"** and vested with **"sufficient independence",** along with other safeguards for individual remedies.[144] Article 13 ECHR does not therefore necessarily require judicial remedies sensu stricto. For the ECtHR, one of the most important features for defining a body as a "tribunal" is that **it carries out a judicial function** – in particular, that it **acts to resolve conflicting interests "on the basis of rule of law, following proceedings conducted in a prescribed manner"**.[145]

A key message is that everyone affected by a state measure adopted in the name of national security has to be guaranteed protection against arbitrariness and the individual must be able to challenge the executive's position based on national security. This was a clear line of argumentation by the ECtHR in Dalea v. France, which concerned the refusal to grant the applicant access to corrections to his personal data recorded in the Schengen Information System (SIS) by the French Security Intelligence Agency for the purposes of refusing entry.[146] Also, in Al-Nashif v. Bulgaria the ECtHR held that "any measure affecting human rights must be subject to a form of adversarial proceedings before an independent body competent to review the reasons for the decision and relevant evidence, if need be with appropriate procedural limitations on the use of classified information".[147]

In a similar vein, the ECtHR has been clear in stipulating that independence is essential in order to prevent a flagrant denial of justice. In Le Compte et al v. Belgium (1981) ECHR Series A no. 43, the Strasbourg Court stated that "the use of the term 'tribunal' is warranted only for an organ which satisfies a series of further requirements – independence of the executive and of the parties to the case, duration of its members' term of office, guarantees afforded by its procedure".[148] Similarly, in Husayn v. Poland,[149] the Strasbourg Court concluded that Poland had violated its responsibility under Article 6.1 of the ECHR as a result of its cooperation with, and assistance to, the CIA in the transfer of the applicant from its territory "despite a real and foreseeable risk that he could face a flagrant denial of justice".[150] The ECtHR held that the US military

---

[140] *El-Masri v. The Former Yugoslav Republic of Macedonia*, Application No. 39630/09, 13 December 2012. Reference was here also made to the *Chahal* case § 151 and *El-Masri* case § 257.

[141] Refer to *Malone v. United Kingdom*, 2 August 1984, Series A no. 82. Also, in its DEB Case C-279/09 *DEB v. Germany*, 22 December 2010.

[142] See for instance *Chahal v. United Kingdom* (1996) 23 EHRR 413, §§ 130-31.

[143] Refer to paragraphs 55-56 in *Klass* and paragraphs 167 of *Kennedy*.

[144] See paragraph 56 of the judgment. The importance of procedures monitored by judicial authorities has been highlighted, for instance, in the context of detention and Article 5.4 ECHR. See *A and other v. UK* (2009) Application no. 3455/05. See also *Lucà v. Italy* (no. 33354/96, § 40, ECHR 2001-II); *Doorson v. The Netherlands*, 26 March 1996, § 70, *Reports* 1996-II, §§ 68-76.

[145] *Sramek v. Austria*, (1984) ECHR Series A no. 84.

[146] *Dalea v. France*, no. 964/07, of 2 February 2010.

[147] Page 16 of the ECtHR note on national security.

[148] See also De Wilde, Ooms and Versyp judgment of 18 June 1971, Series A no. 12, p. 41, par. 78; Neumeister judgment of 27 June 1968, Series A no. 8; Guzzardi judgment of 6 November 1980, Series A no. 39.

[149] *Husayn (Abu Zubaydah) v. Poland*, op. cit.

[150] § 560 of the judgment.

commission did not offer guarantees of impartiality and independence from the executive as required of a "tribunal" under previous case law, and that there was a "sufficiently high probability of admission of evidence obtained under torture in trials against terrorist suspects".[151]

The question as to 'what' constitutes a judicial authority or a tribunal has attracted substantive judicial attention both in Strasbourg and Luxembourg. The need for a 'judicial' actor to be involved or not involved in the scrutiny of 'national security' is one of the most fundamental differences when comparing ECtHR standards on intelligence accountability with those enshrined in the EU Charter of Fundamental Rights and developed by the Court of Justice of the European Union (CJEU) for the European legal system. Indeed, in the scope of EU law, **the CJEU has also underlined the central role of independence and impartiality in determining what is a tribunal**. In the case C-24/92 Corbiau [1993] ECR I-1277, the Luxembourg Court clarified the centrality of independence and its meaning for the purposes of EU law by stipulating that "[it] can only mean an authority acting as a third party in relation to the authority which adopted the decision forming the subject-matter of the proceedings". Moreover, in the case C-506/04 Wilson, the CJEU held that "the concept of independence, which is inherent in the task of adjudication, involves primarily an authority acting as a third party in relation to the authority which adopted the contested decision."[152]

4.2 EU Principles and Standards

In the scope of EU law, the CJEU has also developed a set of judge-determined supranational principles with relevance to cases dealing with national security, state secrets, intelligence and the rights of the defence. A selected list of relevant CJEU case law is provided in Annex 1 of this study. **The EU judicature has considered the role of judicial accountability to be central when determining the legitimacy and legality of Member States' actions and the use of closed evidence in cases related to acts of political violence**. What are the main principles developed by the Luxembourg Court? And how do they differ from ECtHR principles studied in Section 3.1 above?

4.2.1 Judicial scrutiny and effective judicial review in the EU legal system

When looking at the role of judicial accountability in assessing the legality of Member States' actions, Article 47 (Right to an Effective Remedy and Fair Trial) and Article 48 (Presumption of Innocence and Right of Defence) of the EU Charter of Fundamental Rights are of particular relevance. The EU Charter has **the same legal value as primary European law**. While the first paragraph of Article 47 is rooted in Article 6 ECHR, the degree of legal protection offered in EU law is greater. Article 47 stipulates the right to an effective remedy and to a fair trial "before an independent and impartial tribunal" instead of before a "national authority".[153] The judicial nature of scrutiny finds its foundations in CJEU case law, which has considered judicial accountability a "general principle of EU law".[154] Also, unlike Article 6 ECHR, the right to a fair trial enshrined in Article 47 EU Charter is not exclusively confined to "civil law rights". The CJEU held, in Les Verts v. European Parliament,[155] that this is justified because the EU:

---

[151] § 557. Refer also to *Al Nashiri v. Poland*, op. cit., § 562-569. See § 563 for a definition of "flagrant denial of justice".

[152] Paragraphs 49-53 of the judgment. The court clarified that this concept has two other aspects. The first aspect, which is external, presumes that the body is protected against external intervention or pressure liable to jeopardise the independent judgment of its members as regards proceedings before them. That essential freedom from such external factors requires certain guarantees sufficient to protect the person from those who have the task of adjudicating in a dispute, such as guarantees against removal from office. The second aspect, which is internal, is linked to impartiality and seeks to ensure a level playing field for the parties to the proceedings and their respective interests with regard to the subject matter.

[153] Refer to P. Aalto et al. (2014), "Article 47 – Right to an Effective Remedy and to a Fair Trial", in S. Peers, T. Hervey, J. Kenner and A. Ward (eds), *The EU Charter of Fundamental Rights: A Commentary*, Oxford: Hart Publishing, p. 1208.

[154] Refer, for instance, to Case 222/84 Johnston [1986] ECR 1651.

[155] Case C-294/83 *Les Verts v. European Parliament,* 23 April 1986.

> …is a Community based on the rule of law, inasmuch as neither its Member States nor its institutions can avoid a review of the question whether the measures adopted by them are in conformity with the basic constitutional charter, the Treaty.[156]

The basic constitutional charter of the EU now includes as one of its core components the EU Charter of Fundamental Rights and the right of defence outlined in its Title VI (Justice). The relevance of effective and open justice has been recently re-emphasised by the CJEU in ZZ v. Secretary of the State of Home Department C-300/11 of 4 June 2013. The court reconfirmed that the provision of effective judicial review is also of central significance in cases dealing with national security.[157] The CJEU was of the opinion that "the mere fact that a decision concerns State security cannot result in European Union law being inapplicable".[158] It added that, where a national authority opposes precise and full disclosure to the person concerned of the grounds constituting a decision refusing entry into a Member State for reasons of State security,[159] **Member States are required to provide effective judicial review and prescribe rules related to that review**.[160]

This line of jurisprudence has been recently confirmed in the Unitrading case of October 2014,[161] which, while dealing with different subject matter, may help to understand the CJEU's approach on the meaning and reach of 'effective remedy' in the EU. The CJEU confirmed that, while the possibility offered to an individual to challenge the information and present alternative evidence would be sufficient to meet the Article 47 threshold, **the EU law principle of effectiveness calls for further guarantees**. The CJEU found that, in accordance with the EU principle of effectiveness, the national tribunal is required to use all available procedures under domestic law if the burden of proof makes it "impossible or excessively difficult" for alternative evidence to be produced because the evidence relates to data which the person could not possess.[162] This ruling imposes a new obligation on the national court to use all means in procedural rules, including powers of inquiry, to remedy the defect that the individual cannot remedy him- or herself. This requirement may be of central importance in proceedings before the Special Immigration Appeal Commission in the UK.

4.2.2 Key EU case law in the use of intelligence information in EU antiterrorism policies

The 'Kadi case law trilogy' is also of central importance to our discussion, as the Luxembourg Court provided clear legal standards when assessing **the legality of executive interference with the right of the defence by intelligence activities/information in the scope of EU antiterrorism policies**. In order to implement in the EU legal system the various UN Security Council Resolutions calling on States to freeze funds and other financial assets of individuals associated with al-Qaeda and Usama bin Laden, the EU Council adopted a common position and Regulation 881/2002 providing for these measures and an annexed

---

[156] Paragraph 23 of the judgment.

[157] See also the *Kadi* judgement on judicial supervision (http://curia.europa.eu/juris/document/document.jsf?text=&docid=139745&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=205883), paragraphs 326 and 327. The court stated: "The Court has held nonetheless that, even in proceedings under Article 6 for the determination of guilt on criminal charges, there may be restrictions on the right to a fully adversarial procedure where strictly necessary in the light of a strong countervailing public interest, such as national security, the need to keep secret certain police methods of investigation or the protection of the fundamental rights of another person. *There will not be a fair trial, however, unless any difficulties caused to the defendant by a limitation on his rights are sufficiently counterbalanced by the procedures followed by the judicial authorities"* (emphasis added) (§205).

[158] See Case C-387/05 Commission v. Italy [2009] ECR I-11831, paragraph 45.

[159] Paragraph 57.

[160] Paragraph 58. See also paragraphs 65 and 66.

[161] C-437/13 *Unitrading* 23 October 2014.

[162] Paragraph 28 of the judgment states: "In order to ensure compliance with the principle of effectiveness, if the national court finds that the fact of requiring the person liable for the customs debt to prove the place of origin of the goods declared, in that the onus is on him to refute the relevance of indirect evidence used by the customs authorities, is likely to make it impossible or excessively difficult for such evidence to be produced, since inter alia that evidence relates to data which the person liable could not possess, it is required to use all procedures available to it under national law, including that of ordering the necessary measures of inquiry".

list of individuals and entities which is regularly updated on the basis of successive UN resolutions.[163] Mr Kadi, a Saudi resident, and the Al Barakaat International Foundation, established in Sweden, were listed in the EU Regulation. He brought an action for annulment before the Court of First Instance, claiming, inter alia, that his fundamental right of defence had been breached, in particular the right to be heard and the right to effective judicial review. The Court of First Instance (now the General Court) dismissed his claims and concluded that Member States were required to comply with the Security Council resolutions under the terms of the UN Charter, an international treaty that prevails over Community law.[164]

Mr Kadi appealed this decision before the CJEU. In the Joined Cases C-402/05 P and C-415/05 P Kadi and Al Barakaat International Foundation v. Council and Commission [2008] ECR I-6351 (**Kadi I Judgment**) of 3 September 2008, the CJEU reviewed the lawfulness of EU legislation transposing into the European legal system UN Security Council Resolution 1390 (2002). A key issue of concern for the court was that Mr Kadi had not been properly informed of the grounds for the inclusion of his name on the UN terrorist list and hence he could not obtain judicial review of this decision, with the consequence that his right of defence was violated. The court held that an international agreement could not prejudice EU constitutional principles, including that all EU acts must comply with fundamental rights in order for them to be lawful.[165]

Similar to the ECHR standards identified above, the judgment underlined the need to ensure effective judicial review and substantiated this requirement by requiring any Community authority working on issues related to 'national security' to disclose the grounds for including a person or entity on a 'terrorist list' "so far as possible, either when that inclusion is decided on or, at the very least, as swiftly as possible after that decision in order to enable those persons or entities to exercise, within the periods prescribed, their right to bring an action". The Luxembourg Court held that this was necessary in order to guarantee the rights of the defence and allow the Community judicature to review the lawfulness of the EU measure in question.[166] The CJEU also concluded that the rights of the applicants to defend themselves in satisfactory conditions had been violated and consequently their right to an effective remedy had been equally infringed.[167]

Following this judgement, the response of the EU was to request the UN Sanctions Committee to provide the narrative summary of the reasons for Mr Kadi's listing. On the basis of a summary of these reasons, and irrespective of Mr Kadi's arguments against lack of supporting evidence, the European Commission considered justified his insertion in the list and informed Mr Kadi of the adoption of the new Regulation 1190/2008, amending the former Regulation 881/2002, where his name would still appear listed in Annex I for reasons of association with the al-Qaeda network. Mr Kadi brought a new action for annulment before the General Court in early 2009. The General Court held that judicial review should extend not only to the apparent merits of the contested measure, but also to the information on which the findings made in that

---

[163] Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaeda network and the Taliban, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan (OJ 2002 L 139, p. 9).

[164] Case T-306/01 *Yusuf and Al Barakaat Foundation v. Council* and Case T-315/01 *Kadi v. Council and Commission*, of 21 September 2005.

[165] Paragraphs 34 and 35. The court's decision was somehow inspired by the opinion delivered by Advocate-General Maduro in the same case of 16 January 2008, where he underlined: "The claim that a measure is necessary for the maintenance of international peace and security cannot operate so as to silence the general principles of Community law and deprive individuals of their fundamental rights. This does not detract from the importance of the interest in maintaining international peace and security; it simply means that it remains the duty of the courts to assess the lawfulness of measures that may conflict with other interests that are equally of great importance and with the protection of which the courts are entrusted…when the risks to public security are believed to be extraordinarily high, the pressure is particularly strong to take measures that disregard individual rights, especially in respect of individuals who have little or no access to the political process…the courts should fulfil their duty to uphold the rule of law with increased vigilance. Thus, the same circumstances that may justify exceptional restrictions on fundamental rights also require the courts to ascertain carefully whether those restrictions go beyond what is necessary".

[166] Paragraphs 336 and 337.

[167] Paragraph 349.

measure are based. In Case T-85/09, Kadi v. European Commission of 30 September 2010 (**Kadi II judgment**), the court not only confirmed the CJEU Kadi I judgment,[168] but it also stated:

> …although overriding considerations relating to safety or the conduct of international relations of the Community and of its Member States may militate against the communication of certain matters to the persons concerned, that does not mean, with regard to respect for the principle of effective judicial protection, that restrictive measures…escape all review by the Community judicature once it has been claimed that the act laying them down concerns national security and terrorism[169]

The CJEU therefore annulled Commission Regulation 1190/2008 with regard to Mr Kadi. By doing so the Luxembourg Court reiterated **the principle of effective judicial protection as a key EU standard and clarified the degree of judicial review** to be applied in the scope of EU law.

The CJEU was called on again to intervene in light of the appeals by the Commission, the Council and a number of EU Member States. In the **Kadi III judgment**, Joined Cases C-584/10 P, C-593/10 P and C-595/10 of 18 July 2013, the court re-emphasised that EU courts must review the assessment carried out by any EU institution and determine whether the information and evidence on which that assessment has been based is accurate, reliable and consistent. In the court's opinion, such review cannot be barred on the grounds that that information and evidence are secret or confidential.[170] The CJEU confirmed in this judgment that the restrictive measures under consideration enjoyed no immunity from jurisdiction.[171] Also, when re-examining the rights of the defence, the CJEU held that this included **the right to be heard and the right to have access to the file subject to legitimate interests in maintaining confidentiality**. The right to effective judicial protection enshrined in Article 47 of the EU Charter requires that the person involved "must be able to ascertain the reasons upon which the decision taken in relation to him is based". This, in the court's view, constitutes a pre-condition enabling anyone to defend his/her rights and for the court to examine the lawfulness of the decision in question.[172]

The CJEU concluded that the inclusion by the European Commission of Mr Kadi's name in the revised EU Regulation **was not based on 'evidence', but rather on a 'summary of reasons'** provided by the UN Sanctions Committee. The CJEU stated that respect for the rights of the defence and effective judicial remedy require the competent Union authority **to disclose to the individual concerned the evidence against him/her available to that authority, which must include, at the very least, the summary of the reasons**. The individual must benefit from minimal procedural safeguards allowing him/her "to defend [his/her] rights in the best possible conditions" and "effectively make known [his/her] views on the grounds advanced against [him/her]".[173] Also, the court held that the judicial review has to focus on verifying whether the decision restricting the person's fundamental rights has been taken **on a solid factual basis**, which includes verifying whether the decision has been substantiated and the factual allegations in the summary of reasons underpinning the decision.[174]

The Kadi trilogy has generated extensive discussions across the scholarly literature, particularly concerning the way in which the CJEU ruled on the relationship between international relations, national security and the fundamental rights of the individual.[175] De Búrca (2010) argued that "the judgment represents a significant departure from the conventional presentation and widespread understanding of the EU as an actor

---

[168] Paragraphs 132 and 133 of Case T-85/09, *Kadi v. European Commission*, 30 September 2010.

[169] Paragraph 134.

[170] Paragraph 41.

[171] Paragraph 67.

[172] Paragraph 100.

[173] Paragraphs 110 and 111.

[174] The CJEU held that "it is necessary that the information or evidence produced should support the reasons relied on against the person concerned". Paragraph 119. See also Paragraphs 122 and 125.

[175] M. Avbelj, F. Fontanelli and G. Martinico (2014), *Kadi on Trial: A Multifaceted Analysis of the Kadi Trial*, London: Routledge; N. Türküler Isiksel (2010), "Fundamental Rights in the EU after Kadi and Al Barakaat", *European Law Journal*, Volume 16, Issue 5, pp. 551-577; S. Poli and M. Tzanou (2009), "The Kadi Rulings: A Survey of the Literature", *Yearbook of European Law* 28 (1), 533-558.

maintaining a distinctive commitment to international law and institutions."[176] Kokkot and Sobotta (2012)[177] took a different stance:

> Should the EU convey the impression of sacrificing basic constitutional guarantees by accepting the general primacy of Security Council measures, Member States, in particular their constitutional courts, would probably feel tempted to take safeguarding these guarantees into their own hands. From an international perspective this would be even worse: It would not only question the primacy of public international law within the EU legal order but also call into question the primacy of EU law over national law…Also from this perspective Kadi could hardly have been decided differently.[178]

Against the international backdrop of antiterrorism measures, there was indeed a relaxation of the burden of proof prior to coercive measures being adopted and the individual's status as a subject of fundamental human rights was neglected. As Guild (2010) signalled,[179] there is often a sloppy approach by which evidence is contaminated with supposition and conjecture through the use of 'intelligence information'. This came at a time where the right to challenge a decision in an impartial tribunal was being dispensed with as unnecessary. Indeed, in Kadi the European judiciary took a clear and welcome stance for the fundamental rights of the individual and developed far-reaching supranational standards as regards the use of 'intelligence information' in proceedings before European courts. The European judiciary concluded that, **irrespective of international obligations, respect for fundamental rights lies at the very foundations of the Union legal order, including those enshrined in Article 6 of the Treaty on the European Union and the EU Charter**.

Another illustrative case of the challenges posed by confidential information to the European judicature are the 'freezing of funds' decisions adopted by the Council of the EU, which were subject to judicial attention in the Case C-27/09 P French Republic v. People's Mojahedin Organization of Iran (PMOI) of 21 December 2011. The CJEU confirmed the ruling handed down previously by the General Court in the same case, which had concluded that the contested EU decision had been adopted against the EU principles on the rights of the defence.[180] The CJEU upheld **the requirement of prior notification** of a fund-freezing measure, as prior notification of the incriminating evidence against the person would not have harmed the 'effectiveness' of the restrictive measures.[181] The court found that it is essential, if the rights of the defence are to be properly upheld, that the person involved is notified of the incriminating evidence and the right to make representations before the decision is taken, so that he has the opportunity to correct a mistake or "produce such information relating to his personal circumstances as will tell in favour of the decision's being adopted or not".[182] The court held that this 'right' is enshrined in Article 41.2a of the EU Charter of Fundamental Rights.

4.2.3 The use of intelligence information before the Luxembourg courts

The use of intelligence information before the CJEU in Luxembourg remains a contested issue.[183] **Discussions on the use of intelligence information before the General Court** are currently under way.[184]

---

[176] G. De Búrca (2010), "The European Court of Justice and the International Legal Order After Kadi", *Harvard International Law Journal*, Vol. 51, Number 1, pp. 1-49.

[177] J. Kokott and C. Sobotta (2012), The Kadi Case – Constitutional Core Values and International Law – Finding the Balance?, *The European Journal of International Law*, 23, 4, pp. 1015-1024.

[178] Ibid., p. 1019.

[179] E. Guild (2010), "EU Counter-Terrorism Action: A Fault Line between Law and Politics", CEPS Liberty and Security in Europe Series, Brussels.

[180] Paragraph 25 of the judgment. The subsequent decision to freeze funds by which the inclusion of the name of the person/entity is maintained, "must be preceded by notification of the incriminating evidence and by allowing the person or entity concerned an opportunity of being heard…the Council was bound imperatively, to ensure that the PMOI's right of defence were observed, that is to say, notification of the incriminating evidence against it and the right to be heard, before that decision was adopted".

[181] Paragraph 62.

[182] Paragraphs 64 and 65.

[183] C. Murphy (2014), Secret Evidence in EU Security Law: Special Advocates before the Court of Justice?, in Cole, Fabbrini and Vedaschi, op. cit, pp. 1-9.

The **Draft Rules of Procedure of the General Court of the European Union** are being negotiated in the Council and contain one chapter dealing with information or material pertaining to the security of the Union or of its Member States or to the conduct of their international relations.[185] The new Article 105 of the Draft Rules of Procedure would guarantee that the General Court has full access to the information/material in order to determine the extent to which the latter should be confidential to the other main party. If the General Court were to conclude that the information is not confidential, and the first party objected to its communication to the other party, the information would not be taken into account in the determination of the case. Should the Court reach the conclusion that the information is confidential, Article 105.6 would require "a non-confidential version or non-confidential summary of the information or material containing the essential content thereof and enabling the other main party to make its views known". In this way, the new Rules **would require the judge to have access to that information as the central element**.[186] The new draft wording therefore follows to a large extent the above-mentioned case law of the CJEU. However, the proposed paragraph 7 of draft Article 105 would, in our view, pose serious challenges in upholding the rights of the defence laid down in the EU Charter and the Union's constitutional guarantees as the CJEU called for in the Kadi trilogy and PMOI judgements. This paragraph, if finally adopted, would entitle the General Court to base its judgement on information which, due to its confidential nature, would not be communicated to the other party in accordance with the procedures outlined above.[187] This procedure would take us close to the use of closed information in the UK and the Netherlands detailed in Section 1 of this study.

The argument of secrecy (and the state secrets privilege) invoked to obstruct investigations, inquiries and judicial scrutiny has thus created a whole series of tensions between the highest levels of the executive, intelligence communities and judicial authorities in the EU, and has often ended up before European courts. These courts have developed very useful legal standards or 'red lines' when determining the legality of EUMS' and intelligence communities' decisions to invoke national security and state secrets and thereby to interfere with the rights of the defence enshrined in the ECHR and the EU Charter of Fundamental Rights. At the same time, the "national security" justification has often been used to curb freedom of expression and information, also recognised as fundamental rights, and to limit the protection of whistle-blowers, thereby restricting scope for disclosure of these issues in the public interest and often undermining the freedom of the press. This is a key challenge analysed in the following section.

---

[184] Murphy, op. cit., pp. 1-9.

[185] See the Draft Rules of Procedure of the General Court, in particular Chapter 7, available at http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207795%202014%20INIT.

[186] Ibid., new Article 105 of the draft Rules of Procedure.

[187] The proposed Article 105.7 also states that "When assessing the information or material, the General Court shall take account of the fact that a main party has not been able to make his views on it known".

5. Freedom of the press and protection of whistle-blowers

KEY FINDINGS

- The freedom of the press, the protection of sources in journalism, and the protection of whistle-blowers are too often jeopardised when national security is invoked. While forms of protection for journalists and whistle-blowers exist in the EUMS under examination, so do legal restrictions linked to national security arguments.
- In some cases, the involvement of media sources in criminal proceedings has enhanced the protection of the source and the freedom of the press (Germany).
- Judgments handed down by courts in the Netherlands that compromised journalists' sources were challenged by the ECtHR.
- Attempts to compromise source protection and the freedom of the press have also been found in the UK, where contradictory rulings reveal the vulnerability of these freedoms when national security is invoked.
- As regards whistle-blowers, the current debates over Snowden and the nature and consequences of his revelations emphasise further the tensions between security and classified information and the freedom of information.

One of the issues raised by the use of CMPs and the national security argument relates to the pivotal role played by investigative journalism and whistle-blowers in disclosing matters of public interest and concern. Our analysis of EUMS' laws and practices on the use of secrecy sheds an interesting light on the freedom of the press and the protection of whistle-blowers. Both the freedom of the press (and in particular the protection of journalists' sources (4.1)) and the right to be protected if reporting officials' wrongdoing and unlawful practices (4.2) are vital to the proper functioning of our modern democracies. As detailed hereafter, these rights are often compromised and too often jeopardised when national security arguments are invoked. This section argues that restrictions to the freedom of the press and to the protection of whistle-blowers clearly hamper public awareness as regards the functioning of their institutions.

5.1 'State secrets', the freedom of the press and the right to information

To what extent does the use of secrecy obstruct the duty of journalists to inform the public? Recent debates in the UK have revolved around an attempt by the Crown Prosecution Service to hold a terrorism trial entirely in secret in the case referred to as The Crown v. AB and CD. The initial request for a secret trial would have prevented anyone from knowing even the identity of the people accused. Following a legal challenge by *The Guardian* and other media, the request was overturned in June 2014 by the Court of Appeal. The compromise reached in this ruling includes the accreditation of a few journalists, who will be permitted to attend the "bulk" of the trial but will not be able to report on the proceedings until there have been further legal arguments. A transcript of the case could eventually be released but only after further legal argument. This compromise has triggered further debates over restrictions on the principle of open justice. Debates in the UK are still ongoing over how to accommodate in camera trials with access for journalists.

In the context of the debates around the JSA, the UK Human Rights Joint Committee took evidence from an investigative journalist at *The Guardian*, Ian Cobain, who has reported widely in recent years on matters such as complicity in torture and extraordinary rendition.[188] Referring to the Al Rawi and Binyam Mohamed cases analysed in Section 2.3, Cobain told the committee that material disclosed in legal proceedings has been "vitally important" as a source of information to journalists. He said that journalists like himself were "heavily reliant on documents that have been disclosed in court", which were often crucial either to corroborate allegations of wrongdoing which had been heard elsewhere, or to contradict assurances or denials. Cobain argued that the use of CMPs as implemented by the JSA would prevent similar disclosure of

[188] Human Rights Joint Committee: The impact on media freedom and democratic accountability, 2012, available at www.publications.parliament.uk/pa/jt201012/jtselect/jtrights/286/28609.htm#a40.

evidence and documentation that has enabled journalists to build up a true picture of the government's involvement in certain actions since 9/11, such as those demonstrated in the Al Rawi and Binyam Mohamed cases. **The prospect of "a small number" of journalists being officially selected to attend secret sessions in a terrorism trial, and the restrictions that would be applied, has raised fresh concerns about media freedom**.

A related issue concerns the protection of journalists' sources when challenged by national security concerns. The protection of the source is not only key to investigative journalism, but is also a well-established right recognised in European and international law. The ECtHR has repeatedly emphasised that Article 10 of the ECHR safeguards not only the substance and content of information and ideas, but also the means of transmitting them. The press has been accorded the broadest scope of protection in the court's case law, including with regard to confidentiality of journalistic sources. In its 1996 judgement in Goodwin v. the United Kingdom, the ECtHR stated:

> Protection of journalistic sources is one of the basic conditions for press freedom...Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information be adversely affected...[A]n order of source disclosure...cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest.[189]

However, the notion of overriding requirement in the public interest remains quite broad and opens up possibilities of obstructing press freedom. In **France**, for instance, a special law was adopted in 2010 in order to guarantee the protection of sources. However, the law stated that guarantee would be suspended where there was an overriding requirement in the public interest, which illustrates the wide margin of appreciation left to define what constitutes such a requirement. In **Italy**, the only protection offered to investigative journalistic sources is provided by Art 200.3 of the Italian Code of Criminal Procedure, which recognises journalists' right not to reveal their confidential sources in court, unless the judge deems the identification of such sources to be fundamental to the trial. Should that be the case, the judge is entitled to order the journalist to reveal his/her sources. In **Sweden**, the protection of sources appears quite strong. The relationship between the freedom of speech, freedom of the press (both regulated in Sweden's fundamental laws), and secrecy is described in the Public Access to Information and Secrecy Act. While the Act stipulates that freedom of speech and the freedom of the press are suspended if the publication of information could "put the safety of the state in danger or seriously harm the country",[190] the government is "in certain cases allowed to disclose secret information verbally for publication in, for instance, a newspaper, but…it is never allowed to disclose the secret official document which contains this information nor to disclose information if one thereby commits such a crime as referred to in the said fundamental laws".[191] This structure makes it possible for public officials to share secret information without committing a criminal offence. They are allowed to share information to enhance debate among the general public "if they consider that the interest of public access to the authorities' operations weighs more heavily in the balance than the interest to be protected by the secrecy".[192]

Some EUMS under examination have experienced several cases where media sources have been challenged on national security grounds, with different outcomes.

In some cases, the involvement of media sources in criminal proceedings has enhanced the protection of the source and the freedom of the press. In Germany, for instance, the Cicero affair in 2005 led the Federal Constitutional Court to rule that the police search of the editorial department of the monthly news magazine *Cicero* was unconstitutional. In April 2005, *Cicero* published an article on the Islamist terrorist Abu Musab al-Zarqawi in which a top-secret report from Germany's Federal Criminal Police Office (BKA) was quoted. Not long afterwards, the magazine's office in Potsdam was searched along with the apartment of

---

[189] Protection of journalistic sources, ECHR fact sheet, June 2014, available at: www.ECHR.coe.int/ Documents/FS_Journalistic_sources_ENG.pdf).

[190] See: Sveriges Riksdag 2009a: Chap 15, par. 6.

[191] Ministry of Justice (2009), *Public Access to Information and Secrecy Act Information concerning public access to information and secrecy legislation, etc.*, Stockholm: Government Offices, p. 32.

[192] Ibid.

the article's author. *Cicero*'s editor-in-chief filed an official complaint arguing that the search had violated the freedom of the press as guaranteed in the German Constitution. He won the case. Furthermore, and as a result of the Cicero affair, Section 353b(3a) of the Criminal Code was introduced, stating that journalists are not guilty of complicity to commit treason through the simple act of receiving and publishing secret information, which they probably received from a civil servant. As a result, editorial departments can be raided only if there is a suspicion that the journalist him- or herself is the author of a criminal offence.

Some EUMS' courts have seen their judgment compromising journalists' sources challenged by the ECtHR. In the Netherlands, the ECtHR held in the 2012 *Telegraaf* case that the Dutch authorities had disrespected the right of journalists to protect their sources. The case concerned the actions taken by the authorities against two journalists of the national daily newspaper *De Telegraaf* after they had published articles about the Dutch secret service, the AIVD. It was alleged that the journalists had leaked highly secret information to the criminal circuit. The Regional Court and the Supreme Court held that the protection of state secrets justified the interference with the right to source protection. The case was taken by the ECtHR, which found that the AIVD's telephone tapping and surveillance of two journalists lacked a sufficient legal basis, as the law did not provide safeguards appropriate to the use of powers of surveillance against journalists with a view to discovering their sources. Additionally, an order to surrender leaked documents belonging to the security and intelligence services was considered a violation of the journalists' rights as guaranteed by Article 10 of the Convention. Similarly, in the 2007 case Voskuil v. The Netherlands, the ECtHR challenged the Dutch government, which had denied journalists the right not to disclose sources. The applicant, a journalist, had written two articles for a newspaper concerning a criminal investigation into arms trafficking. The journalist was detained for more than two weeks in an attempt by the Dutch authorities to compel him to disclose his sources. The ECtHR found that the Dutch government's interest in knowing the identity of the applicant's source had not been sufficient to override the applicant's interest in concealing it, and held that there had been a violation of Article 10 of the Convention.

Attempts to compromise the protection of the source and the freedom of the press can also be found in the UK, where **contradictory rulings reveal the vulnerability of these freedoms when national security is invoked**.

In March 2014, the Metropolitan Police was prohibited from using secret evidence to seize media materials in the case of R (BSkyB) v. Commissioner of Police [2014] UKSC 17. The Supreme Court dismissed a Metropolitan Police request for media material and ruled that secret evidence cannot be used by the police to obtain court orders requiring journalists to hand over notebooks, photographs or digital files. The alleged offences concerned suspected leaks of top-secret information from meetings of the COBRA Cabinet security committee to the security editor of BSkyB. The Supreme Court based its ruling on the following arguments: while a magistrate may issue a search warrant on an application by a police constable made ex parte – without any other parties being aware or present - this process does not apply to material acquired or created for the purposes of journalism and in the possession of a person who acquired or created it for the purposes of journalism.

However, the conclusions in this case are balanced by the Miranda case. In February 2014, three High Court judges dismissed a challenge that David Miranda, the partner of the former *Guardian* journalist Glenn Greenwald (one of the key reporters behind the first Edward Snowden leaks), was unlawfully detained under counterterrorism powers for nine hours at Heathrow in August 2013. Miranda was carrying encrypted data derived from material received from Snowden. UK authorities took his mobile phone, laptop and memory cards. Miranda had argued that the use of Schedule 7, which enables authorities to stop and question individuals at airports, ports and international train stations, was disproportionate, as he was engaged not in terrorism but "responsible journalism" in the public interest, and that his detention was a contravention of his Article 10 rights under the European Convention on Human Rights. In their ruling, the judges accepted that Miranda's detention and the seizure of computer material comprised "an indirect interference with press freedom", but said this was justified by legitimate and "very pressing" interests of national security. Lord Justice Laws accepted that agreeing not to publish material simply because a government official had said it might damage national security was antithetical to the most important traditions of responsible journalism, but said this was trivial compared with the threat to security. He said neither Greenwald nor Miranda was in a position to form an accurate judgment on the matter because that would depend on knowing the whole "jigsaw" of disparate pieces of intelligence. Miranda's solicitor Gwendolen Morgan declared in a statement after the High Court Judgement in February 2014: "Despite recognising that the proper functioning of a

modern participatory democracy requires that the media be free, active, professional and enquiring, this judgment leaves little room for responsible investigative journalism which touches on national security issues".[193] In May 2014, Miranda was granted permission to appeal against this ruling.

The Miranda case has been widely commented on, including at the EU Level. The then-EU Justice Commissioner Viviane Reding publicly declared she had concerns over press freedom after Miranda's detention. "I fully share Mr. Jagland's concerns", Reding said in a tweeted message, referring to a letter sent to the British government by Council of Europe Head Thorbjoern Jagland. In his letter to Teresa May, Jagland warned, "These measures, if confirmed, may have a potentially chilling effect on journalists' freedom of expression as guaranteed by Article 10 of the European Convention on Human Rights".[194]

The Miranda case is a direct consequence of Snowden's leaks. As such, Snowden's revelations have prompted worldwide scrutiny over the balance between security and disclosure of matters of public concern. This of course raises the question of whistle-blowers and their protection, in which the understanding of what constitutes the public interest is ambiguous.

5.2 Whistle-blowing: public awareness v. classified materials

Whistle-blowing refers to the disclosure by a person, usually an employee in a government agency or private enterprise, to the public or to those in authority, of mismanagement, corruption, illegality, or some other wrongdoing. In its 2010 Resolution 1723 on the Protection of whistle-blowers, the Parliamentary Assembly of the Council of Europe "recognised the importance of whistle-blowers – concerned individuals who sound an alarm in order to stop wrongdoings that place fellow human beings at risk – as their actions provide an opportunity to strengthen accountability and bolster the fight against corruption and mismanagement, both in the public and private sectors." The Assembly resolved that "the definition of protected disclosures shall include all bona fide warnings against various types of unlawful acts" and concluded that Member States' laws "should therefore cover both public and private sector whistle-blowers, including members of the armed forces and special services."[195]

The revelations made by Snowden raised with unprecedented acuity the question of who could be considered a whistle-blower and the protection such an individual should be entitled to. Snowden and the nature of his revelations thus constitute a landmark case in which national security and state secrecy played a major role. The ongoing publication of documents leaked by Snowden has revealed details of a global surveillance apparatus run by the NSA in close cooperation with three of its Five Eyes partners: Australia, the United Kingdom and Canada. The Snowden files also revealed how allies were spying on one another and the ambivalence of private companies in their relationship with the authorities in surveillance programmes. Snowden's revelations have been well documented in our previous study on Mass Surveillance.[196]

On 14 June 2013, US federal prosecutors filed a criminal complaint against Snowden, charging him with theft of government property and two counts of violating the U.S. 1917 Espionage Act through unauthorised communication of national defence information and "willful communication of classified communications intelligence information to an unauthorised person." Each of the three charges carries a maximum possible prison term of ten years. Snowden has been granted temporary asylum in Russia.

A figure that divides opinion, Snowden is portrayed either as a hero/whistle-blower or as a defector/traitor. His supporters contend that he has shone a light on a surveillance system that tracks tens of millions of citizens and is incompatible with democratic values. His opponents argue that he has broken the law (leaking confidential information) and has put the security of his country at risk, as well as damaging US diplomatic relations with some of its allies (for example, Germany). Some have also argued that, given the protection for whistle-blowers in the US, if Snowden were concerned and wanted to be part of the American

---

[193] *The Guardian* (2014), "High court rules against David Miranda over Heathrow detention", 19 February, www.theguardian.com/world/2014/feb/19/high-court-ruling-on-david-miranda-heathrow-detention-live-coverage).

[194] BBC report (2013), "David Miranda: High Court restricts inspection of data, 22 August, www.bbc.co.uk/news/uk-23790578.

[195] Parliamentary Assembly of the Council of Europe (2010), Resolution 1723 on the Protection of whistle-blowers (available at: http://assembly.coe.int/main.asp?link=/documents/adoptedtext/ta10/eres1729.htm).

[196] Bigo et al., op. cit.

debate, he could have been without leaking confidential files to the press. The US Whistleblower Protection Act adopted in 1998 and the Whistleblower Protection Enhancement Act adopted in 2012 protect federal government employees from retaliatory action for voluntarily disclosing information about dishonest or illegal activities occurring at a government organisation. However, there are exceptions under the US whistle-blower laws for national security information, so whether Snowden could have benefited from those protection mechanisms remains an open question.

The current debates over Snowden and the nature and consequences of his revelations are far from over. Snowden's future is still very much uncertain, and the successive refusals (by France and Germany) to grant him permanent asylum, as well as his current prosecution in the US, will certainly fuel discussions of the tensions between security and fundamental freedoms. However, one cannot deny that Snowden's revelations have triggered an extraordinary global debate about the threat that mass surveillance poses to free societies and about how surveillance technologies have outpaced democratic controls.

While some EUMS already have specific legal provisions to protect whistle-blowers, there are restrictions to these when classified information is involved. In Italy, a limited level of protection from any repercussions is afforded to whistle-blowers by Art 54-bis of Legislative Decree 165/2001, aimed at protecting those public officials that report (to their superiors or to judicial authorities) misconduct within their administration. However, such protection does not apply when disclosure of the information at stake constitutes a crime in itself, as is the case for state secrets or classified information.

In Sweden, whilst support for and protection of whistle-blowers is quite strong when they are public employees, there are also several clauses that prohibit such disclosure in national security cases. If, in any way, the material leaked could be harmful to the nation, the protection ceases to exist and the whistle-blowing becomes a criminal offence.[197]

In the UK, whistle-blowers are defined in relation to ordinary employment relations and are protected from dismissal or other unfavourable treatment. The UK is often perceived as 'advanced' in the protection of whistle-blowers, with a comprehensive whistle-blower protection law adopted in 1998, the Public Interest Disclosure Act. The law applies to the vast majority of workers across all sectors: government, private and non-profit.[198] It covers a range of employment categories, including employees, contractors, trainees and UK workers based abroad. This legal protection, however, does not apply to members of the Security Services, whose disclosures are criminalised by the revised Official Secrets Act adopted in 1989. David Shayler, a British journalist and former MI5 officer, was prosecuted for seeking to make disclosures in breach of the Official Secrets Act. He leaked documents to the *Mail on Sunday* in 1997 that alleged that MI5 was bugging left-wing leaders and had investigated Labour Party ministers. In 2003, Shayler lost an appeal against his conviction. The case law makes it clear that a member of the security services must seek advance approval for disclosure of a state secret.

In the other EUMS under examination where there is limited legislation on whistle-blowing, the issue is currently being discussed.

In the Netherlands, a variety of laws and procedures provide the beginnings of a system to protect and enable disclosure from whistle-blowers, but they are very limited. Despite the fact that, in 2001, the Netherlands became one of the first European countries to introduce explicit whistle-blower procedures for public servants, protection of employees depends largely on self-regulation. The Dutch Parliament is currently considering a bill that would establish a 'House for Whistle-blowers' (*Huis voor Klokkenluiders*). The legislative proposal introduces an independent and impartial governmental institution to investigate wrongdoing and assist employees in disclosure proceedings, as well as several rules to protect whistle-blowers.

In France, a law adopted in 2013 protects whistle-blowers who disclose health and environmental risks. The Council of State (the body that acts both as the executive's legal adviser and as the Supreme Court for administrative justice) evoked the scenario of a 'Snowden case' in France in its annual report published in September 2014. . The Council stated that the disclosure of information classified as secret should not be

---

[197] Statens Offentliga Utredningar 2014:31: 288.

[198] Transparency International Report (2013), "Whistleblowing in Europe. Legal Protections for whistleblowers in the EU", p. 85.

considered as a right, even if illegal practices of intelligence services are being reported. The Council only considers it acceptable to raise the issue with an administrative authority, i.e. using internal procedures.

In Spain, there is no overarching legislation to protect employees in the private and public sector from retaliation for exposing wrongdoing. Moreover, there are close to no labour or administrative codes in place to protect whistle-blowers, no palpable culture for employees or citizens to report wrongdoing, and no apparent momentum among political leaders to put in place legal protection for whistle-blowers.[199] In Germany, there is no dedicated legislation to protect whistle-blowers. A complex set of disparate laws and principles has been inconsistently interpreted by the courts, which makes it very difficult for whistle-blowers to predict outcomes. Additionally, under German law, employees who endeavour to expose wrongdoing can face not only dismissal without notice, but also civil liability or even criminal prosecution.[200]

At the EU level, in February 2014, the LIBE Committee rejected an amendment in defence of Snowden tabled to the Report on Mass Surveillance drawn up by Claude Moraes. A separate resolution, also defeated, called upon the US authorities to give amnesty to Snowden for initiating the process of rethinking the course of intelligence agencies.

This section aimed to show that cases in which national security is invoked not only question the balance of powers and the need for appropriate safeguards in judicial scrutiny over CMPs, but also compromise and jeopardise other fundamental rights, such as the freedom of the press, the protection of sources and the right to inform the public. Invoking national security also prevents important revelations of official wrongdoing and limits whistle-blowing laws. These aspects reinforce the need for adequate scrutiny of the executive, which is of critical importance in challenging the State's reasoning of the State where public interest may be undermined.

[199] Ibid., p. 81.

[200] Ibid., p. 43.

6. Conclusions and recommendations

6.1 General conclusions

The study has analysed the use of state secrets, national security and intelligence from the perspective of judicial accountability and its impact on the rights of the defence, the right to a fair trial and freedom of information and expression. A comparative assessment has been carried out looking at the legal regimes and interpretations by domestic and European tribunals. The study has also examined changing developments and contemporary practices, such as the rise of intelligence-led policing and large-scale data surveillance, with a focus on the compatibility of these legal and practical arrangements in the EUMS under investigation with the rule of law and fundamental rights. A key finding from the research is that **the invoking national security and state secrets and the introduction of intelligence information in trials require a careful assessment of compliance with the 'rule of law' foundations** upon which the EU has been built and currently operates. Our examination has revealed four **primary challenges**.

The **first challenge** relates to **the growing reliance on intelligence information and state secrets/national security claims in judicial proceedings** in a majority of EUMS under assessment. The UK (closed materials procedures, CMPs) and the Netherlands (Act on Shielded Witnesses) both have special procedures for the use of intelligence information as evidence in judicial proceedings on the statute books. The UK, however, constitutes an exception among the EUMS examined, as its expansive application of CMPs (see Section 1) demonstrate that it is at the forefront of intelligence-led policing and the logic of preventive law enforcement.

Secret information is not always legal evidence across the EU. Other EUMS covered by our study present different frameworks and experiences when it comes to the possibility of using intelligence information in judicial proceedings. These are closely linked to their respective constitutional, political and historical trajectories. In some EUMS, the constitution expressly forbids the use or framing of intelligence as 'closed evidence' before the courts, as this is considered an unacceptable interference with the rights of the defence, the principles of open justice and adversarial proceedings and the democratic rule of law. In countries such as Germany, Italy or Spain, the rights of the defence cannot be balanced with state interests or national security, as such an effort to balance the two would be unconstitutional. However, in some of these EUMS, national courts may still use classified intelligence information as evidence. In other EUMS, such as Italy and France, secret evidence cannot be used in trials, yet the challenges rather relate to the obstacles faced by judicial authorities in gaining access to materials classified by the executive as 'secret' in the name of national security and the substantial discretion enjoyed by the executive in determining classification (see Section 1).

A **second fundamental challenge** inherent to 'closed evidence' procedures and similar practices relates to **the lack of adequate and accessible legal standards in EUMS' legal systems and practices that would allow individuals to adapt their behaviour accordingly and to reasonably foresee the consequences which a given action may entail (see the foreseeability concept explored in Section 3)**. The systems also too often lack sufficient forms of legal protection and deny the party involved in the case knowledge of the very essence of the allegations against him/her and of the evidence to back up the allegations. Invoking national security therefore becomes an impediment making it impossible for the individual to challenge the executive's position or allegation, which leads in turn, in some of the EUMS under examination, to a breach of the right to a fair trial and the right of defence enshrined in the EU Charter of Fundamental Rights. Based on the expertise gathered in the Country Fiches in Annex 5, it emerges that **most EUMS systems thus fail to pass the "in accordance with the law" test**, developed by the ECtHR and the CJEU as one of the most important legal standards when evaluating the lawfulness of government interference with fundamental rights in the name of national security (see Section 3). Obscure laws, or laws allowing the use of secrecy, are therefore not laws, as they are not in line with European judicial standards.

Moreover, the **disparities among the heterogeneous systems of legal protection** in EUMS also mean that EU citizens and residents who are suspects in judicial proceedings are protected differently or to varying degrees across the EU. There is a patchwork of legal protection systems that challenge the basis upon which the EU Area of Freedom, Security and Justice (AFSJ) was founded and currently operates. There are, in other words, variable 'Areas of Justice' in the EU when it comes to the rights of defence of suspects where national security or state secrets are invoked. This patchwork is at odds with **the ambition of developing a**

***common* AFSJ and achieving non-discriminatory delivery of fundamental rights on the basis of the EU Charter of Fundamental Rights.**

The **third challenge** is **the lack of effective judicial scrutiny** over processes of classification and declassification of information as 'secret', as well the legitimacy of government claims related to national security and state secrets. Questions of independent and impartial judicial oversight are of central importance and an issue of concern across the EUMS under examination. State secrets too often 'over-protect' the executive from proper accountability and oversight in cases of wrongdoing and fundamental rights interferences. Some EUMS' judicial authorities often trust the legitimacy of States' claims of national security and the lawfulness of the intelligence information provided in judicial proceedings. The same judicial authorities often pursue a deferential or minimal oversight approach to government decisions regarding classification/declassification of information and attempts to present intelligence as evidence and are too readily accepting the state secrets narrative, which curbs proper judicial oversight. The reliance on intelligence materials is thus too often based on a presumption that governmental agencies are acting in good faith (see Section 2). As the European Parliament has rightly pointed out, however, the Snowden revelations have led to a 'crisis of confidence', which extends to the "respect for fundamental rights, democracy and the rule of law, as well as the credibility of democratic, judicial and parliamentary safeguards and oversight in a digital society".[201] Indeed, the 2013 Snowden revelations and the increasing number of cases revealing unlawful practices by secret services and governments demonstrate the need for a more careful assessment by judicial authorities.

This need for proper judicial oversight is all the more apparent given the **nebulous, fuzzy way in which the concept of national security is used.** The research outlined in this study shows that national security is an obscure notion encompassing several policy areas and somewhat different meanings across EUMS (see Section 1 and Annex 3). There is not a commonly agreed definition of national security that meets the requirement of legal certainty. The few definitional features that have been identified in this study make it possible for the executive to act arbitrarily and with unfettered power and therefore open up possibilities for further abuses and fundamental rights violations. The blurriness characterising the concept of national security, and the challenges that this poses to effective legal and judicial scrutiny, are further jeopardised in the context of transnational intelligence exchanges, where there is a system of mutual respect for protected secrets. The central role of NATO and of bilateral exchange of information agreements clearly creates tension between the secrecy obligations entered into by the parties to such agreements on the one hand and the requirements of EU Law on the other.

The **fourth challenge** emerges when looking at how state secrets are invoked and how this process interferes with **freedom of expression and information, as well as the protection of the source**. As we have seen in Section 4, EUMS' regimes differ considerably as regards the level of protection granted to journalists' sources, with some legal restrictions severely compromising the confidentiality of these sources. The level of protection afforded to whistle-blowers is also rather heterogeneous and fragmented across the EUMS analysed in this study. Where specific legislative frameworks protecting whistle-blowers do exist in EUMS, they are negatively affected by substantial restrictions in the level of protection in national security cases. In other EUMS there are substantial protection gaps for persons who witness mismanagement, corruption, illegality or wrongdoing.

All these challenges constitute significant barriers to the ability of the judiciary, in a context of 'democratic rule of law with fundamental rights', to properly and effectively adjudicate justice and guarantee the rights of the defence (right to a fair trial and to an effective remedy) as enshrined in national constitutional traditions, the ECHR and the EU Charter of Fundamental Rights. They also sit uneasily with 'rule of law' principles and standards, which, as the European Commission has rightly highlighted, include "legality, which implies a transparent, accountable, democratic and pluralistic process for enacting laws; legal certainty; prohibition of arbitrariness of the executive powers, independent and impartial courts; effective judicial review including respect for fundamental rights and equality before the

[201] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), paragraphs 111-112.

law".[202] More knowledge is needed as regards the various ways in which Member States' regimes and practices protect from disclosure information communicated in confidence in lawyer-client relations and the existence and applicability of European judiciary principles in Strasbourg and Luxembourg, in particular their impact on access to legal advice and to justice and the right to a fair trial.

In view of all the challenges posed by the use of intelligence materials and information in courts in the EUMS examined in this study, there is a clear **risk that an approach in terms of practical arrangements prevails.** Instead, the aim should be to seek the effective implementation of new instruments led by the spirit of the Lisbon Treaty and designed to consolidate fundamental rights and the rule of law in the EU. The newly proposed EU Rule of Law Mechanism is a case in point and could improve democratic 'rule of law' principles and respect for fundamental rights across the Union, without interfering with Member States' national sovereignty.[203] The recommendations outlined hereafter seek to address this risk and to ensure that a "Lisbon" approach prevails.

6.2 Policy recommendations

Recommendation 1: The new EU Framework to strengthen the rule of law should be used to encourage concerned EUMS to modify their current legislation on the use of national security, state secrets and intelligence information in judicial proceedings

The growing reliance of certain Member States on the use of secret evidence in courts raises a number of significant challenges concerning judicial scrutiny, as well as the protection of fundamental rights envisaged by the EU Charter of Fundamental Rights (right to a fair trial and to an effective remedy and the rights of the defence). Significant challenges also arise for freedom of information and expression. Current legal regimes and practices in the seven EUMS under investigation sit uneasily with the legal standards developed by the European Court of Human Rights and the Court of Justice of the European Union, in particular when it comes to the "in accordance with the law" test, the lawfulness/legitimacy of the information gathered, and the lack of effective/independent judicial review.

The European Parliament should call on the European Commission to carefully study the current situation and not to shy away from using the new early warning tool for systemic threats to the rule of law, the EU Rule of Law Framework established in March 2014,[204] to prevent the practices highlighted in this study from threatening the Union's values and legal principles. As rightly clarified by the European Commission, the scope of application of the Article 7 TEU procedure is not limited to Member States' actions when implementing EU law. It could also be triggered in the event of a breach in areas where Member States act autonomously.[205] Moreover, while EUMS enjoy considerable discretion in determining national security questions, the notion of national security is now an autonomous legal concept in the EU legal system, the interpretation and lawful use of which is ultimately determined by judicial authorities both at national and European level. This is particularly the case in areas where there is already EU secondary legislation providing for a national security exception from EU rights and freedoms.[206]

---

[202] Commission Communication, "A New EU Framework to Strengthen the Rule of Law", COM(2014) 158 final/2, Brussels, 19.3.2014.

[203] Carrera, Guild and Hernanz, op. cit.

[204] See the Commission's Communication on "A new EU Framework to strengthen the Rule of Law", COM(2014) 158 final/2, 11 March 2014.

[205] In particular, the European Commission highlighted in its Communication on Article 7 of the Treaty on European Union "the fact that Article 7 of the Union Treaty is horizontal and general in scope is quite understandable in the case of an article that seeks to secure respect for the conditions of Union membership. *There would be something paradoxical about confining the Union's possibilities of action to the areas covered by Union law and asking it to ignore serious breaches in areas of national jurisdiction.* If a Member State breaches the fundamental values in a manner sufficiently serious to be caught by Article 7, this is likely to undermine *the very foundations of the Union and the trust between its members*, *whatever the field in which the breach occurs"* (emphasis added). For specific recommendations as to how to improve the current operability of Article 7 TEU refer to Carrera, Guild and Hernanz, op. cit.

[206] Refer for instance to Recital 34 of the Directive on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, 22 October 2013, which states

The European Parliament should insist that EUMS – where intelligence derived from large-scale surveillance and secret evidence are used in judicial proceedings and formally provided for by the law, and where the rights of the defence are therefore systematically at risk – are called upon to put in place the necessary national reforms in order to fully ensure the respect of the rights of the defence under Articles 47 and 48 of the EU Charter as interpreted by the CJEU. The European Parliament should also call on those Member States where secrecy rules or 'state secrets' prevent judicial authorities from accessing evidence to reform the systems in place and allow declassification of intelligence materials in order for justice to be delivered in accordance with European judicial and legal standards and principles.

Finally, the European Parliament should insist that the new Rules of Procedure of the General Court in Luxembourg must not provide for the use of secret information unless the essential content of that information is communicated and the other main party to the case is able to make its views known. The new Rules of Procedure should fully and consistently follow CJEU jurisprudence according to which it is necessary for European judges to have full access to that information and for the evidence against an individual that is available to the judicial authority to be disclosed to him/her. Only in this way can the rights of the defence laid down in the Charter and the Union's constitutional guarantees be safeguarded.

Recommendation 2: A professional code for the transnational management and accountability of data in the EU: 'What national security is not'

The European Parliament should call for an inter-institutional EU Code for the Transnational Management and Accountability of Information in the EU addressed to the intelligence communities in the Member States. Such a code could aim at ensuring that the practices of intelligence services are in accordance with fundamental rights and 'rule of law' principles without undermining their work. This code should cover the full range of activities carried out by intelligence services and authorities: signals intelligence' collection, information gathering within the State and exchange of information with other States.

The code would lay down European judiciary standards and judge-made principles emerging from the application of the ECHR and the EU Charter of Fundamental Rights to judicial scrutiny of EUMS' actions in the name of national security and state secrets. Particular attention should be paid to the relevance and application of the "in accordance with the law" test, the "necessary in a democratic society" test and principles related to independent judicial review and effective remedies. The code would outline EU guidelines for invoking national security and secrecy in the EU. **It would also present the basis on which national security should not be invoked**, such as personal interests, official wrongdoing, poor quality of the law, interference with freedom of expression and information, and absence of sufficient and effective judicial controls. **In order to promote ethical principles and practices, such a code could be officially signed by law enforcement officers and authorities involved in intelligence gathering**.

The supranational standards identified in this study should hence become an integral part of defining the 'red lines' that intelligence services in democratic systems cannot cross in the name of national security. Effective judicial control, the "in accordance with the law" test and the need to disclose information for it to be regarded as 'evidence' should constitute three central principles of the code. **The independence of the bodies in charge of scrutinising materials provided by intelligence communities should be reinforced in EUMS and included in EU standards.** In delimiting the legitimate parameters of national security claims and making sure they are not used as a cover-up for unlawful practices, independent oversight mechanisms are an absolute requirement to restrain the discretionary powers given to the executive and to the alliance of intelligence services at the European/transnational level.

The code should also provide more legal certainty concerning the kind of information that is exchanged, the parameters for it to be considered as 'intelligence', and a common legal definition of 'law enforcement authorities'. As previously proposed, a 'yellow card, red card system' could be adopted, in which

---

that "this Directive should be without prejudice to a breach of confidentiality which is incidental to a lawful surveillance operation by competent authorities. This Directive should also be without prejudice to the work that is carried out, for example, by national intelligence services to safeguard national security in accordance with Article 4(2) of the Treaty on European Union (TEU) or that falls within the scope of Article 72 TFEU, pursuant to which Title V on an area of Freedom, Security and Justice must not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security."

transmission of tainted information in breach of the common accord would first be signalled by a warning ('yellow card') and, if repeated, would entail exclusion ('red card') from the information-sharing network.[207]

In terms of content, Sir David Omand (former director of GCHQ) recommended some 'promising practices' that could be implemented in order to bring intelligence services closer to democratic rules. They include:[208]

- **There must be sufficient sustainable cause.** Any tendency for intelligence services to encroach on areas unjustified by the scale of potential harm to national interests has to be checked.
- **There must be integrity of motive.** No hidden agendas: the integrity of the whole system throughout the intelligence process must be assured, from collection to analysis and presentation.
- **The methods used must be proportionate.** Their likely impact must be proportionate to the harm whose prevention is being sought, for example, by using only the minimum intrusion necessary into the private affairs of others. The proportionality principle should be qualified by 'within the framework of human rights', thus, for example, excluding torture even when some might consider that to be proportionate to an imminent threat.
- **There must be right and lawful authority.** There must be the right level of sign-off on sensitive operations, with accountability up a recognised chain of command to permit effective oversight.
- **There must be a reasonable prospect of success.** All intelligence operations need careful risk management, and before approval is given there has to be consideration of the likelihood of unintended consequences and the impact if the operation were to be exposed or otherwise go wrong
- **Recourse to secret intelligence must be a last resort.** There should be no reasonable alternative way of acquiring the information by non-secret methods.

Recommendation 3: The EU should strengthen the mainstreaming of supranational human rights and 'rule of law' standards

The EU should establish a strategic partnership with relevant supranational actors engaged in fundamental rights, the rule of law and security in times of mass surveillance and a digital economy. The EU should not only become a more active promoter of these supranational principles and legal standards, but also contribute towards ensuring that EUMS' authorities effectively implement them in light of their obligations under the Treaties and European law. The European Parliament should play an active role of mediation between national parliaments and legal and judicial scrutiny mechanisms in the EU, as well as in other regional and international organisations such as the Council of Europe and the UN. The new Vice-President of the European Commission in charge of Better Regulation, Inter-Institutional Relations, the Rule of Law and the Charter of Fundamental Rights, Frans Timmermans, should follow up on his promises of completing the EU's accession to the ECHR and of further strengthening links with the Council of Europe.[209]

Recommendation 4: Establishing an 'Observatory' to monitor the way in which national security and state secrets are invoked

This study has demonstrated that a number of EUMS use national security and state secrets claims in judicial proceedings to limit accountability for their own wrongdoing or that of intelligence services. The

---

[207] F. Geyer (2007), "Fruit of the Poisonous Tree – Member States' Indirect Use of Extraordinary Rendition and the EU Counter-Terrorism Strategy", Centre for European Policy Studies, 3 April; Bigo, D. (2006), Intelligence Services, Police and Democratic Control: The European and Transatlantic Collaboration. In *Controlling Security*, edited by Didier Bigo and Anastassia Tsoukala, pp. 163-82. Paris: Centre d'Etudes sur les Conflits/L'Harmattan This was already recommended in Carrera et al. (2012), "The results of inquiries into the CIA's programme of extraordinary rendition…" *op. cit.*.

[208] D. Omand (2010), *Securing the State*, London: Hurst, pp. 286-287.

[209] See the answers of Mr Timmermans to the European Parliament's questionnaire in view of his hearing, 7 October 2014, available at http://ec.europa.eu/about/juncker-commission/docs/2014-ep-hearings-reply-timmermans_en.pdf.

justification for using secrecy is often based on the argument of 'national security' or 'state secrets', which entails a limitation of democratic oversight by national parliaments in Member States. There is, however, not a commonly agreed definition meeting 'legal certainty' and 'rule of law' criteria across the EUMS under examination. The European Parliament should therefore launch the idea of establishing an 'EU Observatory' mapping the changing notions of 'national security' across EUMS and following the way in which governments invoke state secrets and courts interpret these arguments. In addition to the professional code outlined in Recommendation 2, the 'Observatory' would facilitate a better understanding of when the 'national security' justification should not be used. The 'Observatory' would consist of a constantly updated database covering all 28 EU Member States and should be subject to independent academic analysis.

Recommendation 5: Adopting an EU framework for the protection of whistle-blowers

The European Parliament Resolution of 12 March 2014[210] proposed the adoption of "A European Digital Habeas Corpus – protecting fundamental rights in a digital age", which among other priorities or actions would:

> Protect the rule of law and the fundamental rights of EU citizens (including from threats to the freedom of the press), the right of the public to receive impartial information and professional confidentiality (including lawyer-client relations), as well as ensuring enhanced protection for whistleblowers.[211]

The European Parliament should follow up this call to develop a systematic protection mechanism for whistle-blowers in an EU legal framework, potentially including strong guarantees of immunity and asylum, and covering cases related to national security.[212]

[210] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)).

[211] Ibid., p. 42.

[212] As proposed in Bigo et al., op. cit.

References

Aldrich, Richard J. (2009), "Global Intelligence Co-operation versus Accountability: New Facets to an Old Problem", Intelligence and National Security, 24:1, pp. 26-56.

Amnesty International (2014), "UK government accused of 'scraping legal barrel' in Belhaj rendition case", 21 July, Press release.

Avbelj, M., F. Fontanelli, and G. Martinico (2014), Kadi on Trial: A Multifaceted Analysis of the Kadi Trial, London: Routledge.

Bigo, D., S. Carrera, N. Hernanz, J. Jeandesboz, J. Parkin, F. Ragazzi and A. Scherrer (2013), "National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law", study for the European Parliament, PE 493.032, November.

Bigo, D. (2013) The Transnational Field of Computerised Exchange of Information in Police Matters and Its European Guilds. In *Transnational Power Elites: The New Professionals of Governance, Law and Security*, p. 155: Niilo Kauppi, Mikael Madsen.

Bigo, D. (2006), Intelligence Services, Police and Democratic Control: The European and Transatlantic Collaboration. In *Controlling Security*, edited by Didier Bigo and Anastassia Tsoukala, pp. 163-82. Paris: Centre d'Etudes sur les Conflits/L'Harmattan.

Bigo, D. (1994), "The European internal security field: stakes and rivalries in a newly developing area of police intervention", in M. Anderson and M. den Boer (eds), Policing Across National Boundaries, Pinter, 161-173.

Brodeur, J.P. and N. Dupeyron (2003), "Democracy and Secrecy: The French Intelligence Community", in J.P. Brodeur, P. Gill and D. Töllborg (eds), Democracy, Law and Security, Aldershot: Ashgate.

Cameron, I. (2005), "Beyond the Nation State: The Influence of the European Court of Human Rights on Intelligence Accountability", in H. Born, L.K. Johnson and I. Leigh (eds), Who's Watching the Spies? Establishing Intelligence Accountability, Dulles, VA: Potomatic Books, Inc.

Carrera, S. et al. (2012), "The Results of Inquiries into the CIA Programme of Extraordinary Renditions and Secret Prisons in European States in light of the New Legal Framework following the Lisbon Treaty", European Parliament study, Brussels.

Carrera, S., E. Guild and N. Hernanz (2013), "The Triangular Relationship between Fundamental Rights, Democracy and Rule of Law: Towards an EU Copenhagen Mechanism", European Parliament DG IPOL, Brussels.

Charles Louis de Secondat, Baron de Montesquieu, Complete Works, vol. 1 (The Spirit of Laws) [1748].

Coster van Voorhout, J. (2007), "Intelligence as Legal Evidence: Comparative Criminal Research into the Viability of the Proposed Dutch Scheme of Shielded Intelligence Witnesses in England and Wales, and Legislative Compliance with Article 6 (3) (d) ECHR", Utrecht Law Review, 2, 2, p. 129.

Danisi, C. (2011), "State Secrets, Impunity and Human Rights Violations: Restriction of Evidence in the Abu Omar Case", Essex Human Rights Review 8, 1, October.

De Búrca, G. (2010), "The European Court of Justice and the International Legal Order After Kadi", Harvard International Law Journal, Vol. 51, Number 1, pp. 1-49.

Dintilhac, J.P. (2003), "L'égalité des armes dans les enceintes judiciaires", Annual Report of the Cour de Cassation.

European Court of Human Rights (2013), "National Security and European case-law", Division de la Recherche/Research Division, Council of Europe.

European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)).

Eijkman, Q., D. Lettinga and G. Verbossen (2012), "Impact of Counter-Terrorism on Communities: Netherlands Background Report", Open Society Foundations, Institute of Strategic Dialogue.

Geyer, F. (2007), "Fruit of the Poisonous Tree - Member States' Indirect Use of Extraordinary Rendition and the EU Counter-Terrorism Strategy", Centre for European Policy Studies, 3 April.

Gill, P. (2000), Rounding up the usual suspects: developments in contemporary law enforcement intelligence, Aldershot, Hants, England; Burlington, VT: Ashgate.

Gill, P. (2012), "Intelligence, Threat, Risk and the Challenge of Oversight", Intelligence and National Security, 27:2, pp. 206-220.

Giménez-Salinas, A. (2003), "The Spanish Intelligence Services", in J.P. Brodeur, P. Gill and D. Töllborg (eds), Democracy, Law and Security, Aldershot: Ashgate, p. 76.

Goede, M. and B. de Graaf (2013), "Sentencing Risk: Temporality and Precaution in Terrorism Trials", International Political Sociology, 7(3), 313-331.

Guild, E. (2010), "EU Counter-Terrorism Action: A Fault Line between Law and Politics", CEPS Liberty and Security in Europe Series, Brussels.

Hickman, T. (2013), "Turning out the lights? The Justice and Security Act 2013", UK Const. L. Blog, 11 June.

House of Lords and House of Commons Counter-Terrorism Policy and Human Rights (2010), Annual Renewal of Control Orders Legislation 2010 (Sixteenth Report) - Human Rights Joint Committee, HL 64/HC 395, p. 21.

Innes, M. and J. Sheptycki (2004), "From detection to disruption: intelligence and the changing logic of police control", International Criminal Justice Review, Volume 14.

Jackson, J. (2013), "Justice, Security and the Right to a Fair Trial: Is the Use of Secret Evidence Ever Fair?", Public Law, 720-736.

Jeandesboz, J., E-P. Guittet and A. Scherrer (2011), "Developing an EU Internal Security Strategy, fighting terrorism and organised crime", Report for the LIBE Committee.

JUSTICE (2014), "NGOs urge Court of Appeal to preserve access to justice in torture claims", 2 July.

Kokott, J. and C. Sobotta (2012), "The Kadi Case – Constitutional Core Values and International Law – Finding the Balance?", The European Journal of International Law, 23, 4, 1015-1024.

Lippmann, W. (1943), U.S. Foreign Policy: Shield of the Republic. Boston: Little.

Lustgarten, L. (2003), "National Security and Political Policing: Some thoughts on values, ends and law", in J.P. Brodeur, P. Gill and D. Töllborg (eds), Democracy, Law and Security, Aldershot: Ashgate.

Lynch, A., T. Tulich and R. Welsh (2014), "Secrecy and Control Orders: The role and vulnerability of constitutional values in the United Kingdom and Australia", in D. Cole, F. Fabbrini and A. Vedaschi, Secrecy, National Security and the Vindication of Constitutional Law, Cheltenham: Edward Elgar.

Messineo, F. (2009), "'Extraordinary Renditions' and State Obligations to Criminalize and Prosecute Torture in the Light of the Abu Omar Case in Italy", Journal of International Criminal Justice 7, 5, 1023-1044.

Miller, R. A. (2010), "Balancing Security and Liberty in Germany", Journal of National Security Law & Policy, Vol. 4, p. 369.

Murphy, C. (2014), "Secret Evidence in EU Security Law: Special Advocates before the Court of Justice?", in D. Cole, F. Fabbrini and A. Vedaschi (eds), Secrecy, National Security and the Vindication of Constitutional Law, Cheltenham: Edward Elgar, 1-9.

Omand, D. (2010), Securing the State, London: Hurst.

Parliamentary Assembly of the Council of Europe (2010), Resolution 1723 on the Protection of whistle-blowers.

Pech, L. (2014), "Article 47, right to an effective remedy", in S. Peers, T. Hervey, J. Kenner and A. Ward (eds), The EU Charter of Fundamental Rights: A Commentary, Oxford: Hart Publishing, pp. 1250-1258.

Poli, S. and M. Tzanou (2009), "The Kadi Rulings: A Survey of the Literature", Yearbook of European Law 28 (1), 533-558.

Report on the Democratic oversight of the security services, adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007).

Roach, K. (2010), "The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations", in N. McGarrity, A. Lynch and G. Williams (eds), Counter-Terrorism and Beyond, Routledge, pp. 48-68.

Shelton, D. (2014), "Article 47, right to an effective remedy", in S. Peers, T. Hervey, J. Kenner and A. Ward (eds), The EU Charter of Fundamental Rights: A Commentary, Oxford: Hart Publishing.

Transparency International Report (2013), "Whistleblowing in Europe. Legal Protections for whistleblowers in the EU"

Türküler Isiksel, N. (2010), "Fundamental Rights in the EU after Kadi and Al Barakaat", European Law Journal, Volume 16, Issue 5, pages 551–577.

Van der Hof, S., E. J. Koops and R. E. Leenes (2009), "Anonymity and the Law in the Netherlands", in V. Steeves, C. Lucock and I. Kerr (eds), Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, New York: Oxford University Press.

Vashakmadze, M. (2014), "Secrecy vs. Openness: Counterterrorism and the role of the German Federal Constitutional Court", in D. Cole, F. Fabbrini and A. Vedaschi (eds), Secrecy, National Security and the Vindication of Constitutional Law, Cheltenham: Edward Elgar, pp. 44-56.

Vatter, M. (2008), "The Idea of Public Reason and the Reason of State. Schmitt and Rawls on the Political", Political Theory 36:239-71.

Vedaschi, A. (2013), "Arcana Imperii and Salus Rei Publicae: state secrets privilege and the Italian legal framework", in D. Cole, F. Fabbrini and A. Vedaschi (eds), Secrecy, National Security and the Vindication of Constitutional Law, Cheltenham: Edward Elgar Publishing.

Wills, A. and M. Vermeulen (2011), "Parliamentary Oversight of Security and Intelligence Agencies in The European Union", European Parliament.

List of Annexes

Annex 1. European and National Case-Law

Selected national case-law where intelligence materials have been used in judicial proceedings or where State secrets have been invoked

United Kingdom:

- Regina (Noor Khan) v. Secretary of State for Foreign and Commonwealth Affairs [2014] EWCA Civ 24; [2014] WLR (D) 14.
- Mastafa v. HM Treasury [2013] 1 WLR 1621.
- Secretary of State for the Home Department v. BM [2012] 1 WLR 2734.
- AF(no 3) v. Secretary of State for the Home Department [2010] 2 AC 269.

France:

- The "Karachi Affair", a case which cannot be solved due to a refusal by the French government to disclose secret evidence to judges (see Section 2.3).

Germany:

- Bundesverfassungsgericht, 27.10.1999, 1 BvR 385/90.
- Bundesverfassungsgericht, 26.5.1981, 2 BvR 215/81.

Italy:

The Abu Omar case:

- Trib. pen di Milano, judgment 535/2009.
- Italian Constitutional Court, judgment 106/2009.
- Corte App., sez. III pen., judgment 3688/2010.
- Cass., sez. V pen., judgment 46340/2012.
- Corte App., sez. IV pen., judgment 985/2013.
- Cass., sez. I pen., judgment 20447/2014.

Spain:

- Tribunal Supremo Sala 2ª, S 27-6-2014, nº 534/2014, rec. 11138/2013.
- Tribunal Supremo Sala 2ª, S 28-5-2014, nº 426/2014, rec. 10742/2013.
- Audiencia Nacional Sala de lo Penal, sec. 2ª, S 25-4-2014, nº 6/2014, rec. 6/2013.
- Tribunal Supremo Sala 2ª, S 23-1-2014, nº 9/2014, rec. 576/2013.
- Tribunal Supremo Sala 2ª, S 28-3-2012, nº 263/2012, rec. 2235/2011.
- Tribunal Supremo Sala 2ª, S 25-10-2011, nº 1097/2011, rec. 10344/2011.
- Tribunal Supremo Sala 2ª, S 10-12-2010, nº 1094/2010, rec. 10251/2010.
- Audiencia Provincial de Madrid, sec. 1ª, S 11-2-2010, nº 61/2010, rec. 36/2009.
- Audiencia Provincial de Madrid, sec. 4ª, S 12-3-2010, nº 36/2010, rec. 64/2008.
- Audiencia Nacional Sala de lo Penal, sec. 2ª, S 27-5-2009, nº 39/2009, rec. 94/2005.
- Tribunal Supremo Sala 2ª, S 13-12-2001, nº 2084/2001.
- Audiencia Nacional Sala de lo Penal, sec. 2ª, S 23-9-2008, nº 37/2008, rec. 44/1998.

The Netherlands:

All judgments related to the Piranha case (2006 – ongoing):

- LJN: AZ3589, Rotterdam District Court, 10/600052-05, 10/600108-05, 10/600134-05, 10/600109-05, 10/600122-05, 10/600023-06, 10/600100-06, 1 December 2006.
- LJN: BF3987, The Hague Court of Appeal, no.2200734906, 2 October 2008.
- LJN: BF5225, The Hague Court of Appeal, no.2200735006, 2 October 2008.
- LJN: BF4814, The Hague Court of Appeal, no.2200735106, 2 October 2008.
- LJN: BF5180, The Hague Court of Appeal, no.2200738406, 2 October 2008.

ECtHR cases on national security, fair trial and effective remedies

- Abu Zubaydah v. Poland, Application no. 7511/13 of 24 July 2014.
- Al Nashiri v. Poland, Application No. 28761/11 of 24 July 2014.
- Bucur and Toma v. Romania, no. 40238/02, 8 January 2013.
- El-Masri v. Former Yugoslav Republic of Macedonia, Application No. 39630/09, 13 December 2012.
- Telegraaf Media and others v. The Netherlands, Application no. 39315/06, 22 November 2012.
- Leas v. Estonia, no. 59577/08, 6 March 2012.
- Kennedy v. United Kingdom, no. 26839/05, 18 May 2010.
- Uzun v. Germany, no. 35623/05, ECHR 2010.
- A and other v. United Kingdom (2009) Application no. 3455/05.
- Iordachi and Others v. Moldova, no. 25198/02, 10 February 2009.
- Liberty and Others v. United Kingdom, no. 58243/00, 1 July 2008.
- Weber and Saravia v. Germany, no. 54934/00, ECHR 2006-XI.
- Rotaru v. Romania, no. 28341/95, ECHR 2000-V.
- Amann v. Switzerland, no. 27798/95, ECHR 2000-II.
- Fitt v. United Kingdom, no. 29777/96, 16 February 2000.
- Jasper v. United Kingdom, no. 28901/95, 16 February 2000.
- Gautrin and Others v. France ECHR 1998-III [58].
- Van Mechelen and Others v. The Netherlands, nos. 21363/93, 21364/93, 21427/93 and 22056/93, 23 April 1997.
- Chahal v. United Kingdom (1996) 23 EHRR 413.
- Doorson v. The Netherlands, 26 March 1996, Reports 1996-II.
- Kruslin v. France, no. 11801/85, 24 April 1990.
- Huvig v. France, no. 11105/84, 24 April 1990.
- Sramek v. Austria, (1984) ECHR Series A no. 84.
- Malone v. United Kingdom, 2 August 1984, Series A no. 82.
- Le Compte et al. v. Belgium (1981) ECHR Series A no. 43.
- Klass and Others v. Germany, 6 September 1978, Series A no. 28.

See also http://echr-online.blogspot.be/2014/02/prism-and-tempora-before-european-court.html

CJEU and General Court cases

- Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, Commission and Others v. Kadi, 18 July 2013.
- C-300/11 ZZ v. Secretary of the State of Home Department, 4 June 2013.
- Case C-27/09 P French Republic v. People's Mojahedin Organization of Iran (PMOI), of 21 December 2011.
- Case T-85/09, Kadi v. European Commission, 30 September 2010.
- Case C-387/05 Commission v. Italy [2009] ECR I-11831.
- Joined Cases C-402/05 P and C-415/05 P Kadi and Al Barakaat International Foundation v. Council and Commission [2008] ECR I-6351.
- Case C-506/04 Wilson [2006].
- Case C-54/96 Dorsch Consult [1997].
- Case C-111/94 Job Centre [1995] ECR I-3361.
- Case C-393/92 Almelo and Others [1994] ECR I-1477.
- Case C-24/92 Corbiau [1993] ECR I-1277.
- Case 109/88 Danfoss [1989] ECR 3199.
- Case 14/86 Pretore di Salò v. Persons unknown [1987] ECR 2545.
- Case 222/84 Johnston [1986] ECR 1651.
- C-294/83 Les Verts v. European Parliament, 23 April 1986.
- Case 61/65 Vaassen (neé Göbbels) [1966] ECR 261.

Annex 2. Relevant Fundamental and Human Rights Provisions: the ECHR and the EU Charter

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)

Article 6 (Right to a Fair Trial)

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

3. Everyone charged with a criminal offence has the following minimum rights:

(a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;

(b) to have adequate time and facilities for the preparation of his defence;

(c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;

(d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

(e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

Article 13 (Right to an Effective Remedy)

Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

Charter of Fundamental Rights of the European Union (EU Charter of Fundamental Rights)

Article 47 (Right to an Effective Remedy and to a Fair Trial)

1. Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.

2. Everyone is entitled to a fair trial and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.

3. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

Article 48 (Presumption of Innocence and Right of Defence)

1. Everyone who has been charged shall be presumed innocent until proved guilty according to law.

2. Respect for the rights of the defence of anyone who has been charged shall be guaranteed

.

Annex 3. Conceptual features of national security in selected EU Member States

The following table outlines the main findings as regards the different concepts used in the Member States examined in Section 1.6 above.

Member State	Term used	Conceptual features
United Kingdom	National security	"The security of the United Kingdom and its people".[213]
France	"*Secret défense*" and national security	"The protection of secrecy concerns all fields of activity related to defence and national security: political, military, diplomatic, scientific, economic, industrial fields".[214]
Germany	Interests of the Federation or of a Land	"…disadvantageous to the interests of the Federation or of a Land".[215]
Spain	Security and defence of the State	"The independence or territorial integrity of Spain, national interests and the stability of the rule of law and its institutions".[216]
Italy	Security of the Republic	"The integrity of the Republic (including in relation to international agreements, the defence of its underlying institutions as established by the Constitution, the State's independence vis-à-vis other states and its relations with them, as well as its military preparation and defence)".[217]
Netherlands	National security	"National security is at stake when one or more of the country's and/or society's vital interests are threatened to such an extent that potential societal disruption could occur".[218]
Sweden	National security	"1. national security or Sweden's relations with a foreign state or an international organisation; 2. the central financial policy, the monetary policy, or the national foreign exchange policy; 3. the inspection, control or other supervisory activities of a public authority; 4. the interest of preventing or prosecuting crime; 5. the public economic interest; 6. the protection of the personal or economic circumstances of private subjects; or 7. the preservation of animal or plant species."[219]

[213] *SSHD v. Rehman* [2003] 1 AC 153, paragraphs 16, 17 and 50.

[214] "Arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale", Titre Ier.

[215] Section 99(1) of the Code of Administrative Court Procedure (English translation may be found at www.gesetze-im-internet.de/englisch_vwgo/englisch_vwgo.html).

[216] Art. 1 Law 11/2002, 6 May 2002, on regulation of the National Centre of Intelligence (CNI).

[217] Article 39.1 of Law 124/2007, available in English at www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html.

[218] 2007 National Security Strategy (*Strategie Nationale Veiligheid*), available at www.nctv.nl/onderwerpen/nv/strategie-nationale-veiligheid.

[219] See Regeringskansliet (2009) Public Access to Information and Secrecy Act: Information concerning public access to information and secrecy legislation, etc., available in English at www.government.se/content/1/c6/13/13/97/aa5c1d4c.pdf.

Annex 4. Proceedings report of the 30 October Focus Groups

European Parliament study on
"National Security Exceptions and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges"

National Experts Focus Group: 30 October 2014, 10.00 – 12.00

Civil Society Focus Group: 30 October 2014, 14.00 – 15.30

Practitioners Focus Group: 30 October 2014, 16.30 – 18.30

The study on "National Security Exceptions and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges", commissioned by the European Parliament, is based on a methodological approach involving intense cooperation and consultation with a network of national scholars/experts that has been set up in each of the seven Member States under examination (United Kingdom, France, Germany, Italy, the Netherlands, Sweden and Spain). Each national expert has elaborated a Country Fiche on the basis of the results contained in questionnaires which were filled in by academics, practitioners and civil society actors who are all experts in their respective countries. This approach ensures the independence of the analysis provided in the Country Fiches. A specific focus group was set up on 30 October 2014 in Brussels, on the premises of the Centre for European Policy Studies (CEPS), in order to gather the inputs and comments of these national experts on the first full draft of the study.

In addition, representatives from civil society organisations and practitioners/policy-makers were invited to join two focus groups in Brussels also on 30 October 2014. The civil society focus group gathered experts working in the fields of access to justice, human rights and digital rights (Center for Democracy and Technology, Privacy International, Justice, Fair Trials Europe, International Modern Media Institute, Amnesty International), who have been active in the debates over the use of closed material procedures and intelligence information in courts as well as counterterrorism. The practitioners' focus group gathered participants from the private sector, legal practitioners (from Spain and the UK), public officials (EDPS, FRA, DG Justice) and former law enforcement and intelligence practitioners with expertise on these topics. All experts in both focus groups were asked to present their work on the topic of the study and to provide comments on a draft outline.

This Proceedings Report presents **the main issues and comments raised during the three focus groups**. Given that the meetings were organised under the Chatham House rule, no statement shall be attributed to a specific participant.

Key issues discussed

1. The definition of national security

National security was a key concept discussed throughout the focus groups. Participants agreed that there was no clear definition of national security in the EU Member States despite the growing reliance on this concept by governments to keep certain evidence secret in trials. The participants suggested that national security should not include the national security of a third country, and underlined that this was the main conclusion of two opinions by the EDPS and the A29WP.[220] Experts also highlighted that the reliance on national security for limiting certain rights had to be necessary and for clearly defined purposes ("in accordance with the law" test). It was pointed out that it would be very difficult to propose a common EU definition of national security given that Member States use different terminology such as "state interests", "state privilege" or "*secret défense*" in French. Instead, participants considered that it would be wiser to propose a definition of what national 'should not be'. For instance, national security should never be invoked when a criminal act has been committed.

2. The question of the constitutionality of closed material procedures

In countries like Germany, Italy and Spain, the introduction of closed material procedures would be considered as unconstitutional. National experts from these countries confirmed that the rights of the defence and the right to a fair trial cannot be balanced against national security. Article 103 of the German constitution prevents the balancing of the rights of the defendant with the national security argument. The use of closed material procedures in Spain would also be made anti-constitutional by Article 24 of the Spanish Constitution. Similarly, in Italy CMPs would be contrary to Articles 24 and 111 of the Italian Constitution.

3. The case of the United Kingdom as an exception in the European landscape

The use of CMPs in the UK is the only case among the examined Member States in which the non-disclosure of sensitive material in court for national security reasons is foreseen in national legislation and practised by the courts. The participants highlighted that the debates surrounding the use of CMPs are therefore very UK-focused. The European Court of Human Rights held that the use of CMPs and special advocates in the UK did not automatically lead to unfair processes, but that each case needed to be examined individually; the Strasbourg Court has set clear standards and conditions for these to be considered compliant with the "in accordance with the law" test.[221] The question of the special advocates was also tackled as a problematic issue: while the system in place might have advantages, it does not work at a practical level due to special advocates not being in possession of the appropriate materials. The opinion of the CJEU's Advocate-General Sharpston was mentioned during the discussions as being cautious regarding special advocates.[222] Similarly, a number of experts noted that while the standards set by the ECtHR in Strasbourg have positively influenced the human rights legislation in the UK, this does not necessarily mean that those standards continue to be respected in daily practices or on the ground especially in terms of the effectively delivery of the "equality of arms" and "in accordance with the law" argument.

---

[220] See the 20 February 2014 Opinion of the European Data Protection Supervisor (available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-02-20_EU_US_rebuliding_trust_EN.pdf) as well as the 10 April 2014 Opinion of the Article 29 Data Protection Working Party on surveillance of electronic communications for intelligence and national security purposes (available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf).

[221] See *ECtHR in A v. UK* (2009) (Application no. 3455/05).

[222] See C-27/09 P *French Republic v. People's Mojahedin Organization of Iran*, Opinion of Advocate-General Sharpston of 14 July 2011.

4. The preventive logics of coercion measures against persons on the grounds of future misbehaviour: an intelligence-led logic taking precedence over a criminal justice approach

This topic was discussed during the focus groups with a particular focus on preventive detention of suspected terrorists, and freezing of assets. A number of experts underlined the fact that the preventive (intelligence-led) logics have changed profoundly the very nature of evidence used in those proceedings: what is information and what is evidence? Evidence used in those cases is very different, and based much more on information (about networks of people, behavioural aspects, etc.) than evidence per se about someone actually committing a crime.

5. The use of intelligence information in adversarial and inquisitorial systems across Member States

Experts discussed the differences between and consequences for the two systems in the Member States under examination, with the adversarial being used more in common law countries while the inquisitorial is more common in civil law countries. In the case of the UK, it was noted that the use of special advocates and the CMPs in general was blurring the boundaries between adversarial and inquisitorial systems due to the fact that the special advocate could not speak to the defendant. The German case, which is under the inquisitorial system, allows the administration to introduce state secrets into the courts while maintaining good safeguards to prevent misuse of closed proceedings.

6. Interpol and the "wanted person" notices

One participant noted that similar challenges to the use of CMPs emerge when looking at Interpol and its "wanted person" notices, especially given the fact that there is no oversight on who is listed as a wanted person by the United Nations or by any other actor. The evidence used by police authorities to prove that a suspect should be listed in Interpol's database is often kept secret and not disclosed to the suspect or its lawyer. There are no effective remedies in place for a suspect to be removed from the database.

7. Freedom of expression and freedom of the press

The notion of freedom of expression was also tackled by experts, especially in relation to intelligence information. The Miranda case, in which the partner of a *Guardian* journalist was detained by British authorities in connection with the Snowden revelations, was mentioned by participants. Both the Council of Europe's Commissioner of Human Rights, Thorbjørn Jagland, and the European Commissioner for Justice, Viviane Reding, expressed concerns over press freedom and freedom of expression as guaranteed by Article 10 ECHR.[223]

8. Large-scale surveillance and international cooperation

Experts came back to the Snowden leaks of intelligence practices by US authorities and the consequences for the level of trust. One participant noted that the Snowden revelations were not surprising as regards the intelligence activities taking place but rather as regards the sheer scale of interception of data. In the past, British judges had already relied on evidence provided by intelligence services in IRA bombing cases (Birmingham Six, Guildford Four, etc.). Participants noted that there was an excess of trust by the courts towards the activities of intelligence officers and police agents, while lawyers were in general mistrusted. This poses serious challenges to lawyer-client confidentiality.

[223] See http://www.eubusiness.com/news-eu/britain-us-internet.qa3.

Annex 5. Country Fiches provided by the National Experts

Country Fiche: United Kingdom

European Parliament study on "*National Security Exceptions and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges*"

Author: Dan Squires

(Barrister, Matrix Chambers, UK)

This "country fiche" summarises the main findings and highlights the main issues underlined in the questionnaires filled in by the UK experts (who wished to remain anonymous).

KEY FINDINGS

- Since "closed material procedures" were first introduced to the UK in immigration cases in the 1990s, the number of areas in which such procedures can be used by the government has markedly increased. Such procedures are now permitted in all civil cases as well as a range of other (non-criminal) statutory schemes.
- Detailed procedural schemes involving Special Advocates appointed to represent parties in "closed" sessions and hearings to determine whether material should be considered in "open" or "closed" sessions have been developed.
- While the courts have held that closed processes with those procedural safeguards are not necessarily unfair, there is an ongoing debate in the UK as to whether a legal process in which one side does not see all of the evidence that is before the court can ever be a properly fair process.

1) Methodological note.

The country fiche was prepared by reading the other two questionnaires and examining case law and statutes that apply to CMPs. In addition I have worked as a lawyer on cases involving CMPs for approximately 10 years (and the same is true of the other two lawyers who filled in the questionnaires). Where there is no reference to a case, statute or news article etc. in the fiche, the information provided comes from my experience working in the area or speaking to others who do.

2) Please describe an illustrative case in your country that highlights the main issues at stake when dealing with secret information in courts.

One of the key disputes in the UK courts as to the use of secret information and Closed Material Procedures ("CMPs") has concerned the level of disclosure which is required in "open" sessions if the person affected by the proceedings is to have a fair trial. This has arisen in particular in relation to regimes which permit very significant restrictions to be imposed on individuals (for example, indefinite detention of foreign nationals suspected of being terrorists pursuant to the Anti-Terrorism Crime and Security Act 2001 or "control orders" imposed on suspected terrorists pursuant to the Prevention of Terrorism Act 2005). The question has arisen as to whether the state should be able to detain people or subject them to measures such as house arrest on the basis of evidence that the persons cannot see.

The particular issue that came before the courts was what would happen if the court had seen evidence in "closed" sessions which strongly indicated that the person was indeed rightly suspected of being a terrorist, but little, or in some cases none, of that evidence was provided to the person himself. Initially the courts in the UK held that in such circumstances it was still possible for the person affected to have a fair hearing. In AF (no 3) v. SSHD [2010] 2 AC 269, in relation to control orders, however, the House of Lords held that that was not the case. In a decision that was heavily reliant on the decision of the European Court of Human Rights A v. UK (2009) (Application no. 3455/05), the court held that an

individual must be provided with the "gist" of the case against him or her if the proceedings were to be compatible with the right to a fair trial protected by Art 6 of the European Convention on Human Rights. The court held that a person could not be subject to restrictive measures based largely or entirely on closed material. That was so even if the evidence against the individual in closed was overwhelming. The individual must be told a minimum of the case against them. This decision was subsequently applied in other areas where CMPs are permitted, such as asset freezing (see Mastafa v. HM Treasury [2013] 1 WLR 1621).

While closed processes remain markedly unfair, as individuals still do not see much of the evidence against them or discover the source of allegations that have been made, the position is a significant improvement. In earlier decisions people were subject to onerous executive orders on the basis that they were suspected of involvement in terrorism but without ever being told the gist of the case they had to meet. That is obviously incompatible with the right to a fair trial.

There are a number of statutory schemes which permit the courts to use CMPs. For example, where the Government wished to indefinitely detain foreign nationals suspected of being terrorists pursuant to the Anti-Terrorism Crime and Security Act 2001 or where they wished to impose "control orders" on suspected terrorists pursuant to the Prevention of Terrorism Act 2005, the courts were permitted to consider evidence whose disclosure would harm the national security in closed sessions. In every case in which individuals were subject to those regimes, CMPs were used.

To give one example see SSHD v. BM [2012] 1 WLR 2734.

BM was made subject to a control order in April 2011. It was said that he was reasonably suspected of being involved in terrorism. In particular, it was said that an American (MJB) who was arrested in New York in 2004 had provided information to the FBI identifying a number of people as having been involved in terrorism-related activity, including BM. Among the allegations were that prior to 2007 BM had attended Al Qaida training camps in Pakistan and transferred funds and equipment to Al Qaida in Pakistan. BM was told little else about the allegations than what MJB had said about him, but as occurs in all control order cases there was also closed material to support the allegations which the Government asserted (and the court accepted) would harm the public interest if disclosed. It is not known what material was contained in closed session, but it is understood that it is usually material obtained by interception or material from secret sources or agents whose identity is not public.

The hearing then proceeded with open and closed sessions. During the open sessions BM's "open advocates" were able to cross-examine a witness for the security service who was anonymous and gave evidence from behind a screen. There were then closed sessions when special advocates (appointed to represent BM and who had seen the closed material) were able to cross-examine the security service witness and to make submissions. Once the special advocates had seen the material, they were not permitted to speak to BM or to his open lawyers.

The court proceeded to give an open and closed judgment, having heard the open and closed evidence. It held that there were reasonable grounds to suspect that BM had been involved in terrorism-related activity and that the Home Secretary was justified in imposing a control order on him. It therefore upheld the order.

3) What are the bodies involved in the production and processing of secret evidence? Is there any oversight of the practices of the antiterrorist and (police-military) intelligence services that provide this evidence?

Material will be classified as "secret" by the Government (in particular the Security Services). It will not be covered by the Freedom of Information Act 2000. Unless a case comes to court, there will be no process by which it will be possible to force the disclosure of material classified as "secret".

That will be different if the courts become involved. In litigation in the UK all parties (including the Government) are required to disclose to the other side and the court all material which helps the other side's case as well as material which they wish to rely on. Where material which would otherwise be disclosed is said to harm national security or other public interests, the Government is permitted by

certain statutory regimes to place the material before the Court in a "closed" session. The material is then seen by the court, by the lawyers for the Government and by "Special Advocates" appointed to represent the interests of the other party. The material is, however, not seen by the other party, their "open" lawyers or the public. Furthermore, once the Special Advocates have seen the "closed material" they are not allowed to disclose the material or indeed speak to the party whose interests they are representing.

The Special Advocates can, however, argue that the material is not relevant or its admission would prevent a fair trial or that it should not be "closed" (for example, because its disclosure would not, in fact, harm national security). That argument will occur in a closed session and ultimately it will be the Court that will have oversight as to whether the material should be admitted in a "closed" session, made "open" or not admitted at all.

4) The concept of national security: how is it framed and understood in your country? On what grounds do authorities in your country define national security and how is this connected to a right to secrecy in courts? Are there any secrecy claims that obstruct oversight?

The concept of "national security" is not defined as far as I am aware in any legislation. Its meaning has, however, been considered by the courts. It was defined in broad terms by the House of Lords in the case of SSHD v. Rehman [2003] 1 AC 153. The House of Lords held that "national security" means essentially the "security of the United Kingdom and its people" (para 50); the interests of national security are not limited to action by an individual which can be said to be "targeted at" the UK, its system of government or its people (para 15); the protection of democracy and the legal and constitutional systems of the state are part of national security as well as military defence (para 16); action against a foreign state may be capable indirectly of affecting the security of the United Kingdom (para 16-17).

The connection between "national security" and "secrecy" in the court process depends on the particular applicable legislative scheme which permits CMPs. For example, the Justice and Security Act 2013 permits the Government to disclose evidence only in a "closed" process, provided it can satisfy the court that public disclosure of the material would harm "national security". In relation to other schemes (such as the Special Immigration Appeal Commission Act 1997) closed processes are permitted in relation to material whose disclosure would harm national security, but also where disclosure would harm the international relations of the UK, the detection and prevention of crime or any other public interest (see Special Immigration Appeals Commission Procedure Rules r 4(1)).

In my view, claims of secrecy clearly obstruct public oversight. If a closed material procedure is put in place, it means, for example, that where claims are brought making serious allegations against public officials of complicity in torture or unlawful rendition, the large majority of the evidence will be presented in closed sessions and considered in closed judgments. The identities of the members of the Security Service accused of wrongdoing are likely never to be revealed. That makes it very difficult if not impossible for the public to know whether serious allegations of misconduct are true and for those affected to hold to account those responsible. It also stymies wider public debate on issues of real importance.

5) What are the procedural guarantees and the protection standards for the rights of the defence, the freedom of the press and the protection of whistle-blowers in your country concerning the use of secret evidence in courts?

The key procedural guarantee protecting the right of the defence is the decision of the House of Lords in AF (no 3) in relation to disclosure required to protect the right to a fair trial pursuant to Article 6 of the European Convention of Human Rights. As set out above (see Section 1) the House of Lords held that a core irreducible minimum of disclosure of the gist of the case must be made in order to secure a fair trial.

As to freedom of the press, it would be possible to argue that permitting secret evidence and closed hearings interferes with the right to freedom of expression protected by Article 10 of the European Convention of Human Rights. If, however, the court concluded that permitting a closed hearing was

necessary to protect national security (which is a requirement for a closed process) it would almost certainly conclude that any interference with Art 10 rights was justified.

I am not aware of any procedural guarantees for whistle-blowers in relation to the use of secret evidence in court.

6) In your view, how do the current debates over the issue of digital surveillance affect the use of secret evidence in courts as regards the practices of intelligence services that have been denounced?

To date there has, to the best of my knowledge, been virtually no impact of the debates about digital surveillance on the use of secret evidence in courts. There is currently litigation in the UK on whether, in light of the revelations made by Edward Snowden, the UK's regime covering digital surveillance is sufficiently robust (see Liberty and others v. Security Services). That has not, however, as far as I am aware, affected the use of secret evidence in courts at least as far as "open" hearings are concerned. The Government's practice in "open" hearings is to "neither confirm nor deny" ("NCND") that it engages in any form of digital surveillance and it has not confirmed or denied the truth of any of the Snowden revelations insofar as they concern the UK engaging in interception of communications. That NCND policy has been accepted by the courts. While it may be that in "closed" hearings Special Advocates have sought to argue that recent revelations of digital surveillance practices means that certain evidence should not be admitted, that would not be made public (and I suspect such an argument will not have succeeded given that the legality of the government's digital surveillance programme is still being considered).

References

Jackson, "Justice, security and the right to a fair trial: is the use of secret evidence ever fair?" (2013) PL 720

Murphy, "Counter-terrorism and the culture of legality: the case of special advocates" (2013) KLJ 19

Chedrawe, "Assessing risk, minimising uncertainty, developing precaution and protecting rights: an analysis of the prohibition on communication between terrorist suspects and special advocates" (2012) O.U.C.L.J 33

Fordham, "Secrecy, security and fair trials: the UK constitution in transition" (2012) JR 187

Otty, "The slow creep of complacency and the soul of justice: observations on the proposal for English courts to adopt "closed material procedures" for the trial of civil damages claims" (2012) EHRLR 267

Kavanagh, "Special advocates, control orders and the right to a fair trial" (2010) MLR 836

Country Fiche: France

European Parliament study on "*National Security Exceptions and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges*"

Author: Roseline Letteron

(Université Paris-Sorbonne)

This "country fiche" summarises the main findings and highlights the main issues underlined in the questionnaires filled in by the following experts:

- **Jean-Philippe Grelot**, Haut fonctionnaire de sécurité de l'IGN-France, Auditeur de l'Institut des hautes études de défense nationale, ancien Conseiller du Secrétaire général de la défense et de la sécurité nationale
- **Patrick Ramaël**, Vice-président au tribunal de grande instance de Paris
- **Roseline Letteron**, Professeur de droit public à l'Université Paris-Sorbonne

This country fiche was originally written in French. English translation has been provided by a professional translator.

KEY FINDINGS

- The "Karachi affair" underlines the dual problem of national defence secrecy within French law: it can be invoked against a judge as well as the Parliament.
- The notion of "secret evidence" does not exist in French law because a confidential document or information may not be communicated to judges. Therefore, it cannot be used as evidence.
- Secrecy is conceived as one of the executive's prerogatives, going far beyond the context of intelligence services. There is very limited control over the way secrecy is being used; control is not exercised by judges, but by the Parliament, in a very restricted way.
- The notion of national security is used in France in a doctrinal, rather than legal manner. Indeed, it appears in texts that define the doctrine of security and defence. When it does occur in legal documents — and that is quite rare — its content is highly uncertain.
- The difficulties inherent to de-classifying secret materials in France are considered by some, including antiterrorism judges, as a breach of the separation of powers.
- It is only recently that French law has shown interest in "whistle-blowers". It provides no legal definition and does not provide for a single system for all whistle-blowers.
- A law adopted in 2010 established the journalists' right to protect their sources. Yet, it stated that it was possible to jeopardise source secrecy "if justified by a prevailing imperative of public interest, and if the contemplated measures are strictly proportional to the objective pursued". The notion of "*prevailing imperative of public interest*" is quite vague, and case law has showed its limits, particularly concerning the resulting difficulties of interpretation.

1) Methodological note.

This country fiche was prepared by the author on the basis of the data available in the questionnaires, which were answered by the above-mentioned French experts.

2) Please describe an illustrative case in your country that highlights the main issues at stake when dealing with secret information in courts.

On 8 May 2002, a Pakistani Navy bus taking 23 French DCN workers to the construction site of submarines sold by France to Pakistan was hit by an explosive-laden vehicle. The suicide attack killed 14 persons and injured 12.

Twelve years later, the investigation remains inconclusive. On 27 May 2002, a preparatory enquiry was initiated for *"murder and complicity in murder attempts related to a terrorist undertaking*". Since that day, various antiterrorism judges have dealt with the case, from Jean-Louis Bruguière in 2002 to Marc Trévidic and Yves Jeanier, who have been in charge since 2008. Several leads have been explored, focusing on al-Qaeda or Indian authorities. Today, judges seem to be considering a third lead involving certain Pakistani groups acting in revenge after France decided to stop paying commissions related to arms contracts.

While judges esteem the latter lead to be "cruelly logical", it remains that the case has not been closed before a criminal court, which reveals the dual problem of national defence secrecy within French law:

- On the one hand, it is opposable to the judge. Since the case began, antiterrorism judges have used the only procedure the law provides for. They have asked the Minister of Defence to declassify some evidence, and the Commission consultative sur le secret de la défense nationale (Consultative Commission on National Defence Secrecy, CCSDN) has been called on to advise on the declassification. The CCSDN has issued 15 advisory opinions since 2002, two-thirds of which are in favour of declassification and one-third completely or partially against it. Yet this does not mean that the evidence required has been given to the judges, since the Minister is not bound by the Commission's opinion.

- On the other hand, secrecy is also opposable to the Parliament. In 2009, the Assemblée nationale created an "*information mission on the circumstances of the attack on 8 May 2002 in Karachi*" ("*mission d'information sur les circonstances entourant l'attentat du 8 mai 2002 à Karachi*"). This parliamentary mission released a report on 12 May 2010, in which it stated the challenges it had to face: "Members [of the Commission] regret that the Government has not transmitted to them the first-hand documents that may have helped them in their task and allowed them to fully exercise their mission of parliamentary control" ("*Ses membres regrettent que le Gouvernement ne leur ait pas communiqué les documents de première main qui auraient pu les aider dans leur tâche et leur permettre d'exercer pleinement leur mission de contrôle parlementaire*"). National defence secrecy has been opposed to their investigations, just like investigation secrecy, since a criminal procedure was being held. As a result, neither the Parliament nor the judges could access relevant information.

3) What are the bodies involved in the production and processing of secret evidence? Is there any oversight of the practices of the antiterrorist and (police-military) intelligence services that provide this evidence?

The notion of "secret evidence" does not exist in French law, because a confidential document or information may not be communicated to the judges. Therefore, it cannot be used as evidence.

Evidence is freely discussed in criminal law as long as it has been lawfully obtained. A document covered by national defence secrecy will be admissible evidence only if it has been declassified. Thus it can only be included in the case or be mentioned at a hearing after having been declassified. If a judge were to override this principle, they would be compromising national defence secrecy.

Secrecy is conceived as one of the executive power's prerogatives, going far beyond the context of intelligence services (I). There is very limited control over the way secrecy is being used; it is not exercised by judges, but by the Parliament, in a very restricted way (II).

I – A prerogative of the executive power

In its current definition, national defence secrecy is governed by the provisions of article 413-9 of the Code pénal (Criminal Code), as modified by law No. 2009-928 of 29 July 2009 on military planning for

the years 2009 to 2014, stating several provisions concerning defence, and as modified by the article 1 of decree No. 2010-678 on 21 June 2010 on the protection of national defence secrecy.

As quoted respectively:

- article 413-9 in the Criminal Code:

> Under this section, the processes, objects, documents, information, computer networks, computerised data or files of interest for the national defence that have been subjected to classification measures aiming at restraining their access or divulgation are considered to be a secret of national defence.
>
> Processes, objects, documents, information, computer networks, computerised data or files whose divulgation or access to which might damage national defence or might lead to uncovering a secret of national defence may be subjected to such measures.
>
> Classification levels of processes, objects, documents, information, computer networks, computerised data or files presenting the character of national defence secrecy and the authorities responsible for defining the ways in which their protection is organised are both determined by decree in State Council.[224]

- article R. 2311-3 in the Code de la défense (Code of Defence):

> Level Very Secret-Defence is reserved to information and media pertaining to government priorities in defence and national security, whose divulgation might very severely damage national defence.
>
> Level Secret-Defence is reserved to information and media whose divulgation might severely compromise national defence.
>
> Level Confidential-Defence is reserved to information and media whose divulgation might damage national defence or might lead to uncovering a national defence secret classified as Very Secret-Defence or Secret-Defence.[225]

General organisation befalls the Prime Minister under article 21 of the Constitution: *"*The Prime Minister leads government action. He is responsible for national defence*"* ("*Le Premier ministre dirige l'action du Gouvernement. Il est responsable de la défense nationale"*) and article L. 1131-1 of the Code of Defence: *"*The Prime Minister leads government action in matters of national security*"* ("*Le Premier ministre dirige l'action du Gouvernement en matière de sécurité nationale"*). In this respect, the Prime Minister is helped by the General Secretary for Defence and National Security, who, under §3 of article R.* 1132-2 in the Code of Defence, "suggests, communicates and ensures the enforcement and control of necessary measures for the protection of national defence secrecy*"* ("*propose, diffuse et fait appliquer et controller les mesures nécessaires à la protection du secret de la défense nationale*").

Consequently, each minister is responsible for adapting most measures to the idiosyncrasies of their ministry's activities as well as those of related operators, under the provisions of article L. 1141-1 in the

---

[224] In French: *"Présentent un caractère de secret de la défense nationale au sens de la présente section les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.*

Peuvent faire l'objet de telles mesures les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation ou auxquels l'accès est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Les niveaux de classification des procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de la défense nationale et les autorités chargées de définir les modalités selon lesquelles est organisée leur protection sont déterminés par décret en Conseil d'État".

[225] In French: *"Le niveau Très Secret-Défense est réservé aux informations et supports qui concernent les priorités gouvernementales en matière de défense et de sécurité nationale et dont la divulgation est de nature à nuire très gravement à la défense nationale.*

Le niveau Secret-Défense est réservé aux informations et supports dont la divulgation est de nature à nuire gravement à la défense nationale.

Le niveau Confidentiel-Défense est réservé aux informations et supports dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié au niveau Très Secret-Défense ou Secret-Défense".

Code of Defence: "Each minister is responsible, under the authority of the Prime Minister, for preparing and executing defence and national security measures pertaining to the department they are in charge of." ("*Chaque ministre est responsable, sous l'autorité du Premier ministre, de la préparation et de l'exécution des mesures de défense et de sécurité nationale incombant au département dont il a la charge.*") Since level Very Secret-Defence is by nature attached to government priorities, related modalities remain centralised (cf. article 9 in the inter-ministerial investigation No. 1300 on the protection of national defence secrecy, approved by an order on 30 November 2011).

Declassification decisions are thus always issued by the French administration. Yet security agreements binding France to foreign States, or international rules concerning certain organisations, can organise a system of mutual respect of protected secrets. A State may receive classified documents from another State, provided they have both concluded a security agreement. Such an agreement determines equivalences and ensures that each State will protect the other State's classified information in the same way as its own classified information of equivalent level. Such is the case, for instance, of the Agreement for the security of information on 6 March 2007, binding the States that are parties to the North Atlantic Treaty, which France signed on 13 October 1997 and has been enforced since 25 April 2001.

In practice, the fundamental legal provisions of national defence secrecy that all other provisions will refer to do not pertain so much to how this secrecy is qualified as to the breach constituted by its divulgation, and the subsequent criminal penalty.

The aforementioned instruction establishes the set of access rules to national defence secrecy, such as concerned persons' prior authorisation and the "need to know": a person's rank and their authorisation to access the required level do not grant them any "right of access". They must need to know the information at stake because of their attributions or activities. The instruction also determines material measures of information protection and material measures related to electronic communication networks, on which the information can be stored or kept.

Intelligence services are attached to the relevant ministry: Direction générale de la sécurité extérieure (General direction of foreign security); Direction du renseignement militaire (Direction of military intelligence) and Direction de la protection et de la sécurité de la défense pour le ministère de la Défense (Direction of defence protection and security for the Ministry of Defence); Direction générale de la sécurité intérieure pour le ministère de l'Intérieur (General direction of domestic security for the Ministry of Interior). While their missions entail deciding how to classify a high number of information and documents, the procedures they use to that end are not specific in any way.

Once the information has been classified, the fundamental principle is that no one is qualified to know it unless they are authorised at the required level and need to know it (R. 2311-7 in the Code of Defence). Authorisation is granted at the outcome of a procedure checking that a person may, without hazard to national defence and security or their own security, know classified information while exercising their function.

Thus the judicial authority is in no way involved in this classification process.

II – Parliament's limited control

There is no judicial control over the classification procedure.

Parliamentary control over intelligence services is extremely limited. Law No. 2007-1443 on 9 October 2007 created a parliamentary delegation for intelligence. Members are authorised to receive such data, but their activity remains restricted to intelligence, and whether they have access to all information useful for its control is uncertain.

This initiative has not substantially questioned the principle of national defence secrecy's opposability to members of Parliament. Thus investigative commissions cannot obtain in this manner classified evidence (order of 17 November 1958). The Conseil constitutionnel (Constitutional Council) confirmed this prohibition in its decision No. 2001-456 DC on 27 December 2001.

One can argue that Law No. 2013-1168 of 18 December 2013 on military planning for the years 2014 to 2019, stating various provisions concerning national security and defence, broadened somewhat the scope of information members of Parliament may access, by listing the documents that could be

transmitted to them. Yet these documents are of a general nature, or are inspection reports. Indeed, the law cautiously establishes that such transmission shall pertain "neither to current operations in these services, nor to instructions given by public powers in this respect, nor to operational procedures and methods, nor to exchanges with foreign services or with international bodies that are competent in the field of intelligence".[226] In the current state of law, Parliamentary information in this field remains very lacking.

4) The concept of national security: how is it framed and understood in your country? On what grounds do authorities in your country define national security and how is this connected to a right to secrecy in courts? Are there any secrecy claims that obstruct oversight?

The concept of "national security" has an Anglo-Saxon origin. It appeared in the United States in 1947 with the National Security Act, by which the Truman administration established the country's legal framework of defence and intelligence.

The notion of national security is used in France in a doctrinal, rather than legal manner. Indeed, it appears in texts that define the doctrine of security and defence. When it does occur in legal documents – and that is quite rare – its content is highly uncertain.

I – The defence and security doctrine

In the preface to the Livre blanc sur la défense et la sécurité nationale (White Paper on National Defence and Security) released in 2008, then-President of the Republic Nicolas Sarkozy asserted: "From this work, a new concept emerges: that of a national security strategy*."* ("*De ce travail émerge un nouveau concept : celui d'une stratégie de sécurité nationale*"). The military planning law of 29 July 2009, which implemented the White Paper recommendations, segues in article 5:

> The national security strategy aims to identify all threats and hazards that might affect the life of the Nation, particularly concerning the protection of the population, the integrity of the land and the permanence of the Republic's institutions, and to determining the response that public powers must give*"* (art. L 1111-1, Code of Defence).[227]

This "national security strategy" rests on two principles. On the one hand, the affirmation of a "defence-security continuum" ("continuum défense-sécurité"), a popular phrase at the time that asserted a unity of threat, whether foreign or domestic. On the other hand, the idea that this national security policy must cause a certain centralisation, as services are tightened around the President of the Republic, particularly with the creation of an Intelligence Coordinator ("Coordinateur du renseignement").

This evolution remained moot. Those who thought that the notion of "national security" would replace from now on the notion of "national defence" had to acknowledge this notion's demotion in the following years. The White Paper of 2013 does maintain the title "*National Defence and Security*" ("*défense et sécurité nationale*") but does not assert a defence-security continuum. Law No. 2013-1168 of 18 December 2013 concerning military planning for the years 2014 to 2019 mentions "national security" in its title, but the gist of it returns to a traditional, thus narrower, conception of national defence.

II – Legal texts

The term "national security" comes up *expressis verbis* in some texts.

---

[226] In French: "*ni sur les opérations en cours de ces services, ni sur les instructions données par les pouvoirs publics à cet égard, ni sur les procédures et méthodes opérationnelles, ni sur les échanges avec des services étrangers ou avec des organismes internationaux compétents dans le domaine du renseignement".*

[227] In French: *"La stratégie de sécurité nationale a pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter*" (art. L 1111-1 code de la défense).

The oldest is certainly article 3 in law No. 91-646 of 10 July 1991, which already invokes "national security" as one of the reasons justifying a security interception, that is, phone tapping ordered by the administration. It is merely a reference to "*intelligence of relevance for national security*" ("*renseignements intéressant la sécurité nationale*"), a phrase that the legislator intended as a reference to foreign intelligence. Similarly, article 4 in decree No. 2002-890 of 15 May 2002 on the Conseil de sécurité intérieure (Domestic Security Council) grants this institution competency on matters that "are relevant to intelligence and national security planning" ("*intéressant le renseignement et la planification de la sécurité nationale*").

More recently, one finds the notion of "national security" in the order (arrêté) of 30 November 2011, bearing the approval of inter-Ministry general instruction No. 1300 on the protection of national defence secrecy, signed by the delegation of the Prime Minister and by the General Secretary of Defence and National Security (*Secrétaire général de la défense et de la sécurité nationale*, SGDSN). It states, "The protection of secrecy concerns all fields of activity related to defence and national security: political, military, diplomatic, scientific, economic, industrial fields".[228] Yet, regarding the legal regime implemented, this text bears no consequence. Implemented procedures remain those that were devised about the secrecy of national defence; public security secrecy is not distinguished from them.

After the 2009 military planning law, the notion of "national security" has been used as a foundation for "*national security planning*" ("*planification de sécurité nationale*"), a phrase that covers most government plans aiming at managing crises related, for instance, to terrorist actions or catastrophes. The General Secretary for Defence and National Security is responsible for their elaboration (article R* 1332-3 of the Code of Defence).

Thus the notion of national security is used either as an umbrella notion motivating measures taken to ensure security, or more simply as a synonym of national defence when qualifying intelligence activities.

Generally speaking, these security matters do not give rise to any kind of debate in France. The fight against terrorism is an effective argument for justifying increasing investigation powers of intelligence services, particularly concerning access to personal information.

5) What are the procedural guarantees and the protection standards for the rights of the defence, the freedom of the press and the protection of whistle-blowers in your country concerning the use of secret evidence in courts?

As mentioned above, national defence secrecy is opposable to everyone, judge or journalist. Any person who learns of or issues classified information commits the crime of compromising national defence secrecy and may as a penalty be imprisoned for five years and pay a €75,000 fine.

Yet there exists a certain number of derogatory procedures that allow one to either access classified information or not be prosecuted and punished for gaining knowledge of it. Three agents have been evoked: judges, whistle-blowers and members of the press. Their respective situations vary widely. It is thus appropriate to treat them separately.

I – Judges

In principle, a document covered by national defence secrecy may constitute receivable evidence only if it has already been declassified. Yet refusing to transmit information covered by national defence secrecy to a judge might constitute contempt of court. For this reason, the law allows for a specific procedure allowing the judge to obtain that requested evidence be declassified. This purely administrative declassification procedure entails serious issues related to the principle of separation of powers.

1° – An administrative procedure

[228] In French: "*La protection du secret concerne tous les domains d'activités relevant de la défense et de la sécurité nationale : politique, militaire, diplomatique, scientifique, économique, industriel*".

This declassification is an administrative decision that can be analysed as an authorisation, granted to the judge, to make certain decisions within criminal proceedings:

- a search, that is, a visit to places containing classified information;
- the hearing of an authorised person, who must be freed from their obligation by the competent minister;
- a judicial requisition, that is, the judge is provided with elements that are relevant for manifesting the truth. In that case, one must distinguish between two situations: either the judge has identified classified elements and asks for their communication, directly addressing a declassification request to the classifying authority; or the judge cannot precisely identify the evidence, in which case he asks the administration to search for it.

This declassification procedure is organised by law No. 98-567 of 8 July 1998. It involves the Commission consultative du secret de la défense nationale (CCSDN, Consultation commission for national defence secrecy), an authority that is qualified as independent and is related to the Prime Minister.

In the sense of its article 4, any French jurisdiction, "within the context of proceedings initiated before it, may ask for the declassification and communication of information that is protected in the name of national defence secrecy, to the administrative authority in charge of such classification".[229] The competent authority must then appeal "promptly" ("sans délai") to the CCSDN, which advises within two months on the potential declassification of the requested evidence. This opinion "takes into account the missions of the public service of justice, compliance with the presumption of innocence and the rights of defence, respect of France's international commitments and the necessity to protect the defence capacities and the security of staff" (art. 7).[230] The CCSDN does not explain the motives for its advice, which means that the judicial authority never knows whether refusal is based on the document's sensitive nature or the fact that it is irrelevant to the case in hand. The CCSDN, in its latest report on the period 2010-2012, suggests adopting the principle of explaining the motives of its advice precisely in order to avoid this uncertainty. As of now, this suggestion has not given rise to any practical measure.

This advice is not effectively binding on the competent authority. When it is negative, the authority can opt for declassification. When declassification is advised, the authority may refuse it and take a position against the communication of requested evidence. Because of this procedure, one can assert that the CCSDN, even though it is by law an independent administrative authority, is actually an ordinary consultation commission devoid of any normative power. In no circumstance can it impose that a document be declassified.

It must be noted that in the French system, the declassification request procedure by a judicial authority does not apply to information that has been classified by a foreign State according to its own provisions. Conversely, in some States, such as the United Kingdom, in which national interest – determined in a sovereign manner – prevails over international agreements, classified information of foreign origin may be transmitted to a jurisdiction upon request. Such a situation is problematic in French law, since information transmitted under a security agreement may be accessed by British judges but not by French judges.

2° – The principle of separation of powers

This procedure is considered by some authors, including antiterrorism judge Marc Trevidic, as a breach against separation of powers, a principle that is guaranteed by article 16 of the 1789 Declaration of the Rights of Man and Citizen : "Any society in which rights are not guaranteed or separation of powers is

---

[229] In French: "*dans le cadre d'une procédure engagée devant elle peut demander la déclassification et la communication d'informations, protégées au titre du secret de la défense nationale, à l'autorité administrative en charge de la classification*".

[230] In French: "*prend en considération les missions du service public de la justice, le respect de la présomption d'innocence et les droits de la défense, le respect des engagements internationaux de la France ainsi que la nécessité de préserver les capacités de défense et la sécurité des personnels*".

not determined, has no constitution" ("*Toute Société dans laquelle la garantie des Droits n'est pas assurée, ni la séparation des Pouvoirs déterminée, n'a point de Constitution*") (Marc Trévidic, Au cœur de l'antiterrorisme, Jean-Claude Lattès).

The question has been raised about the military planning law of 29 July 2009, authorising the classification of information and of the places that store them. In this case, temporary declassification of a place could only be obtained by authorisation of the minister, after the CCSDN communicated its advice to the department concerned by the search. Thus it appears clearly that the administrative authority can block the judges' investigations in this way, which seems to hint at a breach against separation of powers. This breach might be invoked against the whole declassification procedure, be it applied to locations, documents or information.

Yet the issue of this procedure's constitutionality has been raised on the subject of the places covered. Advocates of this measure based their reasoning on the need to protect judges by avoiding the risk of any proceedings against them for compromising the "secret défense". By searching in a classified place, didn't the judge risk seizing classified evidence that was unrelated to the case at hand? The judge might then compromise top-secret defence matter in spite of themselves.

In its decision of 10 November 2011, rendered on a priority question on constitutionality (*question prioritaire de constitutionnalité*, QPC), the Conseil constitutionnel esteemed that the lawmaker had operated an "unbalanced conciliation" ("*conciliation qui est déséquilibrée*") between the demands of fair trial and compliance with the separation of powers granted by article 16 in the Declaration of 1789. The Conseil has thus punished the provision for breach of separation of powers (order No. 2001-192 QPC Ekaterina B et al.)

This decision has stirred a doctrinal movement that considers that the reasoning followed by the Conseil constitutionnel may be extended to all of the procedures organising national defence secrecy.

II – Whistle-blowers

It is only recently that French law has shown interest in "whistle-blowers". It provides no legal definition and does not contemplate a single legal regime for all whistle-blowers. The latter are submitted to fragmentary provisions; looking for legal consistency within a rather disparate set would be vain.

- Whistle-blowers attracting attention to work conditions or corruption within a private company are provided for by law No. 2013-117 of 6 December 2013 on tax fraud and major economic and financial crime. Article 35 forbids any direct or indirect disciplinary action against an employee denouncing facts establishing a breach that came to their knowledge during their professional activities. The penalty lies in reversal of the burden of proof. In case of dispute, the company director must demonstrate that the measure against the employee was not motivated by the latter's denunciation.
- Whistle-blowing civil servants are protected by article 6 of the 1983 statute, from law No. 2012-954 of 6 August 2012. It is mentioned that no measure concerning recruitment, establishment, training, rating, discipline, promotion, assignment and transfer may be taken regarding a civil servant because he has filed proceedings by an officer or by a court, or born witness in cases related to moral or sexual harassment, or discriminatory practices.

tive loe scope is much narrower in the public than in the private sector. On the one hand, protection covers only civil servants, not all agents. On the other hand, the guarantee does not concern all breaches that might come to the knowledge of civil servants while exercising their function, but only those that are related to foul treatment of other agents, cases of discrimination or harassment.

It seems that this situation will not be questioned, at least in the short term. In its annual report released on 9 September 2014, the Conseil d'État considers the hypothesis of a "Snowden case", that is, the case of an intelligence service civil servant denouncing illegal activities. According to the Conseil, "violating national defence secrecy shall not become a right, even when the denunciation of an illegal programme is at stake" ("*la violation du secret de la défense nationale ne saurait devenir un droit, même lorsqu'il s'agit de dénoncer l'existence d'un programme illégal*"). The agent sending documents to the press is thus guilty of compromising national defence secrecy. Yet the Conseil d'État suggests that in this case, a

"right to signal" ("droit de signalement") should be acknowledged concerning agents involved in data collection. This right would be exercised with an intelligence services control authority (autorité de contrôle des services de renseignement, ACSR), that would, obviously, be an administrative authority. Thus the Conseil d'État suggests leaving whistle-bowers only an internal path of action within the administration.

Positive law concerning the protection of whistle-blowers is both, as yet, fragmentary and unfinished. Trial judges are fully aware of this and strive to drive for purely judicial evolutions. In a decision of 15 July 2014, the administrative court of Cergy-Pontoise voided, on the grounds of misuse of power, the refusal to reintegrate the manager of a public institution who had denounced fraudulent procurement procedures, which had led to a criminal sentence for some agents. The court based its order on a general principle that forbids retaliating against civil servants who have denounced illegal acts. The principle is unheard of and its endurance is hard to vouch for. Indeed, there is no guarantee that the Conseil d'Etat will adopt and approve this principle (Administrative court of Cergy-Pontoise, 15 July 2014, Revue des droits de l'homme, note by J.P. Foegle, August 2014).

III – Journalists and the press

Journalists are not considered "whistle-blowers" by French law, but those who pass on information to them may be considered such, at least in some hypotheses. This is why the right to source secrecy is now established, even though it is exercised in relatively stringent conditions.

- The first text involved in this matter was article 109 in the Code of Criminal Proceedings (Code de procédure pénale), derived from law No. 93-2 on 4 January 1993. It authorised the journalist who served as a witness not to mention their sources before the instruction judge. Yet this right to silence did not forbid the judge from obtaining these sources by other means of investigation, such as searches. The European Court sanctioned this precise possibility in two successive orders, *Martin vs France* on 12 April 2012, and *Ressiot vs France* on 28 June 2013. Both orders were related to searches conducted on the newspapers' premises or at the journalists' homes.
- The law of 4 January 2010 is the first text sanctioning journalists' right to secrecy of their sources in French law. Yet it stated that it was possible to jeopardise source secrecy "if justified by a prevailing imperative of public interest, and if contemplated measures are strictly proportional to the objective pursued" ("*si un impératif prépondérant d'intérêt public le justifie et si les mesures envisagées sont strictement proportionnées au but poursuivi*"). The notion of "*prevailing imperative of public interest*" (*impératif prépondérant d'intérêt public)* came across as quite vague, and case law has showed its limits, particularly concerning the resulting difficulties of interpretation.

In order to illustrate these difficulties, two precedents must be mentioned:

- In 2009, *Le Figaro Magazine* published pictures of a criminal, taken by surveillance cameras during his escape from the penitentiary institution where he was imprisoned on a long-term sentence. The police officer who was suspected of having provided those photographs was sued for breaching professional secrecy and the journalist was sued for concealing a breach of professional secrecy. The latter asked the Instruction Chamber of the Paris Court of Appeal (Chambre d'instruction de la Cour d'appel de Paris) to void several acts of procedure, including a search at his home where his computer and mobile phone had been seized, as he deemed that these measures violated source secrecy. The Chamber, in its judgement on 4 June 2013, esteemed that the condition of "*prevailing imperative of public interest*" was fulfilled, since a police officer was being suspected of severely failing to fulfil their obligations. The Court of Cassation did not retain this analysis. On the contrary, it considered that the Court of Appeal had not demonstrated that "the disputed interventions resulted from a prevailing imperative of public interest" (Criminal Court of Cassation, 25 February 2014, Appeal No. 13-84761). Thus this notion appears to be highly subjective when it does not specify definition criteria for this "*prevailing imperative of public interest*".

- The most mediatised case related to source secrecy is the one that was initiated by the press release of Mrs Bettencourt's phone conversations; the recordings were made without her knowledge and consent by one of her employees. In September 2012, *Le Monde*, which released transcripts of some conversations,

filed a complaint for breach of right to protect information sources, asserting that the executive power asked domestic intelligence services (services de renseignement intérieur, DCRI) to find the person who tipped a journalist about the case. At the same time, it appeared that the prosecutor of Nanterre, then in charge of the case, had obtained from an operator the detailed invoicing of the journalist's phone, which had allowed him to identify the source, a magistrate who worked at the cabinet of the Minister of Justice. This case is still pending before the criminal judge.

As regards source secrecy, the case nevertheless allowed the Court of Cassation to render a judgement in a decision of 6 December 2011. In the case in hand, the Court of Cassation sanctions the order of the Instruction Chamber for the Court of Appeal, which had voided the prosecutor's demands during due diligence to phone operators in order to identify the journalists' contacts. For the Court, searching for the source does not constitute a "*prevailing imperative of public interest"*. Indeed, at the time, no judicial information was open and the breach invoked – violation of professional secrecy – remains purely hypothetical (Criminal Court of Cassation, 6 December 2011, appeal No. 11-83970).

This decision, by confirming the annulment of demands aimed at identifying the journalist's source, indicated that the 2010 law was being questioned. Indeed, this text could not prevent a magistrate, related to the executive power, to find a journalist's source, even if his demands were voided afterwards. In this regard, the law failed in the media aspect first and foremost, and also in the legal aspect, since the law relied on notions that were too vague. The very persons who wanted to undermine source secrecy vastly exploited these imprecisions.

A recently drafted law is thus more precise. The draft asserts that there is a manifest attempt at undermining source secrecy if three conditions are met:

- the need for undermining, that is, the fact that the author of a severe breach cannot be found by any other way;
- the proportionality of the measure, which finds its origin in precedents of the European Court for Human Rights, as seen above;
- "[u]ndermining is justified by the prevention or repression either of a crime or an infraction constituting severe damage for the person or the Nation's fundamental interests…" ("*L'atteinte est justifiée par la prévention ou la répression soit d'un crime soit d'un délit constituant une atteinte grave à la personne ou aux interest fondamentaux de la Nation (...)*".

The first two conditions were already mentioned in the 2010 text, but the reference to "*the Nation's fundamental interests*" ("*intérêts fondamentaux de la Nation*") is new. Will this notion be an improvement on the "*prevailing imperative of public interest*" ("*impératif prépondérant d'intérêt public*")? One may doubt it, since the draft contains as yet no serious definition of this concept, and provides for derogation to source secrecy not only with the aim of repressing breaches but also with that of preventing them.

6) In your view, how do the current debates over the issue of digital surveillance affect the use of secret evidence in courts as regards the practices of intelligence services that have been denounced?

This question is impossible to answer. In French law, the evidence produced in court may not be protected by national defence secrecy. Thus there is no judicial control of intelligence services' activities.

References

Vincent Boulanin, Retour sur l'adoption du concept de sécurité nationale, ou l'assimilation d'un discours de sécuritisation dominant, Le Débat stratégique, n° 176, mai 2009

Conseil d'Etat. Le numérique et les droits fondamentaux. Rapport. 9 septembre 2014.

Francis Delon, Secret de la défense nationale, intervention du Secrétaire général de la défense et de la sécurité nationale. Défense, revue de l'IHEDN, avril 2009.

du Cheyron, Les secrets de la défense nationale. In Y. Loussouarn et P. Lagarde (dir.), L'information en droit privé, travaux de la conférence d'agrégation, LGDJ, 1978, p. 570 et s.

Marc Guillaume, Secret de la défense nationale et Etat de droit. In « L'Etat de droit », Mélanges en l'honneur de Guy Braibant, 1996, p. 383 et s.

Nicole Guimezanes et Christophe Tuaillon, Droit pénal de la sécurité et de la défense, L'Harmattan, 2006

Roseline Letteron, L'Etat de droit face au terrorisme, Annuaire français de relations internationales, 2008.

Roseline Letteron, Le secret de la défense nationale, Questions Internationales, Janvier 2009.

Roseline Letteron, Le système français contre le terrorisme et la garantie de l'Etat de droit, Regards sur l'Actualité, La Documentation française 2010 (sous le pseudonyme d'Agnès Blanco).

Roseline Letteron (sous la dir.), La liberté d'expression du fonctionnaire en uniforme, Economica, 2000.

Marc Trévidic, Au cœur de l'antiterrorisme, Jean-Claude Lattès.

Bertrand Warusfel, Contre-espionnage et protection du secret - Histoire, droit et organisation de la sécurité nationale en France , Lavauzelle, 2000.

Bertrand Warusfel, La sécurité nationale, nouveau concept du droit français. In : Les différentes facettes du concept juridique de sécurité – Mélanges en l'honneur de Pierre-André Lecocq, Université Lille 2, 2011, pp. 461-476

Bertrand Warusfel, Le cadre juridique des relations entre défense et sécurité nationale », Cahiers de la sécurité n° 14, INHESJ, décembre 2010, p. 61 et s.

Bertrand Warusfel, Le contrôle du secret de la défense nationale : une exigence de l'Etat de droit. Droit et Défense 1996 n° 4, p. 23 et s

Country Fiche: Germany

European Parliament study on "*National Security Exceptions and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges*"

Author: Nikolaus Marsch

(University of Freiburg)

This "country fiche" summarises the main findings and highlights the main issues underlined in the questionnaires filled in by the following experts:

- **Jan Bergmann**, Judge
- **Udo Kauß**, Lawyer
- **Nikolaus Marsch**, University of Freiburg
-

KEY FINDINGS

- All evidence introduced to court proceedings and used by the courts has to be disclosed to all parties to the proceedings. An introduction of a close material procedure into German law would be unconstitutional.
- Intelligence information can indirectly be used in court proceedings via second-hand evidence ("hearsay"). In this case, the court has to take into account the lower probative force of second-hand evidence.
- If, for reasons of national security, the intelligence services refuse to give access to secret information, the parties to court proceedings can challenge this refusal in order to get access to the information. The legality of the refusal is assessed by a higher Administrative Court in an intermediate *in camera* procedure.
- "National security" can be a reason to refuse access to intelligence information. German courts interpret this reason for refusal narrowly.
- Illegally gathered intelligence information can be used in court proceedings if the court - when balancing the two sides - determines that the general interest of fighting crime outweighs the rights of the accused, which have been infringed by the intelligence services. There is no general fruit-of-the-poisonous-tree-doctrine in Germany.
- While there are no general rules on the protection of whistle-blowers in Germany, the press has enjoyed a privilege in criminal law since 2012. Journalists can no longer be accused of complicity to breach an obligation of secrecy.

Some introductory and methodological remarks

The present country fiche is based on two pillars: First, the way in which the German legal system deals with the use of intelligence information in court proceedings is regulated by the German constitutional law and the jurisprudence of the Federal Constitutional Court. This normative basis is described in the following by summarising the applicable law and jurisprudence. Second, the indirect use of intelligence information – which has been held as conforming to the constitution by the Federal Constitutional Court – has a strong practical dimension. For this reason, an interview with a presiding judge of an administrative Court (Prof. Dr. Jan Bergmann, LL.M.) has provided valuable insights to judicial

practice.[231] The same is true for the answers of Dr. Udo Kauß (lawyer and one of the leading members of the Humanistische Union) with regard to the control of intelligence services by the citizens via a right of access to the files.[232]

The aim of the present country fiche is to allow a comparison of the way in which the German and other legal orders deal with secret information in court proceedings. In order to facilitate such a comparison, a structured template for the country fiches with numerous specific questions has been developed by the authors of the overall study. The author of the present country fiche is fully aware that such a structure is of great importance to rendering a well-founded comparison. However, in accordance with the topic of the study, the underlying basis of the questions is the existence of secret evidence/closed material proceedings in the national legal order. As for constitutional reasons such closed material proceedings do not exist in Germany, the questions do not fit the German legal order and it is not possible to answer most of them. Because of this, the country fiche does not follow the proposed structure but rather tries to explain the indirect use of intelligence information by German courts (III. and IV.) and the intermediate *in camera* procedure, which has been introduced to the Administrative Court Procedure Act in order to strengthen the right of an effective remedy (V.). In addition to that and in order to give the most concrete answers possible to the questions raised by the authors of the study, short overviews are given on the questions regarding which authority is competent (and on what ground) to classify intelligence information as being secret (VI.), whether illegally gathered intelligence information can be introduced to court proceedings (VII.) and whether whistle-blowers and journalists enjoy particular protection when publishing secret intelligence information (VII.).

I. Illustrative cases

The indirect use of intelligence information

In 1980 Friedrich Cremer, a member of the Parliament of Bavaria, was sentenced to prison for having spied for the intelligence service of the German Democratic Republic (MfS). The court based its judgement inter alia on the reading of the minutes of a police interrogation of a former collaborator of the MfS, Werner Stiller, who had fled from the GDR and lived under the protection of the West German intelligence service in a secret place in West Germany. The court also heard as a witness the police officer who had interrogated Stiller. However, the court did not succeed in summoning Stiller, as the West German intelligence service refused to reveal the location of his residence, citing well-grounded information that GDR authorities were planning to kidnap and execute him. The Federal Constitutional Court dismissed as unfounded Cremer's appeal of the criminal court's verdict (Federal Constitutional Court, 26.5.1981, 2 BvR 215/81; see under III. and IV.).

The strengthening of the right of a judicial remedy via an intermediate in camera *procedure*

Mr U was a collaborator in an authority, which was inter alia competent for the public procurement of military goods. Therefore, and with his consent, the intelligence service undertook a security screening of Mr U. As a consequence of the negative result of the security screening, Mr U was dismissed.

Mr U now wanted to have access to the files of the intelligence service in order to know on what facts the intelligence service had based its assessment. As the intelligence service refused to give access to the documents, Mr U challenged the refusal before the administrative courts. In the court proceedings, the intelligence service, on the basis of the former Section 99(1) Administrative Court Procedure Act, refused to submit the documents to the administrative court, as they were secret and their disclosure could cause inter alia the disclosure of the name of an informer. In accordance with the former Section 99(2) Administrative Court Procedure Act, the administrative courts, without having access to the documents, held that the intelligence service had furnished prima facie evidence that the disclosure of the documents could have the asserted negative effects.

---

[231] See the questionnaire and the answers given by Prof. Dr Bergmann, on file with the authors of the overall study.

[232] See the questionnaire and the answers given by Mr Kauß, on file with the authors of the overall study.

On the constitutional complaint of Mr U the Federal Constitutional Court held that Section 99(2) Administrative Court Procedure Act was unconstitutional, as it constituted a violation of the right of an effective judicial remedy, enshrined in article 19 par. 4 Basic Law (Federal Constitutional Court, 27.10.1999, 1 BvR 385/90). The Federal Constitutional Court obliged the legislator to introduce an intermediate *in camera* procedure, in order to balance the interest of the intelligence service and the citizen (see V.).

II. The constitutional right to be heard as a prohibition of closed material court procedures

In Germany, intelligence information can be used in court procedures like any other information. However, the information has to be formally introduced and revealed to all parties to the court procedures as German courts cannot base its judgments on secret information (see Federal Constitutional Court, 26.5.1981, 2 BvR 215/81). This follows from art. 103 par. 1 Basic Law,[233] which guarantees the right to be heard and from which the Federal Constitutional Court has deduced (1) a right of all parties of a court procedure to know all evidence on which the court envisages to base its judgment, and (2) a right to comment on all of this evidence.[234] As a consequence of the constitutional enshrinement of a right to be heard and the jurisprudence of the Federal Constitutional Court with regard to this fundamental right, closed material court procedures are not allowed in Germany and an introduction by the legislator would be unconstitutional.

III. The indirect use of intelligence information via second-hand evidence

As very often the intelligence services are reluctant to reveal the sources of their information, the introduction of intelligence information in court procedures turns out to be problematic. For this reason, documents or witnesses (e.g. informers of the intelligence services) regularly are not introduced directly to the court procedure, but the information is introduced, for example, by the testimony of an officer of the intelligence service, who reports from the secret documents or the cognition of an informer whose identity cannot be revealed.[235] The Federal Constitutional Court has accepted such use of second-hand evidence in court procedures as being no violation of the right to be heard, even if the first-hand evidence would have been unavailable for the very reason that the intelligence services did not give access to it (see Federal Constitutional Court, 26.5.1981, 2 BvR 215/81). Nevertheless, the Federal Constitutional Court held that the courts have to take both the lower probative force of second-hand evidence and the fact that in these cases neither courts nor the parties have the possibility to assess the reliability of the first-hand evidence (for example, through cross-examination of a witness). Thus the fair-trial principle obliges the courts to be particularly careful and critical when considering second-hand evidence. It is difficult to assess how the courts apply these constitutional standards in everyday practice, as this would require an in-depth analysis of the consideration of evidence in many judgments. In any case, it has to be stressed in this regard that German administrative courts and judges are bound by a duty to investigate the relevant facts and not to rely only on the information provided by the administration (see Section 86(1) Administrative Court Procedure Act[236]).[237] Furthermore, section 108(1) Administrative Court

---

[233] For an English translation of the German Basic Law see www.gesetze-im-internet.de/englisch_gg/.

[234] See the judgment of the Federal Constitutional Court cited above; see further Radtke/Hagemeier, in: Epping/Hillgruber (eds), *BeckOK GG*, Art. 103 par. 6-16 with more references.

[235] This is e.g. regularly the case if the expulsion of an asylum-seeker based on fundamentalist political activities is challenged before the administrative court. In these cases, the information on the fundamentalist political activities is regularly gathered by the intelligence services, very often with the help of informers, whose identity cannot be revealed. As a consequence, a civil servant of the intelligence service is invited to report in the oral proceedings from the file (for further information see the answers of Prof. Dr. Jan Bergmann, LL.M., Presiding Judge at the Administrative Court of Stuttgart, on file with the authors of the study).

[236] For an English translation of the German Administrative Court Procedure Act see http://www.gesetze-im-internet.de/englisch_vwgo/.

[237] This is highlighted by Prof. Dr. Jan Bergmann, LL.M. (see above).

Procedure Act enables the court to weigh the evidence[238] so that an indirect use of intelligence information which respects the fundamental rights of the claimant seems at least possible.

IV. Judicial control of the administrative refusal to submit secret documents – introduction of an intermediate *in camera* procedure

If the intelligence service or the Ministry of the Interior refuses to submit secret files or documents to the courts in order to prevent them from being disclosed in a court procedure, this refusal can be challenged before the Administrative Courts. Within such a procedure, the competent Higher Administrative Court can – on the claimant's request – assess the legality of the administrative refusal in an intermediate *in camera* procedure (Section 99 Code of Administrative Court Procedure). This procedure has been introduced to the Code of Administrative Court Procedure in order to strengthen the constitutional right to a judicial remedy, and as a consequence of a judgment of the Federal Constitutional Court (see Federal Constitutional Court, 27.10.1999, 1 BvR 385/90). It aims at balancing the interests of the claimant, in particular the effectivity of his claim, with the public interest of secrecy by giving access to the documents only to the judges of the Higher Administrative Court (not to the claimant) in order to enable them to fully control the refusal of the administration. However, it has to be stressed that if the refusal to disclose the document is considered legal by the Higher Administrative Court, the consequence is that the documents will not be introduced to the main proceedings. The Administrative Court, in turn, will not be able to base its judgment on this evidence.

V. "National security" as a reason for refusing access to intelligence information

As pointed out by Dr. Udo Kauß (a German lawyer and expert in the topic of intelligence services)[239] the most important grounds of refusal to give access to the documents of intelligence services in the Administrative Court Procedure Act, in the Freedom of Information Acts and in the Acts on the intelligence services can be classified into four groups: 1. information that is secret by nature, 2. the protection of informers, 3. the protection of state interests of the Federation or the federal states and 4. the protection of the effectivity of the intelligence services.[240] It is the grounds of refusal in number 3. which come close to a concept of "national security". In the words of Sect. 99(1) Administrative Court Procedure Act, access to administrative documents can be refused "if the knowledge of the content of these certificates, files, electronic documents or this information would prove disadvantageous to the interests of the Federation or of a Land". As the wording of this ground of refusal is rather broad, German courts and doctrine try to ensure a rather narrow interpretation by restricting the application of the ground of refusal to the disclosure of information which would prove disadvantageous to *important* interests such as, for example, the external and internal security or the existence or the functioning of the Federation or a federal state as such; furthermore, the realisation of the disadvantages has to be sufficiently probable.[241]

---

[238] "The court shall rule in accordance with its free conviction gained from the overall outcome of the proceedings."

[239] See the questionnaire on file with the authors of the overall study.

[240] See inter alia Sect. 99(1) Administrative Court Procedure Act, Sect. 3 of the Federal Freedom of Information Act (see an English translation under http://www.gesetze-im-internet.de/englisch_ifg/index.html), Sect. 15 Bundesverfassungsschutzgesetz.

[241] Rudisile, op. cit.; Posser, op. cit.

VI. The use of illegally gathered intelligence information

The use of illegally gathered information in criminal proceedings is one of the major issues of criminal procedural law in Germany.[242] The Federal Supreme Court developed a number of general principles on this topic, which also apply to the use of intelligence information. According to this jurisprudence, the importance of the rights of the accused which have been violated by the measure of information gathering have to be balanced with the importance of the general interest to fight crime. This means that the violation of important rights of the accused leads to an exclusion of the illegally obtained evidence if the concrete criminal offence is not particularly heavy. Furthermore, the fruit-of-the-poisonous-tree-doctrine only applies in very exceptional cases. As a consequence, the German police can use illegally obtained information as a starting point for further investigation and the information which is gathered in a legal way at a later point in time can be used in court proceedings.

VII. The protection of whistle-blowers and journalists

There are no general rules on the protection of whistle-blowers in Germany. With regard to intelligence information, civil servants are regularly under an obligation of secrecy. Only if the secret information causes a reasonable suspicion of a major criminal offence (e.g. murder, high treason) or a criminal act related to corruption is the civil servant allowed to inform the competent state authority (not the press). In contrast to this, the position of journalists has been strengthened by the Federal Constitutional Court (Federal Constitutional Court, 27.2.2007, 1 BvR 538/06) and the legislator. Editorial departments cannot be raided in order to identify the person who has informed the press and thereby breached his or her obligation of secrecy. Furthermore, since 2012 journalists can no longer be accused of complicity to a breach of the (civil servant's) obligation of secrecy when receiving and publishing secret information (see the modified Section 353b(3a) Criminal Code[243]).

---

[242] Mareike Rehbein (2011), *Die Verwertbarkeit von nachrichtendienstlichen Erkenntnissen aus dem In- und Ausland im deutschen Strafprozess*, Berlin: Duncker & Humblot.

[243] For an English translation of the German Criminal Code see http://www.gesetze-im-internet.de/englisch_stgb/.

References

Benedikt, Matthias, Geheimnisschutz im deutschen Verwaltungsprozess und im Verfahren vor der Unionsgerichtsbarkeit. Eine Untersuchung der Vorlage- und Auskunftspflichten staatlicher Stellen im gerichtlichen Verfahren, Baden-Baden 2013 (Nomos).

Greve, Holger, Korruptionsbekämpfung und Whistleblowing. Überlegungen zur Auflösung des Konflikts zwischen Transparenz und Datenschutz, Zeitschrift für Datenschutzrecht (ZD) 2014, p. 336 ff.

Gribbohm, Günter, Der Gewährsmann als Zeuge im Strafprozeß. Wege der neueren Rechtsprechung zur V-Mann-Problematik, Neue Juristische Wochenschrift (NJW) 1981, p. 305 ff.

Rehbein, Mareike, Die Verwertbarkeit von nachrichtendienstlichen Erkenntnissen aus dem In- und Ausland im deutschen Strafprozess, Berlin 2011 (Duncker&Humblot), Die Verwertbarkeit von nachrichtendienstlichen Erkenntnissen aus dem In- und Ausland im deutschen Strafprozess, Berlin 2011 (Duncker&Humblot).

Schmidt-De Caluwe, Pressefreiheit und Beihilfe zum Geheimnisverrat i.S. des § 353b StGB. Der Fall Cicero und die Entscheidung des BVerfG, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2007, p. 640 ff.

Soiné, Michael, Erkenntnisverwertung von Informanten und V-Personen der Nachrichtendienst in Strafverfahren, Neue Zeitschrift für Strafrecht (NStZ) 2007, p. 247 ff.

Trips-Herbert, Roman, Cicero, WikiLeaks und Web 2.0. Der strafrechtliche Schutz von Dienstgeheimnissen als Auslaufmodell? Zeitschrift für Rechtspolitik (ZRP) 2012, p. 199 ff.

Country Fiche: Italy

European Parliament study on "*National Security Exceptions and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges*"

Author: Arianna Vedaschi

(University of Bocconi)

This "country fiche" summarises the main findings and highlights the main issues underlined in the questionnaire filled in by the author.

KEY FINDINGS

- Art. 202 of the Italian Code of Criminal Procedure, as well as art. 41 of law 124/2007, provide that when a public servant is requested to testify on matters which he/she deems covered by the state secrets privilege, he/she is obliged to refrain from answering the questions or otherwise revealing the information at stake. Moreover, the Italian Code of Criminal Law severely punishes those who reveal state secrets or classified information.
- When such an issue is raised, the presiding judge must suspend the hearing and refer the matter to the Prime Minister. The Prime Minister's office has 30 days to confirm the information is secret (in which case the information will not be used as evidence). If not, the information will be used, applying ordinary evidentiary rules.
- If the existence of state secrets is confirmed and the judge considers the information essential for the trial, he/she will be forced to dismiss the case due to the state secrets privilege. If the judge considers he/she is able to decide the case without using the information at stake, the trial can proceed.
- If the public prosecutor or the judge considers the information to be illegitimately classified as a state secret, he/she can challenge the classification before the Constitutional Court, raising a conflict of powers with the Prime Minister.
- In the Abu Omar case, the Constitutional Court adopted (and confirmed in three successive judgments) a "weak syndicate" model. According to the court, government choices on national security and state secrets in particular cannot be subject to any judicial review, as they are of an essentially political nature and involve sensitive issues such as foreign relations and national defence. The court limited its oversight power to the formal scrutiny of the procedural rules governing the classification of documents and information as state secrets.
- Oversight procedures do exist with regard to the use (or misuse) by the government of the state secrets privilege. Beside the "judicial" review system via the Constitutional Court, law 124/2007 provides for a parliamentary oversight mechanism, assigned to the Joint Parliamentary Committee for the Intelligence and Security Services (COPASIR).
- The state secrets privilege cannot be invoked by the government if the COPASIR, with a majority of two-thirds of its members, decides to investigate the operations of the intelligence services in order to evaluate their compliance with the law.
- Neither the Joint Committee nor the Parliament can overturn the Prime Minister's decision to classify information and documents as state secrets.
- Italian law provides no proper definition of national security. However, a definition can be deduced from law 124/2007 and from the judgments of the Constitutional Court. Law 124/2007 lays down a number of critical matters the protection of which justifies the non-disclosure of information in order to protect the "security of the Republic". The Italian Constitutional Court interpreted the state secrets privilege as a legitimate "tool" aimed at protecting the supreme

interests of the State. In the Abu Omar case, the same Court seemed to take a step backward, scrutinising the use of secrecy with excessive caution and granting the executive very wide discretionary power.

- The *Datagate* scandal has had the positive effect of raising the level of public awareness of and concern about basic and fundamental rights such as the right to privacy and to a family life. This has led to widespread demands for stricter rules and greater accountability with respect to governments and intelligence agencies in particular. Such demands were clearly reflected by the recent CJEU judgment annulling the Data Retention Directive (2006/24/EC) on the basis of a proportionality test.
- The use of secret evidence in courts can be problematic, since such evidence relies on covert investigation activities carried out by intelligence agencies, without any of the guarantees provided by ordinary evidentiary rules within criminal investigations. No effective review is provided as to the methods used to collect such evidence before it is presented to the judge for his/her perusal. The question is quite clear: how can we consider a trial based on secret evidence "fair" if we cannot be sure that evidence was collected in a fair way?
- Clear evidentiary standards should be set with respect to secret evidence, and effective forms of oversight should be provided to ensure such standards are respected before a piece of evidence can be presented in a court of law.
- In conclusion, we consider it appropriate to completely exclude the use of secret evidence against the defendant in a court of law, thus safeguarding the rights of the defence and the right to a fair trial.

1) Methodological note.

Our whole contribution to this study is characterised by a rigorous scientific approach, focused on the ultimate aim of the research. Therefore, we have tried to offer an overview – as clear, objective and impartial as possible – of the Italian legal system with respect to secrecy, national security and the use of intelligence information, especially in the courts of law.

Our approach is based on an initial reading of the statute law followed by an examination of the interpretation of the legislation provided by the Italian courts in actual cases. We have based our answers to the proposed questions, first of all, on a thorough understanding of the legal and regulatory framework that directly affects the issues at stake. A merely normative approach would most probably not have served the purpose of the study and, ultimately, it would not be what was required of us. Consequently, we have striven to demonstrate how the Italian legal system works in practice by stressing the importance of judicial interpretation (especially in the case law of the Constitutional Court) and in legal administrative practices. Indeed, both the Constitutional Court and the other domestic courts have made an outstanding contribution to the regulatory framework, setting interpretative guidelines and balancing conflicting interests in a field as sensitive as that of national security. The "illustrative case" that we have chosen to analyse undoubtedly epitomises the current legal debate concerning state secrets and national security in general. Legal scholars interested in such matters, throughout the last decade, have mainly focused on this case and have thereby developed their analyses and theories. By following the stages of the case, we have had the chance to provide a useful and clear example of the "law in action", with all its highlights and still obscure areas. Section 5 of the Country Fiche, finally, gives us the opportunity to broaden our focus, summarising our point of view on the recent *Datagate* revelations in the US and its implications for the use of secret evidence in court. In particular, starting from the essential principles that inform modern judicial systems, we express our concern with regard to the indiscriminate use of intelligence documents and information in court, in the absence of appropriate procedural guarantees. We conclude by endorsing the choice made by the Italian legal system not to renounce its legal and judicial tradition, by avoiding the introduction of closed material proceedings within the Code of Criminal Procedure.

2) Please describe an illustrative case in your country that highlights the main issues at stake when dealing with secret information in courts.

While the use of classified material (secret evidence) in courts is extraneous to the Italian criminal law system,[244] the implications of state secrecy have raised a number of problematic issues with respect to criminal prosecutions, especially in the aftermath of the 9/11 attacks. The global fight against international terrorism and its following counterterrorism measures have also involved Italy due to the extraordinary rendition (ER) of a suspect terrorist carried out in a joint operation by the US Central Intelligence Agency (CIA) and the Italian Military Intelligence and Security Service (SISMI now AISE). Such a controversial case involved secret information in Italian courts called on to decide on the abduction of Nasr Osama Mustafà Hassan, known as Abu Omar and imam at a mosque in Milan. The case has attracted significant attention thanks to its international resonance: on 17 February 2003, the Muslim cleric and suspected terrorist was abducted by SISMI and CIA agents and then flown – through the Aviano (Italy) and Ramstein (Germany) NATO bases – to Egypt. There, according to his account, he was tortured and harshly questioned with respect to his alleged connections with al-Qaeda and jihadist groups.

Criminal investigations, led by the Office of the Public Prosecutor of Milan, resulted in a first judgment by the Criminal Court of Milan (Trib. pen di Milano, judgment 535/2009) that convicted CIA agents (directly or indirectly involved in the case) [245] of kidnapping and two SISMI agents for abetment. The then-head of the SISMI and another high-ranking officer of the Italian secret service were acquitted due to the existence of state secrets on the documents and information proving their involvement in the case. In fact, during criminal procedure and court hearings, Italian officers claimed the state secrets privilege.[246]

According to Art. 202 of the Italian Code of Criminal Procedure (CCP), as well as Art. 41 of Law 124/2007, when a public servant is requested to testify on matters which he/she deems covered by the state secrets privilege, he/she is obliged to refrain from answering the questions or otherwise revealing the information at stake. This duty is reinforced by the provisions (Arts. 261-262) of the Italian Penal Code that severely punish those who reveal state secrets or other classified information.[247] When such an issue is raised during a criminal proceeding, the Public Prosecutor or the judge is obliged to suspend the hearing and refer to the President of the Council of Ministers (PCM) on the issue of state secrecy.[248] Should the PCM officially confirm the information in question to be covered by the state secrets privilege, such information will not be revealed within the trial and as a consequence will not be admissible as evidence. By contrast, should the PCM deny the existence of the privilege (or remain silent within 30 days), the information will be used according to ordinary evidentiary rules. In case of confirmation, if the judge considers the information essential for the trial, he/she will be forced to dismiss

[244] As a general principle, in Italian criminal law, each and every piece of evidence which the Public Prosecutor or judge uses during a trial must be disclosed to the defendant and his/her defence counsel. No evidence can ground a judgment in a criminal court, unless it was disclosed to the defendant, for his/her perusal, in the course of the trial. Such principle stems from Art. 24 and Art. 111 of the Italian Constitution, which protect the right to defence and the right to a fair trial respectively (see questionnaire).

[245] Robert "Bob" Seldon Lady, Head of the CIA office in Milan. Jeff Castelli, then-head of the CIA office in Rome, was acquitted by the Criminal Court due to diplomatic immunity, but subsequently convicted by the Court of Appeal and the Supreme Court of Cassation. The Italian then-Minister of Justice, Roberto Castelli (centre-right) refused to demand extradition of the CIA agents convicted by the Criminal Court. His successor Clemente Mastella (centre-left) acted on the same line.

[246] Lt. Gen. Nicolò Pollari, then-head of the SISMI, and another high-ranking officer of the Italian secret service, Marco Mancini.

[247] Arts. 261 and 262 of the Italian Penal Code establish severe punishments for such a crime (see questionnaire).

[248] This procedure is provided by the same Art. 202 of the Italian Code of Criminal Procedure and Art. 41 of Law 124/2007.

the case due to the existence of state secrets. Conversely, if the judge considers the information to be non-essential, he/she can decide to proceed anyway, without the use of such information.[249]

However, if the Public Prosecutor or the judge does not agree with the confirmation of the PCM and considers the information to be illegitimately classified as a state secret, he/she can challenge such classification before the Constitutional Court by raising a conflict of powers against the PCM. Then, the Constitutional Court is called to assess the legitimacy of state secret claimed (whether the PCM had the legitimate power to classify as a state secret the information at stake).

The above-mentioned conflict of powers was raised by the Office of the Public Prosecutor of Milan in 2009, with regard to the existence of state secrets, claimed by the SISMI officers and then confirmed by the PCM in the *Abu Omar* case.

In a much-debated judgment (106/2009) the Constitutional Court ruled in favour of the PCM, upholding the legitimacy of the privilege claimed. In its reasoning the Constitutional Court adopted a formalistic and deferent approach, thus greatly limiting its own power of review. In fact, the Court limited its scrutiny merely to verify the correct application of the procedural rules. This self-restraint is due to the fact that the choices of the PCM on national security matters and state secrets in particular are of a political nature and involve sensitive issues which have an impact on foreign relations. In the words of the Court, the integrity of the Republic and its institutions, which the state secrets privilege is aimed at protecting, shall prevail over the need to investigate serious crimes and the attempt to seek convictions of those accused of criminal offences. Indeed, the Court went even further, by affirming the legitimacy of the secrecy claim, even if the information has already leaked. In the case at stake, the Court found that the procedural rules concerning state secrets have been respected and so upheld the legitimacy of the claimed privilege.

The decision of the Constitutional Court has been criticised by some scholars, who have argued the Court refused to play its proper role and exert the powers granted to it by law to ascertain the legitimacy of State secrecy by reviewing the decision of the PCM in order to verify its compliance with the law (Art. 39 Law 124/2007, which explicitly provides a number of situations in which State secrecy can be claimed) and in so doing discourage (at least indirectly) possible wrongdoings by government. This is not intended to restrict the discretionary power of the PCM on matters of national security but rather to avoid the totally arbitrary decision of the PCM on State secrecy, which could also have as a consequence the granting of immunity from prosecution to public servants (namely intelligence service members) accused of acting beyond any legal authority. By limiting its own power to effectively review the claim of State secrecy, the Constitutional Court opened a disturbing loophole in the "checks and balances" safeguards of the Italian Republic, leading to a lack of democratic accountability and negative effects on the rule of law.

In 2010, following the judgment of the Constitutional Court, the Court of Appeal of Milan confirmed (and strengthened) the convictions of the CIA agents, but it could not rule otherwise, accepting the argument of the state secrets privilege claimed by Nicolò Pollari and Marco Mancini (Corte App., sez. III pen., judgment 3688/2010).

In 2012 the Supreme Court of Cassation overturned the Court of Appeals' judgment and reinterpreted the judgement of the Constitutional Court, overcoming the severe limits imposed by constitutional judges with respect to the state secrets privilege (Cass., sez. V pen., judgment 46340/2012). The Supreme Court based its reasoning on the assumption that only documents and information related to legitimate intelligence actions can be classified as state secrets, since the state secrets privilege is aimed at protecting the integrity of the Republic and its institutions by concealing sensitive information relating to national security, defence and foreign relations. In the case in question, the PCM and the SISMI had always denied any official Italian involvement in Abu Omar's ER. Therefore, the Supreme Court argued that Italian officers involved in the case had acted without any official mandate. As a consequence,

[249] The same procedure is provided by Art. 256 of the Italian Code of Criminal Procedure, with regard to documents covered by the state secrets privilege. Public servants, requested to surrender such documents, must refuse such a request claiming the existence of the state secrets privilege, to be confirmed by the PCM within 60 days (see questionnaire).

information and documents related to their involvement in the case could not be classified as state secrets, since the state secrets privilege could not (in the opinion of the Supreme Court) be invoked properly. Ruling accordingly, the Supreme Court of Cassation annulled the Court of Appeals' judgment and ordered a new appeals trial to be held. Following the reasoning of the Court of Cassation, in 2013, the Court of Appeal of Milan sentenced Nicolò Pollari and Marco Mancini to 10 and 9 years in prison, respectively (Corte App., sez. IV pen., judgment 985/2013). The Italian government raised a new conflict of powers before the Constitutional Court, claiming the Court of Cassation – by means of its innovative judgment – had violated the PCM's constitutional authority with respect to the issue of state secrets. In 2014 the Constitutional Court,[250] once again, upheld the PCM's stance and reaffirmed its previous interpretation on the legitimate resort to the state secrets privilege. As a consequence, the Court of Cassation finally acquitted Pollari and Mancini (Cass., sez. I pen., judgment 20447/2014).

3) What are the bodies involved in the production and processing of secret evidence? Is there any oversight of the practices of the antiterrorist and (police-military) intelligence services that provide this evidence?

As previously stated, no secret evidence (i.e. evidence not disclosed to the defendant) is allowed within the Italian criminal law system. As a consequence, no antiterrorist practices can result in covert evidence useful for a trial.

However, Law 124/2007 (as revised by Law 133/2012) and the Italian Code of Criminal Procedure provide at least two kinds of oversight in relation to the state secrets privilege and, in particular, to those cases in which such privilege is claimed to avoid disclosure of information and/or documents during a trial. In practice, the state secret claim can be subjected to a judicial review and to a political oversight.

As regards judicial review, it must be underlined that only the Constitutional Court has this province. In *Section 1* and in the *Questionnaire*, we have already outlined the procedural sequence provided by the Italian Code of Criminal Procedure (Art. 202 and 256) and Law 124/2007 (Art. 41) on matters of state secrets. In particular, we have observed that the invocation of state secrecy during a trial must be properly confirmed by the PCM. This PCM's confirmation can be challenged before the Constitutional Court by the judge of the trial or the Public Prosecutor. It is worth remembering that the Constitutional Court enjoys full access to any document/information classified as state secret (Art. 202.8, 204.1-*quater* of the Italian Code of Criminal Procedure; Art. 41.8 of Law 124/2007), so it is in the best position to verify whether the state secret claim complies with the law. However, as the *Abu Omar* case has shown, the Constitutional Court envisages its review as limited to formal and procedural aspects, without any chance to test whether the PCM's decision was reasonable. This tendency effectively transforms the self-restraint of the Court into great deference to the government and in so doing the Court weakens its (effective) review.

Beside the judicial review, entrusted to the Constitutional Court, Law 124/2007[251] provides political oversight, assigned to the Joint Parliamentary Committee for the Intelligence and Security Services (*Comitato Parlamentare per la Sicurezza della Repubblica* – COPASIR). The Joint Committee – comprised of five members of the House of Deputies (*Camera dei Deputati*) and five members of the Senate (*Senato della Repubblica*) and chaired by a member of the parliamentary opposition – exerts general oversight powers over the intelligence and security services. With particular regard to the state secrets privilege, each time the PCM confirms the classification as state secrets of certain information or documents, he/she is obliged to promptly inform the Joint Committee (Art. 41.9 of Law 124/2007). The President of the Joint Committee has the power to summon the PCM to provide, within a secret hearing, each and every necessary piece of information to evaluate the merits of the case at stake.[252] Should the Joint Committee deem the confirmation of the classification as being illegitimate, the Joint Committee is entitled to inform the House of Deputies and the Senate, allowing them to take any appropriate measure.

---

[250] Judgment 24/2014.

[251] Arts. 30-31 and 32.

[252] This power was introduced by Law 133/2012.

In any event, the state secrecy privilege cannot be invoked by the government if the Joint Committee, with a majority of two-thirds[253] of its members, decides to investigate the operations of the intelligence services in order to evaluate their compliance with the law. If, on the one hand, quite pervasive powers are granted to the Joint Committee by the law, on the other hand neither the Joint Committee nor the Parliament can overturn the PCM's choice to classify information and documents as state secrets. While it certainly maintains its power to force the government to resign, it is unlikely Parliament will resort to such power as a consequence of a violation of Law 124/2007 or other provisions related to state secrets and national security as a whole.

Both kinds of oversight provided by the law, the one relying on the Constitutional Court and the other entrusted to the Joint Parliamentary Committee for the Intelligence and Security Services, have proven quite ineffective in restricting the wide discretion granted to the executive branch due, in the first case, to voluntary self-restraint and, in the second case, to a substantial lack of power to overrule PCM's decision.

4) The concept of national security: how is it framed and understood in your country? On what grounds do authorities in your country define national security and how is this connected to a right to secrecy in courts? Are there any secrecy claims that obstruct oversight?

As we had the chance to explain within the Questionnaire, no proper definition of "national security" is provided by Italian law. Nevertheless, with regard to the state secrets privilege, Art. 39.1 of Law 124/2007 sets out a number of critical matters whose protection justifies the non-disclosure of information/documents. In other words, in order to protect the "security of the Republic", the PCM can decide to keep information secret. Specifically, according Art. 39.1 such critical matters are: a) the integrity of the Republic; b) the defence of its underlying institutions as established by the Constitution; c) the Republic's independence vis-à-vis other States and its relations with them; d) military preparation and defence. However, according to Art. 39.11 of Law 124/2007, the state secrets privilege must not be invoked to conceal information, documents or matters concerning: a) acts of terrorism; b) acts subverting the constitutional order; c) acts constituting the criminal offences of devastation and ransacking (Art. 285 of the Italian Penal Code), mafia-style criminal organisation (Art. 416-bis of the Italian Penal Code), political-mafia exchange (Art. 416-ter of the Italian Penal Code) and mass murder (Art. 422 of the Italian Penal Code).

Such "definition" of national security (recte "security of the Republic") is not explicitly limited to the purposes of the intelligence services but can (and shall) be generally applied within the whole legal system.

With its judgments 82/1976 and 86/1977 the Italian Constitutional Court interpreted the state secrets privilege as a legitimate "tool" aimed at protecting the supreme interests of the State, thus granting its survival and integrity as a democratic community of individuals and not as "bureaucratic apparatus". However, with judgments 106/2009, 40/2012 and 24/2014, regarding the *Abu Omar* case, the same Court adopted a quite controversial approach, granting the executive branch a wide discretionary power with respect to national security and state secrets. In fact, within the broad definition outlined above, the government, acting by itself, is entitled to decide – case by case – what concerns national security (and shall be classified as a state secret), leaving to judicial review (by the same Constitutional Court) a merely formal role. As a consequence, the government enjoys the power – in cases relating to national security – to determine which information can be disclosed as evidence in court and which must be kept secret in the interests of the State (in the name of public security, with significant impacts on criminal prosecution and, ultimately, on the separation of powers).

[253] Such a majority was introduced by Law 133/2012. The previous rule provided for the Joint Committee to vote unanimously.

5) What are the procedural guarantees and the protection standards for the rights of the defence, the freedom of the press and the protection of whistle-blowers in your country concerning the use of secret evidence in courts?

Since no secret evidence can be used in court, this question cannot be referred to the Italian legal system.

6) In your view, how do the current debates over the issue of digital surveillance affect the use of secret evidence in courts as regards the practices of intelligence services that have been denounced?

The recent and very well-known digital surveillance scandal (the so called "*Datagate"*) has raised some major issues with respect to the protection of privacy and family life. In particular, intelligence agencies (such as the CIA, the NSA and GCHQ) have seemed to consider themselves somehow "above the law", within their data collection activities, gaining full access to virtually everyone's electronic communications, from ordinary citizens to prominent government officials of foreign allies. Revelations from the *Datagate* scandal have had – in our opinion – the undoubtedly positive effect of raising the level of public attention to and concern about basic and fundamental rights such as privacy, leading to a widespread demand for stricter rules and greater accountability in particular with respect to governments and intelligence agencies. People – and especially legal scholars – in democratic countries have started thinking that, given the sophistication of the technology available in the field of communication and the wide range of privacy violations that such technologies allow with relative ease, governments can no longer simply take the public's trust for granted. Instead, governments should enhance transparency, limit secrecy claims to the absolute minimum and provide effective forms of oversight. Such demands for a stricter scrutiny on intelligence activities, especially on data collection and data retention, was clearly reflected in the recent judgment of the European Court of Justice that declared invalid the much debated *Data Retention Directive* (2006/24/EC), basically due to a lack of proportionality between the purpose it was aimed at pursuing and the means set up to achieve such a purpose. Specifically, the Directive violated Arts. 7 and 8 of the EU Charter of Fundamental Rights.

In this regard, the use of secret evidence in courts raises more than mere concern, since such evidence relies on covert investigation activities carried out by intelligence agencies, without any of the guarantees provided by ordinary evidentiary rules within criminal investigations. It is quite clear to us that an essential precondition to admit the use of secret evidence in national security cases (even if we cannot endorse such use) is the good faith of governmental agencies involved in data collection and analysis, in terms of compliance with laws and fundamental rights. The *Datagate* revelations just showed the opposite. In this sense, the use of secret evidence in courts appears to be particularly worrying, since no real scrutiny and no effective review is provided as to the procedures adopted to collect such pieces of evidence before it is "packaged" for the judge's perusal. The question, in our opinion, is quite clear: how can we consider a trial based on secret evidence "fair" if we cannot be sure that evidence was fairly collected (i.e. in a manner that respects the law and fundamental human rights)? The answer obviously lies in procedural guarantees. If governments feel closed material proceedings are indispensable when it comes to national security, they should at least set clear evidentiary standards with respect to secret evidence and provide effective forms of oversight to ensure such standards are respected, before a piece of evidence can presented before a court during a trial.

As we have explained in several places above, the Italian legal system excludes absolutely the use of secret evidence. This is a rule that must certainly be endorsed since it respects fundamental constitutional principles, such as the right to a fair trial, which underlie democracy and the rule of law. Though still very far from perfect, the Italian legal system offers stronger guarantees to the defendant, as regards the basic right to be fully informed of the evidence supporting a criminal charge, stating clearly that the principle of personal freedom cannot be sacrificed in favour of national security. Even in the aftermath of 9/11, Italy did not take a step backward and, on the contrary, safeguarded full evidentiary disclosure as a cornerstone of democracy. Ultimately, in our opinion and for the reasons explained above, resorting to the use of secret evidence should be avoided within any modern judicial system, based on adversarial trials. Indeed, the recent *Datagate* scandal has done nothing but reinforce such an opinion.

References

Anzon Demmig, Il segreto di Stato ancora una volta tra Presidente del Consiglio, autorità giudiziaria e Corte costituzionale, Giurisprudenza costituzionale, 2009, n. 2, 1020;

F. Fabbrini, Understanding the Abu Omar case: The State Secret Privilege in a Comparative Perspective, paper presented at the World Congress of the International Association of Constitutional Law – Workshop No. 6, "The Rule of Law in the Age of Terrorism" – Mexico City, 6 December 2010;

F. Messineo, 'Extraordinary Renditions' and State Obligations to Criminalize and Prosecute Torture in the Light of the Abu Omar Case in Italy, in 7 Journal of International Criminal Justice 1023, 2009;

M. Nino, The Abu Omar Case in Italy and the Effects of CIA Extraordinary Renditions in Europe on Law Enforcement and Intelligence Activities, in 78 Revue Internationale de Droit Penal 113, 2007;

Pace, Le due Corti e il caso Abu Omar, Giurisprudenza costituzionale, 2014, 389;

Spataro, Abuse of state secrecy and national security, contribution to meeting in Tbilisi, September 2010 available at www.assembly.coe.int;

Vedaschi, Il segreto di Stato tra tradizione e innovazione: novità legislative e recenti evoluzioni giurisprudenziali, Diritto Pubblico Comparato ed Europeo, 2012, n. 3, 978-1012;

Vedaschi, La Cassazione solleva il "sipario nero" calato dalla Consulta: il caso Abu Omar si riapre, Percorsi costituzionali, 2013, n. 1, 163-193;

Vedaschi, Arcana Imperii and Salus Rei Publicae: State Secrets Privilege and the Italian Legal Framework, in D. Cole, F. Fabbrini, A. Vedaschi (cur.), Secrecy, National Security and the Vindication of Constitutional Law, Cheltenham (UK) & Northampton (US), Elgar Publishing Ltd, 2013, 95-111;

Vedaschi, Il segreto di Stato resta senza giudice, Giurisprudenza costituzionale, 2014, n. 1, 394-40

Vedaschi, Has the balancing of rights given way to a hierarchy of values?, Comparative Law Review, 2010, 1-40.

Country Fiche: Spain

European Parliament study on "*National Security Exceptions and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges*"

Author: Mar Jimeno Bulnes (University of Burgos)

This "country fiche" summarises the main findings and highlights the main issues underlined in the questionnaires filled in by the following experts:

- **José Ricardo de Prada Solaesa,** judge at the *Sala de lo Penal de la Audiencia Nacional de España*
- **Gonzalo Boyé Tusset,** human rights lawyer, Boye-Elbal y Asociados, Madrid
- **Mar Jimeno Bulnes,** Professor at the Faculty of Law of University of Burgos

KEY FINDINGS

- In Spain, secret information in court relates to the use of intelligence materials in order to incriminate people. These intelligence materials are considered expert evidence to be freely evaluated by judges and courts. Intelligence reports need to be presented in court but not necessarily by the authors of the reports.
- Currently intelligence materials are only used in specific criminal cases involving terrorism and organised crime.
- No secret evidence can be used in court. For this reason, intelligence must first be declassified; only the Council of Ministers is allowed to classify materials as secret. Two categories of classification exist: "secret" and "confidential".
- No definition of national security is given. Some legislation contains only a partial definition of 'classified materials'. The National Centre for Intelligence and Delegated Government Commission for Intelligence are two institutions dealing with national security.
- The Spanish Constitution provides for the right of defence in Article 24 under the title of 'fair trial', which has been interpreted on many numerous occasions in constitutional case law. Constitutional case law follows the legal interpretation provided by ECtHR.
- Nevertheless, practitioners and, specifically, defence lawyers argue that in practice the rights of the defence are not always observed in court; they complain that intelligence materials are introduced as "hearsay" and treated confidentially.
- Article 120 of the Spanish Constitution and Article 680 of the Act on Criminal Procedure regulate whether judicial proceedings are held in public. Trials can only exceptionally take place in camera. One of the reasons cited in the Act on Criminal Procedure is maintaining public order, where the concept of national security can be included.
- No definition of whistle-blower exists, but related information is contained in the Spanish Criminal Code.
- No specific provision on the use of technology and/or digital surveillance is included in ordinary criminal procedure legislation in Spain, although it does exist in judicial practice.
- Specific legislation has been enacted in order to make the use of digital surveillance evidence in court possible, but with no necessary link to the topic of secret evidence (or intelligence information).

1) Methodological note.

This present country fiche takes into account two main sources. First, the answers to the questionnaire by the author as expert academic (M. Jimeno-Bulnes) and two practitioners, one judge (*magistrado*) at the National Court (J.R. de Prada Solaesa) and a lawyer with relevant experience at the National Court (G. Boye Tusset), which has jurisdiction over aggravated crimes and those with an international connection, such as terrorism. Second, particular knowledge on the topic by the author has been added concerning the quotation of legislation, jurisprudence and literature. Appropriate mention of specific answers on the questionnaire and references has been included where necessary.

2) Please describe an illustrative case in your country that highlights the main issues at stake when dealing with secret information in courts.

Illustrative case: STS 2084/2001, 13 December (Supreme Court, Criminal Chamber. Judge rapporteur: Juan Saavedra Ruiz).[254]

This is an illustrative case because it was the first judgement pronounced by the Supreme Court dealing with intelligence information in criminal proceedings and its recognition as expert evidence. But many other judgments have been pronounced by the Supreme Court's Criminal Section in relation to the topic, some of them mentioned in answers to the questionnaire by the defence lawyer expert.[255]

INTRODUCTION: Judgement resolves the cassation appeal promoted by the defendants against their conviction by the National Court (Criminal Division, Section Three) on 20 January 2000. After conviction, three defendants were sentenced to 19 years in prison for committing a terrorist crime regulated in Art. 572 Criminal Code. The Supreme Court upheld their prior conviction but reduced their sentence to 18 years.

FACTS: The defendants belonged to Comando Araba, part of the ETA Basque terrorist organisation, which carried out the bombing of the Civil Guard barracks in Llodio (Vitoria, Basque Country) on 26 July 1989. In order to carry out this bombing, explosive material was moved by car to a sewer close to the main façade of the barracks. Bombing caused significant damage to the five-floor Civil Guard property (32,960,928 pts or 198,099,17 euros); to a neighbouring high school (816,579 pts or 4,907.74 euros); and to several Civil Guard and private vehicles parked in the area (28,315,426 pts or 170,179.14 euros).

LEGAL REASONING: Several reasons were alleged by the defendants to justify cassation according to requirements expressed in Art. 846 bis c) Act on Criminal Procedure (1882, henceforth LECrim), such as the violation of constitutional rules, especially Art. 24 Spanish Constitution (1978, henceforth CE), in the provision of effective judicial protection and due process of law as well as the infraction of other legal precepts contained in ordinary criminal procedural legislation. In relation with the topic of the study, the defendants' allegation is based on the violation of the presumption of innocence (ex Art. 24 (2) CE) and questioning the value attributed to certain reports on intelligence delivered by Civil Guard civil servants as incriminating evidence.

The Supreme Court adopted the same criterion as the National Court in order to evaluate whether the specific reports written by law enforcement authorities were expert evidence and not testimonial evidence. It was here recognised that the function of these police reports "is to relate different information, based on certain technical knowledge possessed by the Civil Guard, to draw conclusions, i.e. through all the information available to them (not only in this case but that which was derived from a myriad of police procedures and documentation); the Civil Guard comes to certain conclusions which are

---

[254] Information taken from M. Jimeno-Bulnes's questionnaire, para. 1.5. Source: Spanish General Council of the Judiciary official website (www.poderjudicial.es/search/index.jsp).

[255] Sentences pronounced on 1 October 2007, 10 December 2007 and 28 March 2012 according to information provided by G. Boye, paras. 1.1 and 1.3. By contrast, selected judgment belonged to the author of present country fiche, who also has dealt with both similar and different case law on the topic.

in turn applied to concrete actions. It is therefore expertise which links information in order to draw clear conclusions; under no circumstances could it be considered testimonial evidence".[256]

The Supreme Court also added statements in order to discern the concepts of expert and witness: "Expert evidence in the form of personal knowledge delivered in court constitutes a statement of knowledge by the expert proving that he can provide to the judge a number of technical, scientific, artistic or practical skills (Articles 456 LECrim and 335 LEC) with the objective of establishing a reality which the judge cannot directly observe (unlike witness testimony) and which is non-binding. The expert, by comparison to the witness, possesses technical, scientific, artistic or practical skills acquired prior to the process and indifferent to it (…). The witness testifies about past events related to the process and that he/she perceived with his/her senses, thereby being irreplaceable, having a passive position, as him- or herself is under review".[257] Also, the court justified the need to acquire such specific knowledge as a "means of assistance" when the judge cannot verify the truth of the facts on his or her own.

Lastly, it is argued that appropriate procedural requirements have been observed, such as the physical presentation of the reports by experts (354 pages), and the opportunity of the defence to confront. In fact, it is declared literally: "The impossibility of contradiction of the expert opinion cannot be invoked because what is involved here is the possibility given to the defence counsel to contradict this expert opinion, while the defence keeps open the aforementioned channel."[258]

Other cases in relation with the employment of intelligence materials in judicial proceedings to incriminate **people**:

All cases are judgments pronounced by the Supreme Court Criminal Chamber known by the initials STS and are available at http://www.poderjudicial.es/search/index.jsp.

Only cases where a conviction has been achieved are taken into consideration, as they have reached the Supreme Court; these include cases where police secret evidence has been used but not considered intelligence information. In sum, the Supreme Court evaluates on a case-by-case basis if the so-called intelligence materials are in fact intelligence expertise or just usual police information to be presented in court according to general requirements (testimonial evidence: declaration by police officers who elaborate reports as witnesses at the trial).

- STS 786/2003, 29 May 2003: The Supreme Court recognised the validity of the 'police intelligence evidence' in order to provide the judge with the appropriate technical knowledge according to Article 456 Spanish Act on Criminal Procedure. This was another case concerning ETA terrorism, and the National Court's conviction of the accused was upheld. As legal reasoning, prior STS 2084/2001 was employed.
- STS 655/2007, 25 June 2007: The conviction of five persons was confirmed by the Supreme Court in relation with membership in the GRAPO terrorist organisation. They presented a defence appeal in which they challenged the intelligence report, which included civil guards' but not the authors' signatures. Hearsay and intelligence reports were admitted. The judge did not evaluate whether the authors were experts or witnesses, considering this irrelevant because the criterion of free evaluation of evidence was applied.
- STS 480/2009, 22 May 2009: The famous Ekin case, where several Basque companies and enterprises linked to the ETA terrorist organisation were convicted of funding it. Again the Supreme Court recognised the validity of such intelligence reports, formally introduced in court by persons who were not their original authors. The evidence was presented in court by other police officers; the Supreme Court considered that all of them were working together as an official laboratory team. It implied the introduction of new evidence under the title of 'intelligence expertise', not (yet) provided by law.

---

[256] Para.11.VII; personal translation, unless otherwise indicated.

[257] Para.11.VIII.

[258] Para.11.IX.

- STS 290/2010, 31 March 2010: Five persons were convicted by Supreme Court decision of belonging to an illicit association that constituted a terrorist organisation. These were youth organisations such as Jarrai and Haika attached to ETA-KAS and Ekin. Prior case law such as STS 786/2003 was applied, considering the intelligence materials as intelligence expertise evidence, where ratification by all authors at the trial was not required as long as police forces (here considered law agencies) worked as a team of scientific police.
- STS 156/2011, 21 March 2011: In the Kalashov case, six members of a criminal organisation were convicted of money laundering. The employment of intelligence materials was justified on the basis of complex criminality, as it was an organised and transnational crime. It was argued that the impartiality of the scientific police was to be presumed on the basis of their status as a law enforcement agency.
- STS 1097/2011, 25 October 2011: One person was convicted of belonging to a terrorist organisation (Ekin) and the formal introduction of evidence was obtained under cassation to the Supreme Court. Nevertheless, judge Perfecto Andrés Ibañez dissented from the majority opinion, criticising its consideration of the intelligence evidence as 'expertise', at least in relation with the present cause. The intelligence reports were written and presented in court by civil guard agents.
- STS 697/2012, 2 October 2012: Four persons were convicted of belonging to ETA, a decision related to a terrorist attack that caused injuries to 95 persons, and obtained and ratified by the Supreme Court. There was only one brief comment in relation to the admission of intelligence materials as expertise. After this case, there are no more cases in relation to possible discussion of evaluation of such intelligence materials.
-

3) What are the bodies involved in the production and processing of secret evidence? Is there any oversight of the practices of the antiterrorist and (police-military) intelligence services that provide this evidence?

General regulation is only provided by pre-constitutional legislation, such as the Law on Official Secrecy (1968), which according to practitioners is insufficient and out-dated.[259]

According to Art. 4 Law 9/1968, 5 April, on Official Secrecy – amended on 11 October 1978, due to the enactment of the Spanish Constitution – qualifying materials as classified is the responsibility of the Council of Ministers (government) and the Assembly of State Chiefs (military authority). Only these authorities shall be responsible for declassifying materials, according to Art. 7. Qualification as classified materials must also indicate whether they are "secret" or "reserved", according to the required degree of protection (Art. 3).

Qualification of materials as classified shall be adopted by a "formal act";[260] this qualification does not affect the Parliament, which shall always have access to such information according to Art. 10. These specific rules are contained in Art. 11 Decree 242/1969, 20 February, implementing prior Law 9/1968. The same Decree established a deadline for classification, if possible (Art. 3), as well as custody, transfer and destruction of such classified materials qualified as "secret" or "reserved".

A current example of classified materials are those produced by the activity carried out by the National Centre of Intelligence (CNI), created by Law 11/2002 of 6 May 2002, on behalf of national security. According to Art. 5 (1) Law 11/2002, the CNI's "internal organisation and structure, methods and procedures, personnel, facilities, databases and data centres, information sources and the information or data that can lead to knowledge are considered classified information". Parliamentary control of CNI is provided according to Art. 11 and judicial control according to Art. 12 and specific legislation, such as Organic Law 2/2002 of 6 May 2002.

---

[259] Judge J.R. de Prada's questionnaire, para. 1.3.

[260] Usually a specific law under proposal by the government. Information taken from J.R. de Prada's questionnaire, para. 2.2.

Organic Law 2/2002 establishes administrative (and not judicial) proceedings for adopting measures affecting fundamental rights in order for CNI to carry out its function of intelligence gathering, e.g. intervention of communications which are protected by privacy rights. CNI must request specific authorisation to the appropriate judge (*magistrado*) of the Supreme Court, who is in charge of this issue and serves a five-year term upon nomination by the General Council of the Judiciary. The judge shall decide according to rules and deadlines in this specific legislation. This law amends the Act on the Judiciary (1985).

4) The concept of national security: how is it framed and understood in your country? On what grounds do authorities in your country define national security and how is this connected to a right to secrecy in courts? Are there any secrecy claims that obstruct oversight?

According to legal rules there is no common concept and/or definition of national security. Only indirect references are contained in certain specific pieces of legislation that are more related to home affairs than to justice issues. For example, Art. 2 prior Law 9/1968 on Official Secrecy declares that "for the purposes of this Act, any issues, events, documents, information, data and objects that could damage or threaten the safety and defence of the State should their existence be made public, may be declared 'classified materials' ['materias clasificadas']". Consequently, the adoption of such classified materials in court requires a declassification proceeding by the same authority that had classified them;[261] this authority is in practice the national government, according to specific legislation such as Law 11/2002.

Art. 1 Law 11/2002, 6 May, on regulation of the National Centre of Intelligence (CNI), establishes CNI as the public institution charged "to provide the Prime Minister and the government with information, analyses, studies or proposals to prevent and avoid any danger, threat or aggression against the independence or territorial integrity of Spain, its national interests, and the stability of the rule of law and its institutions". Further, Art. 3 Law 11/2002 declares that "the government shall determine and approve annually the objectives of the National Intelligence Service by Directive, which is to be kept secret"; this annual programme is called the Intelligence Directive.

The same law provides in Art. 6 for the creation of a Delegated Government Commission for Intelligence. This commission "shall be presided over by the Deputy Prime Minister and composed of the Ministers of Foreign Affairs, Defence, Home Affairs and Economy and by the General Secretary of the Presidency, the Secretary of Security and the Secretary of the State Director of National Centre of Intelligence, who shall act as Secretary". It shall "ensure the proper coordination of all information and intelligence services of the State in order to create a community of intelligence". Its concrete tasks shall be: "a) propose to the Prime Minister the annual objectives of the National Centre of Intelligence (CNI), which shall integrate the Intelligence Directive; b) monitor and evaluate the development of CNI's objectives; c) ensure coordination of the CNI, the information services provided by the Forces of State Security and the organs of civil and military administration".

No legal provision on decisions about national security exists. As indicated above, provisions only relate to the qualification of certain information as 'classified materials' and further as either "secret" or "reserved" according to their relevance and their need to be protected. At the moment, these classified materials must conform to common rules on evidence according to the Act on Criminal Procedure and constitutional jurisprudence in interpretation of the fair trial rules (Art. 24 CE) if they are introduced in court and evaluated as evidence. In this context, the possibility of confrontation by defence counsel must be guaranteed, although it does not mean that in practice it must take place according to the case cited above.

Neither Organic Law 2/2002 nor Law 11/2002 addresses a specific declassification procedure of classified materials; in judicial practice, common proceedings before administrative courts must be used prior to criminal procedure.[262] It has been argued that a recent missed opportunity to provide such a

[261] G. Boye's questionnaire, para. 2.1.

[262] G. Boye's questionnaire, para. 2.2. and 2.3.

proceeding was the recently enacted (2013) Law on Transparency;[263] this specific legislation addresses the right to have access to public information, although its effect is absent in practice due to various limitations contained in Article 14, national security included. For all these reasons there is no general practice allowing for classified materials in court.[264]

In sum, there is not yet – according to legal rules – the resources to include closed materials in court in relation to parties of the criminal proceeding. However, exceptional rules contained in the Constitution (Art. 120 CE) and ordinary criminal procedural legislation (Art. 680 LECrim) can be invoked to restrict publicity to third parties and the public during the trial. In these cases, the trial shall take place in camera but always in the presence of the parties, prosecution and defence counsel.

Nevertheless, according to practitioners' opinions, there are informal resources to provide information to the court via indirect channels and pre-trial investigation.[265] Such information or materials are afterwards subject to police preliminary investigations. Specifically, it is the police activity carried out under this investigation which is later introduced in court as evidence.

Lastly, at the present time, the concept of national security has been subject to recent political debate regarding the accountability of national government and intelligence service practices in connection with the Snowden case. In Spain, due to the leaks involving Snowden, the highest authority of the Spanish secret services was summoned to appear before the appropriate commission of the Spanish Parliament in order to provide explanations. But no real debate has been generated in Spain in comparison to other countries.[266]

5) What are the procedural guarantees and the protection standards for the right of the defence, the freedom of the press and the protection of whistle-blowers in your country concerning the use of secret evidence in courts?

The right of defence is addressed in general for all procedures (civil, criminal, administrative, labour…) in Art. 24 CE: "1. Every person has the right to obtain the effective protection of the judges and the courts in the exercise of his or her legitimate rights and interests, and in no case may he go undefended. 2. Likewise all persons have the right of access to the ordinary judge predetermined by law; to the defence and assistance of a lawyer; to be informed of the charges brought against them; to a public trial without undue delays and with full guarantees; to the use of evidence appropriate to their defence; to not make self-incriminating statements; to not declare themselves guilty; and to be presumed innocent".[267]

Numerous relevant instances of case law have been pronounced by the Constitutional Court regarding these prescriptions according to interpretation provided by the ECtHR in relation to Art. 6 ECHR. Also, violation of these constitutional courts can be alleged anytime in any sort of appeal before all judges and courts belonging to any jurisdiction according to the general rule contained in Art. 5 (1) Act on the Judiciary. Lastly, Art. 24 CE belongs to the catalogue of fundamental rights provided in Arts. 14-30 CE, which can be subject to special remedy before the Constitutional Court after ordinary appeals (ordinary appeal and cassation); after that, only defence appeal before the ECtHR is possible.

Nevertheless, defence lawyers have argued that the right of defence in criminal procedure is violated in practice when procedural parties have no access to specific information provided by intelligence services and/or authorities.[268] In practice, this intelligence information is introduced at the trial by a police authority who has not dealt directly with such information and whose declaration is considered "hearsay". Additionally, such information is considered 'confidential' and, in this context, accepted as

[263] Law 19/2013, of 9 December, on Transparency, access to public information and good government.

[264] G. Boye's questionnaire, para. 2.4.

[265] J.R. de Prada's questionnaire, para. 1.6.

[266] G. Boye's questionnaire, para. 1.4.

[267] Official translation available at www.congreso.es/constitucion/ficheros/c78/cons_ingl.pdf.

[268] G. Boye's questionnaire, para. 1.1., 1.5. and 1.6.

valid evidence without being properly presented in court. Discussion also ensues related to the qualification of this concrete evidence, either as expertise or testimony; discussion was exposed in relation with the case indicated in Section 1. Last and even more controversial is the issue of what is called under judicial practice 'judicial private knowledge', defined as the private and personal knowledge of the judge, which cannot be contradicted (because it stems from a judicial authority) and is not considered as evidence per se. According to defence lawyers,[269] this judicial practice is also employed in order to introduce extra-procedural facts and data at the trial.

Freedom of the press in relation with the use of secret evidence in courts can be underlined under Art. 120 (1) CE, which declares "judicial proceedings shall be public, with the exception of those provided for in the law of procedure". In Spanish criminal procedure, general rules affecting the access of the press to judicial proceedings are contained in Art. 301 LECrim regarding the secrecy of the pre-trial investigation ('*secreto de sumario*') and Art. 680 LECrim regarding the publicity of the trial. Nevertheless, Art. 680 LECrim addresses the possibility of restricting such publicity during the trial on a case by case basis under judicial order by president of the court because of reasons of "morality and public order as well as the respect due to the victim ["*persona ofendida*"] or his family". Judicial order in relation with such restriction of publicity for the trial can be adopted ex officio or ex parte (defendant) and shall require the deliberation between the judges of the court. Also, relevant and extensive constitutional case law has been pronounced, taking into account the jurisprudence pronounced by ECtHR on the topic.

Lastly, there is no definition of whistle-blower is Spanish law. But related information is contained in the Spanish Criminal Code in relation to specific offences, such as Arts. 376 and 579 (4). In both cases reduction of punishment is provided to those persons who have abandoned criminal activities and have cooperated with (police) authorities in order to prevent crimes, obtain relevant evidence, make possible the capture of other responsible persons or impede the development of criminal organisations to which they belonged.

Protection of whistle-blowers in Spanish criminal procedure can only take place through the application of specific legislation on protection of witnesses and experts; this is Organic Law 19/1994, of 23 December, on the protection of witnesses and experts in criminal proceedings. It provides different degrees of protection under judicial order, ensuring anonymity via absence of visual identification at the trial and other means. In general, according to judicial practice, such specific legislation is not subject to much contention,[270] but in some cases, if employed, it has been applied in relation to whistle-blowers; an example is the Lasa and Zabala case, ruled by the National Court (Criminal Division) on 26 April 2000.

In this case, certain members of specific Spanish police forces (Civil Guard) in Basque Country were condemned for the assassination of two members of the ETA terrorist organisation who were refugees in France, José Antonio Lasa and José Ignacio Zabala. They were kidnapped and transferred to Spain by car and arrested on charges of bombing Civil Guard barracks in Basque Country. Remains of their bodies were found years later on the Mediterranean coast, covered with soil and quicklime; it was proved that both of them were blindfolded, bound, gagged and shot. The judicial decision condemned to 28 years of imprisonment the five accused persons on charges of assassination and illegal arrest; the defendants belonged to the police forces and GAL (Grupos Antiterroristas de Liberación). In order to obtain convictions, it was essential to declare witness number 2346 a protected witness.[271]

Another well-known case is the Marey case, ruled by Supreme Court on 29 July 1998 and confirmed by the Constitutional Court on 16 March 2001 as well as the European Court of Human Rights on 16 April 2010. This case concerned the kidnapping of Segundo Marey by GAL, which was promoting the 'dirty war' (*guerra sucia*) against ETA terrorism; in fact, GAL erroneously identified Segundo Marey as an ETA terrorist. Prominent Spanish politicians, such as José Barrionuevo, the Minister of Home Affairs in Felipe González' government, and his Secretary of State, Rafael Vera, were convicted as participants, as

---

[269] Ibid., para. 1.7.

[270] Ibid., para. 3.1.

[271] M. Jimeno-Bulnes's questionnaire, para. 3.3. A film concerning these facts and this case has been recently presented in the San Sebastián Cinema Festival under the title "Lasa and Zabala" (2014).

they had been informed of the existence of this terrorist group, which had been condemned after a prior conviction by the National Court of ex-police authorities (José Amedo and Michel Domínguez) on 9 September 1991, who acted as whistle-blowers in the Supreme Court case. Also relevant was the request by the Supreme Court for the declassification by the government (at the time under the presidency of José María Aznar, conservative party or PP) of 13 secret documents.

A more recent case is the Falciani case,[272] which concerned national security-relevant economic information related to Switzerland. In this context, Spain dealt with the extradition proceeding of Hervé Falciani, whose surrender was requested by Swiss judicial authorities and denied (as it was an extradition process) by Order 19/2013 pronounced on 8 May 2013 by the National Court, Criminal Section. The defendant worked as a computer programmer in a Swiss bank and was accused of economic espionage; according to Swiss authorities, Falciani employed data-mining in order to provide secret information on personal data to other banks and services with the result of violating bank secrecy. Spanish judicial authorities rejected the extradition request due to the lack of a double incrimination requirement, under the consideration that, according to Spanish legislation, "secrecy is not a concrete value to be protected but an instrument in order to protect real legal values and goods".[273] In this case, there was sufficient proof of serious illegal activities and the accused cooperated with administrative and judicial authorities, making it possible to investigate crimes in several countries. In sum, the requested person here acquired the role of a whistle-blower.

6) In your view, how do the current debates over the issue of digital surveillance affect the use of secret evidence in courts as regards the practices of intelligence services that have been denounced?

There is a specific constitutional provision in relation with the employment of computer technology affecting the right of privacy: Art. 18 (4) CE, which states, "The law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights".

Nevertheless, no specific provision on the employment of technology and/or digital surveillance is included in ordinary criminal procedure legislation, such as LECrim, although in judicial practice it does exist, e.g. in relation to intervention in communications per Art. 579 LECrim (only post, telegraphic and telephone communications are specified). Some additional legislation has been enacted, making it possible to intervene in digital communications and video surveillance, which afterwards shall be evaluated as evidence at the trial.

In this context, Art. 1 Law 25/2007, 18 October, on retention of data relating to electronic communications networks and public communication, imposes retention on telecom operators (wire, mobile and Internet) in order to make data available to police forces under judicial authorisation in relation with ongoing criminal investigations. Telecom operators have to retain such data for 12 months following the communication, and according to Art. 5 the judicial authorisation should determine the date on which the order is delivered to the police authorities as referred in Art. 7 of the same law. Nevertheless, this legislation implements the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, which has been recently declared invalid by the Court of Justice of the European Union in the famous case Digital Rights Ireland judged on 8 April 2014 (joined cases C-293 and C-294/12); for this reason its future is uncertain.

This is also the case of Organic Law 4/1997, 4 August, regulating the installation of video cameras (fixed and mobile) by law enforcement authorities in public spaces, which requires prior authorisation by administrative authority. Nevertheless, prior to this authorisation, a report by a specific committee under the President of the Regional Supreme Court shall be required. Final administrative resolution must determine the concrete public space where such a video camera shall be located. The enforcement of the

[272] J.R. de Prada's questionnaire, para. 3.3., and G. Boye's questionnaire.

[273] Para. Segundo II.j) in relation with the review of extradition requirements. Judge rapporteur of present decision was J.R. de Prada.

principle of proportionality is assured and images must be destroyed after one month, except when they are related to serious administrative infractions, criminal acts or ongoing police investigations or administrative/judicial proceedings.

In both cases, ordinary rules in relation to evidence must be applied if information derived from such digital intervention or video surveillance is introduced in court, which means that it has to be presented as proper evidence under the principles of contradiction and publicity. Introduction usually takes place during testimony by police, who have carried out a proper investigation and produced evidence related to the specific criminal case. Again, there is no legal possibility in Spain for the employment of secret evidence in court and, at the moment, no special legal provisions on the basis of intelligence services is foreseen.

References

R. Castillejo Manzanares (2011), "La prueba pericial de inteligencia", Diario La Ley, 16 December, no 7756 (http://diariolaley.laley.es).

E. De Llera Suárez-Bárcena (2013), "La utilización de la información policial y de los servicios de inteligencia como prueba en el proceso penal", Diario La Ley, 19 December, no 8215 (http://diariolaley.laley.es).

M. de Prada Rodriguez & J. Santos Alonso (2012), "La valoración de la prueba en los delitos de terrorismo: los informes de inteligencia", in J. Pérez Gil (ed), *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*, Madrid: La Ley, pp. 87-106.

F. Gudín Rodriguez-Magariños (2009), "La presunta prueba policial de inteligencia: análisis de la STS de 22 de mayo de 2009", La Ley Penal, no 64 (http://revistas.laley.es).

S. Guerrero Palomares (2011), "La denominada 'prueba de inteligencia policial' o 'pericial de inteligencia'", Revista Aranzadi de Derecho y proceso penal, no 25, pp. 75-91.

J.J. Hernández Domínguez (2013), "Valor procesal del informe de inteligencia policial", Diario La Ley, 21 October, no 8174 (http://diariolaley.laley.es).

M. Jimeno-Bulnes (2004), "After September 11th: the fight against terrorism in national and European Law. Substantive and procedural rules: some examples", *European Law Journal*, vol. 10, no 2, pp. 235-253.

J.A.E. Vervaele (2012), "Medidas de investigación de carácter proactivo y uso de información de inteligencia en el proceso penal", in J. Pérez Gil (ed), *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*, Madrid: La Ley, pp. 27-85.

Country Fiche: The Netherlands

European Parliament study on "*National Security Exceptions and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges*"

Author: Anja Wiesbrock

(University of Oslo)

This "country fiche" summarises the main findings and highlights the main issues underlined in the questionnaires filled in by the following experts:

- **Constant Hijzen**, University of Leiden
- **Wil van der Schans**, Investigative Journalist
- **Anja Wiesbrock**, University of Oslo

KEY FINDINGS

- The "Act on Shielded Witnesses" (*Wet afgeschermde getuigen*), introduced in 2006, permits the use of secret information originating from intelligence services as well as the hearing of intelligence officers as shielded witnesses in criminal procedures on the basis of national security concerns.
- It is the intelligence services themselves who have the authority to define the concept of national security.
- The ex parte and in camera procedure before the examining magistrate (who is restricted in his examination by the officer's duty of secrecy) and reliance upon the transcript as evidence while the trial judges are unable to examine the witness, pose a challenge to the right to a fair trial under Article 6 ECHR.
- Even though the Minister of Internal Affairs, a special parliamentary committee (CIVD) and an independent supervisory committee (CTIVD) are supposed to guarantee the accountability of intelligence services, in practice there is little oversight and control, in particular due to the close cooperation and exchange of information between the AIVD and the public prosecutor as well as the presumed legitimacy of information provided by the intelligence services.
- There are currently no specific procedures under national law to protect the freedom of the press and whistleblowers and several cases before the European Court of Human Rights illustrate the danger of national authorities abusing the possibility of using special powers and requesting the surrender of journalist sources and documents without providing sufficient reasons.

1) Methodological note.

This country fiche has been prepared on the basis of the information contained in the stakeholder questionnaires and after a careful examination of the relevant national legislation, case law and literature. The relevant legislation can be found on this official website of the Dutch government: http://wetten.overheid.nl/. Furthermore, I have made use of the website www.rechtspraak.nl in order to search for relevant cases, where secret information obtained by intelligence services played a role. Moreover, I have looked at the material provided by the intelligence service (AIVD) itself, in particular the yearly reports and the national security strategy. A further important source of information has been implementing reports commissioned by the Ministry of Justice, such as the final report on the Protected Witnesses Act by R.J. Bokhorst (*De Wet afgeschermde getuigen in de praktijk*, 2012). I have also studied newspaper articles and the relevant literature on the topic both in Dutch and in English, such as the book

by Marlies Zevenhuizen (2007) "*De afgeschermde getuige: Steunpilaar van staatsveiligheid of struikelblok in Straatsburg?*" and various publications by Quirine Eijkman.

2) Please describe an illustrative case in your country that highlights the main issues at stake when dealing with secret information in courts.

An important case regarding the tension between the use of secret information from intelligence services in criminal and civil procedures and the right to a fair trial was decided by the Administrative Division of the Council of State in November 2011 (ABRS 30 November 2011, LJN BU6382, AB 2012/142).

The applicant had successfully applied for a function at an airport, but his contract ended once it became clear that he would not be granted a certificate of no objection (*verklaring van geen bezwaar*) by the Interior Minister. The certificate was refused on the basis of information from the intelligence service (AIVD). The applicant did not have the possibility to see the information and was therefore not able to defend himself. This procedure was based on Article 87(1) Wiv in conjunction with Article 8:29(1) Awb.

The applicant's appeal against the decision was dismissed by the district court, but at the final instance the Administrative Division of the Council of State decided in favour of the applicant and found that his right to access to court under Article 6 ECHR had been violated.

Under the General Administrative Law Act, parties who are obliged to provide information or submit documents may, if there are compelling reasons, refuse to provide such information or submit such documents or inform the court that it alone may take cognisance of the information or documents concerned. It is for the court to decide whether the refusal or restriction on the cognisance is justified. However, the Intelligence and Services Act 2002 provides that where cases were covered by that Act, as the present case was, only the intelligence service and not the court could decide on that justification.

The Administrative Division of the Council of State cited case law from the European Court of Human Rights, holding that this case law relating to the right to adversarial proceedings in criminal law disputes is also relevant to cases concerning the determination of civil rights, such as the present case. Should national security be at stake, refusals to provide information or to submit documents are only justified if the court has jurisdiction to adjudicate their necessity and justification, taking into account the nature of the matter concerned and the residual options available for parties to obtain the information required. In the light of recent case law from the European Court of Human Rights, the Administrative Division of the Council of State did not follow its own previous case law, but held that it could not give judgment on the basis of evidence without first reviewing the necessity and justification for the Minister's refusal to provide the information requested by the applicant.

The Administrative Division of the Council of State therefore held that in this case the relevant provision of the Intelligence and Services Act 2002 could not be applied, since it was not in conformity with Article 6 ECHR and that the regular provisions of the General Administrative Law Act should instead be applied. It reopened the examination of the case in order to decide on the justification of the restriction on cognisance.

This case thus clarified that it must always (in criminal, civil and administrative law) be up to the court to decide on the possibility of a closed materials procedure by balancing the interest in state security with the procedural interests of the individual concerned.

3) What are the bodies involved in the production and processing of secret evidence? Is there any oversight of the practices of the antiterrorist and (police-military) intelligence services that provide this evidence?

The AIVD and the MIVD are responsible for the production and process of secret evidence. A major task of the AIVD is to carry out investigations relative to organisations and persons who, by the aims which they pursue or their activities, give rise to serious suspicion that they constitute a danger to the continued existence of the democratic legal order or to the security or other weighty interests of the State (Section 6(2) Wiv). It also has the task to promote measures for the protection of those interests, including

measures aimed at securing information which needs to be kept secret in the interest of national security. In carrying out those tasks, the service may make use of special investigative powers. The service may use nearly all means: monitoring, observing, telephone tapping, etc.

One key element of the Dutch antiterrorism strategy has been to increase the cooperation and exchange of information between the intelligence services and the judiciary. The adoption of the Act on the Criminal Investigation of Terrorist Crimes not only increased the investigative capacities of the criminal investigation, but also stimulated the transfer of information from the AIVD to the public prosecutor at an earlier point in time. The police and judiciary can thus use the AVID official message as a starting point for a criminal investigation. Since the entry into force of the Shielded Witnesses Act in 2006 AIVD official reports can also be used as evidence in court. Not only AIVD information has been accepted as a source of evidence, but also information from foreign intelligence services and intelligence collected by international intelligence gathering bodies. Moreover, the Shielded Witnesses Act provides for the possibility of hearing AIVD officers as shielded witnesses on the basis of national security concerns.

Moreover, the courts have played an important role in accepting the use of AIVD reports as starting information for a criminal investigation and as evidence in criminal trials. The Supreme Court accepted for the first time in *Eik* that an AIVD report could establish a reasonable suspicion of a crime having been/being committed. In the well-known terrorism case of *Piranha*, decided in 2008, both the district court and the Court of Appeal approved that the initial criminal investigation activities were based upon official reports by the AVID, which can establish a reasonable suspicion. There are, however, certain restrictions. The Supreme Court held in 2008 in a case involving a terrorist threat that an anonymously provided tip to the AIVD was insufficient to establish reasonable suspicion, especially since the checking of the information by the public prosecutor and the police did not establish any additional incriminating information (HR 11 March 2008, NJ 2008, 328, para 3.4).

The minister of internal affairs is responsible for the oversight of the AIVD. The service reports to the minister, who in turn is accountable to the Lower House of Parliament. The Parliament has a separate commission (*Commissie voor de Inlichtingen- en Veiligheidsdiensten*, CIVD), which gets to see secret information from the intelligence service and on this basis exercises parliamentary control. Since the entry into force of the new Intelligence and Security Act (WIV) in 2002, an independent supervisory committee appointed by the Second Chamber (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*, CTIVD) oversees compliance with the WIV. However, this committee does not report in public to the Second Chamber on a regular basis.

As pointed out by Wil van der Schans in his questionnaire, in practice there is very little oversight of intelligence services that provide evidence to be used in court. After having received an official report (*Ambtsbericht*) from the AIVD with the relevant information, the Public Prosecutor on Counter-Terrorism has the task of analysing all the relevant information, before a criminal investigation is initiated. Yet it appears from the case law that the extent to which the public prosecutor has to check the information collected by the AIVD is very limited. Since the AIVD is already monitored in other ways, the public prosecutor is supposed to presume the legitimacy of the information provided by the intelligence services, unless the information has been obtained unlawfully.

4) The concept of national security: how is it framed and understood in your country? On what grounds do authorities in your country define national security and how is this connected to a right to secrecy in courts? Are there any secrecy claims that obstruct oversight?

The concept of national security is not specifically defined in legislation, but the Council of State in its case law has emphasised the responsibility and discretion of the AIVD in deciding what constitutes a threat to national security (Raad van State, 04-07-2006, 200602107/1). The Law on the Intelligence and Security Services Act 2002 states that Intelligence and Security Services perform their duties in the interest of national security and it is the responsibility of the Intelligence Service (AIVD) to investigate the possible existence of a threat to national security. According to the AIVD the concept is best understood by looking at those issues that are considered to pose a threat to national security, as specified in its annual report. These include, for example, terrorist violence, the proliferation of weapons of mass

destruction or espionage activities (see for the latest report AIVD, Jaarverslag 2013). According to the National Security Strategy (*Strategie Nationale Veiligheid*) published in 2007, national security is at stake when one or more of the country's and/or society's vital interests are threatened to such an extent that potential societal disruption could occur. These interests are: territorial security, economic security, ecological security, physical security and social and political stability. Thus the intelligence services have great discretion in defining the concept of national security.

The concept of national security plays a major role in justifying the use of secret information in criminal procedures under the "Act on Shielded Witnesses" (*Wet afgeschermde getuigen*) which was introduced in 2006. In order to protect national security, the special examining magistrate (*rechter-commisaris*) may withhold certain information from the public domain (Amendment to Article 187d CPC). This means that this specific information is not disclosed to participants in the criminal process or the public. Moreover, the examining magistrate may decide, again in the interest of national security, to hear the intelligence officers as shielded witnesses in the specialised court in Rotterdam. In most cases the procedure is *ex camera* and *ex parte*, as a list of questions for the witness is handed to the special magistrate by the council representing the suspect and the trial judge, for whom the hearing is shielded. The report of the hearing will only be submitted to the parties with the consent of the shielded witness. No recourse is open to the decision to grant anonymity. Parties cannot appeal to the Court of Appeal or to the Supreme Court.

5) What are the procedural guarantees and the protection standards for the rights of the defence, the freedom of the press and the protection of whistle-blowers in your country concerning the use of secret evidence in courts?

The procedural guarantees and the protection standards for the rights of the defence under the Shielded Witnesses Act are limited. The defendant has limited opportunities to test the witness's reliability, due to the general non-disclosure of intelligence and information concerning the officer's identity, the duty of secrecy and the mandatory consent of the officer before the transcript is submitted to the defence. In addition, the examining magistrate's and the trial judge's assessment of the witness's credibility is restricted by the duty of secrecy of the officer and by having to rely exclusively on the transcript (the trial judge). As mentioned above, no recourse is open to the decision to grant anonymity. Parties cannot appeal to the Court of Appeal or to the Supreme Court. Hence the *ex parte* and *in camera* procedure before the examining magistrate, who is restricted in his examination by the officer's duty of secrecy, and reliance upon the transcript as evidence while the trial judges are unable to examine the witness, pose a challenge to the right to a fair trial under Article 6 ECHR (see also the stakeholder questionnaires). The courts are required to examine in each individual case whether to admit secret evidence, after verifying whether the far-reaching restrictions on the rights of the defence have been compensated for by the judicial procedure followed. However, overall the regime does not impose the proper checks and balances to compensate the significant restrictions that are inherent to the shielded witness's regime.

There are no specific procedures under national law to protect the freedom of the press and whistle-blowers, but the European Convention on Human Rights has turned out to be an effective tool in this regard. The Netherlands does not have legislation ensuring the right of journalists to protect their sources, but this right can be invoked under Article 10 of the European Convention on Human Rights. A well-known recent example was the case of two journalists of the daily newspaper *De Telegraaf*, who were imprisoned in 2006 for refusing to reveal their sources in the case of an intelligence service agent who was suspected of leaking classified information to crime syndicates. They refused to answer questions that might lead to the identification of the person from whom they had received the secret AIVD documents. They were detained for failure to comply with a judicial order but released a few days later as the Regional Court recognised the importance of the protection of journalistic sources. The Regional Court further found that no issue of state security could arise since the availability of the documents outside the AIVD had been common knowledge in the media. Relying on Articles 8 (right to respect for private and family life) and 10 (freedom of expression and information), the applicants complained about the order to surrender documents which could identify journalistic sources and about the use of special powers by the State. The ECHR found that the targeted surveillance of the journalists

had been a violation of Articles 8 and 10 ECHR, since the use of special powers had been authorised without prior review by an independent body. Moreover, the government had not given "relevant and sufficient" reasons for the order to surrender documents, and there had thus been a violation of Article 10.

Similarly, in the Netherlands there is currently no specific legislation on whistle-blowing. Protection of employees depends largely on self-regulation and decisions in Dutch courts are usually based on Article 7:611 of the Dutch Civil Code, which is a general legal requirement to maintain good employer and employee practices. There are no arrangements for financial compensation, and damages awarded by courts are usually very limited.

The Dutch Parliament is currently considering a bill that would establish a "House for Whistle-blowers" (*Huis voor Klokkenluiders*) in the Netherlands (see also the questionnaire by Constant Hijzen). The House for Whistle-blowers would provide limited protection for whistle-blowers who disclose problems to their employers or to the 'House,' but no protection for those who disclose to others, such as law enforcement or the Parliament. The House will provide advice to the employee on steps that should be taken and whether the facts presented by the employee qualify as wrongdoing. The proposal defines wrongdoing as an act or omission that puts public interests at stake. This could be the case due to threats to public health, the safety of individuals, the environment or the functioning of public service institutions and companies.

6) In your view, how do the current debates over the issue of digital surveillance affect the use of secret evidence in courts as regards the practices of intelligence services that have been denounced?

The use of digital surveillance by intelligent services that is then used as secret evidence in courts represents a double challenge to democratic accountability and to the rights of the defence. The increased use of Internet-monitoring and in particular mass surveillance (the bulk interception and storage of citizens' communications and online activities) is highly problematic in itself, but it poses an ever greater challenge to fair-trial rights ex Article 6 ECHR when combined with a procedure that allows for the reliance on secret information and shielded witnesses in criminal procedures.

References

R.J. Bokhorst, *De Wet afgeschermde getuigen in de praktijk*, Memonrandum 2012-3, The Hague: Ministerie van Veiligheid en Justitie, Wetenschappelijk Onderzoek- en Documentatiecentrum, available at: https://www.wodc.nl/onderzoeksdatabase/toepassing-van-de-wet-afgeschermde-getuigen-in-de-praktijk.aspx?cp=44&cs=6800

M.A.H. Woude, *Wetgeving in een Veiligheidscultuur: totstandkoming van antiterrorismewetgeving in Nederland bezien vanuit maatschappelijke en (rechts)politieke context* (2010), Doctoral thesis, Leiden University.

M. Zevenhuizen, *De afgeschermde getuige: Steunpilaar van staatsveiligheid of struikelblok in Straatsburg?* (2007), Scriptie Rechtenfaculteit Rijksuniversiteit Groningen.

J.E.B. Coster van Voorhout, "Intelligence as Legal Evidence: Comparative Criminal Research into the Viability of the Proposed Dutch Scheme of Shielded Intelligence Witnesses in England and Wales, and Legislative Compliance with Article 6(3)(d) ECHR" (2006), *Utrecht Law Review* 2(2), pp. 119-144.

Q. Eijkman & B. van Ginkel, "Compatible or Incompatible? Intelligence and Human Rights in Terrorist Trials" (2011), *Amsterdam Law Forum* 3, pp. 3-16.

Country Fiche: Sweden

European Parliament study on "*National Security Exceptions and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges*"

Author: Emmy Eklundh

(University of Manchester)

This "country fiche" highlights the main issues in Sweden as regards the use of intelligence information and secret evidence in courts. Emmy Eklundh, a Swedish national, is currently a PhD Researcher at the University of Manchester.

KEY FINDINGS

- Intelligence materials presented in trials are produced by the Police and the Security Police. The Swedish Armed Forces can also produce this type of evidence, and sit within the Military Intelligence and Security Directorate (MUST).
- The Swedish Commission on Security and Integrity Protection was instituted in 2008 in order to make sure that the Police and the Security Police followed current laws regarding the handling of information retrieved through interception so as to make sure that the integrity of the citizens was upheld.
- However, in a 2013 government report, questions were raised regarding oversight of the Police and the Security Police. The report states that the Police and the Security Police now have more tools to deny the rights of citizens, especially with regard to surveillance.
- Sweden adopted a new terrorism law in 2003, which granted Sweden's intelligence services greater scope for their actions. These laws were later complemented with increased possibilities of surveillance, with the FRA law (National Defence Radio Establishment) implemented in 2009. The FRA law enacted a cluster of changes to the existing legislation on surveillance and intelligence.
- These laws were debated intensely and many public agencies, political parties, lawyers and foreign actors thought that it instituted a significant threat against individual integrity and was not justified based on threats to national security.
- There were also changes made in the secrecy laws. National security arguments play a central role when it comes to invoking secrecy. This is described in the Public Access to Information and Secrecy Act, which ensures access to public information, but also regulates when secrecy can be invoked. There is a section devoted to the right to invoke secrecy based on national security concerns, and it refers to any sort of information which can harm the country.
- Sweden is often criticised for having insufficient support for whistle-blowers. Even though the level of protection is quite strong in the public sector, it is very deficient in the private sector
- Swedish fundamental laws protect the freedom of the press, as well as freedom of speech. In addition, there is a clause which prohibits any (public) employer from further investigate the identity of the whistle-blower. In other words, the right to anonymity is quite strong in the public sector.
- The relationship between freedom of speech and the freedom of the press (both regulated in Sweden's fundamental laws) and secrecy, is described in the Public Access to Information and Secrecy Act. This stipulates that freedom of speech and the freedom of the press are suspended if the publication of information could "put the safety of the state in danger or seriously harm the country".

- Important debates have centred on the use of new surveillance methods and breaches of personal integrity. Indeed, the laws implemented in 2008 did give the FRA almost *carte blanche* to intercept internet and telephone conversations. The law was implemented by the conservative government, but there was severe disagreement within the coalition.
- There have since been changes to factor in considerations of personal integrity. The biggest changes lie in the creation of a court to assess the request to intercept, as well as the oversight body, the Swedish Commission on Security and Integrity Protection.
- However, this new arrangement has been criticised as, on the ground, the surveillance practices of the FRA remain difficult to assess.

1) Please describe an illustrative case in your country that highlights the main issues at stake when dealing with secret information in courts.

First and foremost, it is vital to point out that in Sweden there have only been 26 arrests in the name of the Terrorism Act since 2003 (Sveriges Riksdag 2003:148), and only two of these have led to jail sentences. All of these arrests have included Sunni Muslim men.

The 2003 Terrorism Act (Sveriges Riksdags 2003), implemented 1 July 2003, made it easier to detain and try an individual for the preparation of crimes, not only their execution. The Act is based upon the European Union Framework for Combating Terrorism that was adopted in June 2002. According to many critics, and perhaps especially the civil society organisation Charta 2008, the new Terrorism Law of 2003 allows for much less secure and transparent trials. This is particularly demonstrated in the following case:

On 19 April 2004, the National Police Guard, which is a militarised branch of the police, went into a flat in Gothenburg, Sweden. They arrested two men of Swedish citizenship but of Kurdish descent. The accusation was "preparation of terror crimes". The two men, Ali Berzengi and Ferman Abdullah, were accused of sending money to Iraq, where they would allegedly support terrorist attacks. When the trial started they were charged with "preparing acts of terrorism and preparing for criminal destruction under § 3 paragraphs one and two of the law on prosecution for financing particularly serious criminal acts in certain cases, etc. (2002:444) for offences against the said law" (Stockholm Tingsrätt 2005). The first sentence came from the Stockholm District Court on 12 May 2005. The defendants appealed, but the District Court's decision was further confirmed by Svea High Court, and they were sentenced to jail on 3 October 2005.

The evidence presented at the trial was of a multifaceted nature. It was obvious that the security police (SÄPO) had been monitoring the two men for quite some time, tapping their phones and intercepting their email conversations. In addition to this type of evidence, there were witness statements of individuals who claimed that they had seen Berzengi and Abdullah collecting money at mosques to send to terrorists. Both Berzengi and Abdullah claimed their innocence, saying that they had indeed sent money to Iraq, but only to help victims of the war. The money-distributing facility they were running, the hawala, was, according to them, only one of many similar institutions.

At the beginning of the trial, both the defendants and their legal councils were restricted from sharing any information about the trial with the media or the general public. The only party in the trial able to share information was Agneta Hilding Qvarnström, Deputy Chief Prosecutor at the International Prosecutors Chamber in Stockholm. This has been widely criticised by both the media and by civil society, which claim that this gave an skewed picture of the trial to the public (Hulten and Sonne 2011).

However, the most pressing critique regarded the handling of some evidence. Whilst the Swedish police and prosecution had produced much evidence themselves, there was in the judgment great reliance on German and US intelligence. Gösta Hulten, a journalist who has been scrutinising the whole process, has been granted access to the over 10,000 pages of evidence material from Sweden and Germany. However, the material from the US is classified. According to Hulten, some of the evidence was not presented to the court in written form, but only orally communicated by an FBI representative, which is against all Swedish legal practice (Hulten and Sonne 2011: 35). It is very clear that the court trusts what they call

"international legal assistance" (Stockholms tingsrätt 2005). According to *Sydsvenskan*, one of the largest Swedish dailies, the Swedish security police had no notice of the two men until US and German intelligence services contacted them in the wake of a terrorist attack in Arbil in Kurdistan. Apparently, the attack was financed by the organisation Ansar-al-Islam. German and US intelligence indicated this organisation was the actual recipient of the money transfers from Abdullah's and Berzengi's hawala (Sydsvenskan 12/02/2006). The defendants were sentenced to five (Berzengi) and four-and-a-half (Abdullah) years in prison and deportation (Stockholms tingsrätt 2005-05-12).

In its confirmation of the sentence, the Svea High Court decided to maintain secrecy of a number of pieces of information, with reference to national security. The reason for keeping this secrecy, as will be shown below, is that the information given to Sweden from the US was produced by "krigsförande part" (a party engaged in war), and therefore the information cannot be public (Sveriges Riksdag 2009).

2) What are the bodies involved in the production and processing of secret evidence? Is there any oversight of the practices of the antiterrorist and (police-military) intelligence services that provide this evidence?

PRODUCTION AND PROCESS

Regarding evidence produced in trials such as the one mentioned above, most of the evidence is produced by the police and the security police (SÄPO). The Swedish Armed Forces (Försvarsmakten) can also produce this type of evidence, which comes from the Military Intelligence and Security Directorate (MUST). MUST consists of three departments, Underrättelsekontoret UNDK (Intelligence Office), Säkerhetskontoret SÄKK (Security Office) and Kontoret för Särskild Inhämtning KSI (Office for Special Collection). MUST handles all intelligence and security service within the Swedish Armed Forces (Försvarsmakten 2013). There is also a collaborative institute among the Police and the military called the National Centre for Terrorist Threat Assessment (NTC), which "produces long and short-term strategic assessments of the terrorist threat against Sweden and Swedish interests" (Säkerhetspolisen 2014). However, the NTC does not investigate crime per se, but provides analysis for both the military and the police. The unit is staffed by personnel from the National Defence Radio Establishment (FRA), MUST and the Säkerhetspolisen (Swedish Security Service).

Secret evidence retrieved by **interception** can only be produced upon request by Regeringen (the Cabinet), Regeringskansliet (Cabinet Offices), Försvarsmakten (Swedish Armed Forces), Rikskriminalpolisen, and Säkerhetspolisen (Swedish Security Services). The only body allowed to conduct interception is the National Defence Radio Establishment (FRA). Within the Police, Polismyndigheten (Swedish Police), Säkerhetspolisen (Swedish Security Service) and Ekobrottsmyndigheten (Swedish Economic Crime Authority) are capable of handling evidence produced through interception. Within the military, we can count several institutions: Försvarsmakten (Swedish Armed Forces), Försvarets radioanstalt (National Defence Radio Establishment), Totalförsvarets forskningsinstitut (Swedish Defence Research Agency) and Försvarets materielverk (Swedish Defence Materiel Administration). Interception is produced only with the permission of Försvarsunderrättelsedomstolen (Swedish Defence Intelligence Court).

"All reconnaissance performed by FRA needs permission from the court. It shall be stated in the permission who requested the information, which search terms can be used, as well as other conditions needed in order to limit the effect on individual integrity. The court decision cannot be appealed" (Försvarsunderrättelsedomstolen 2014).

OVERSIGHT

The police and the security police are overseen internally and externally. Firstly, Rikspolisstyrelsen (National Police Board) has the main responsibility to oversee the police. This is not an independent body, but is a part of the police and is headed by the National Police Commissioner. This has been subject to some debate recently, in the government report *Inspection of the Police* (SOU 2013:42). These debates are further explained in Section 3.

However, the police are also overseen by external bodies, through what is called ordinary and extraordinary oversight. The difference is that extraordinary oversight does not include the right to interrupt the activity or to give guidance in special cases. The extraordinary oversight is rather concerned with systemic and constitutional problems. Ordinary oversight is conducted by the by Säkerhets- och integritetsskyddsnämnden (Swedish Commission on Security and Integrity Protection) and the Data Inspection Board. Extraordinary oversight is conducted by two bodies under the Department of Justice: Justitieombudsmannen (Parliamentary Ombudsmen) and Justitiekanslern (Chancellor of Justice).

The Data Inspection Board ensures that the police and the security police handle personal data appropriately and in accordance with the law. The Board also oversees all public offices.

The Swedish Commission on Security and Integrity Protection was instituted in 2008 in order to make sure that the police and the security police followed current laws regarding the handling of information retrieved through interception as to make sure that the integrity of the citizens was upheld. Based on a court ruling in the European Court for Human Rights in 2006 (in the case Segerstedt-Wiberg m.fl. mot Sverige (European Court of Human Rights: 62332/00)), Sweden was exhorted to change its practices regarding the handling of sensitive information, since its current practice did not uphold Article 13 of the European Convention on Human Rights. The difference between the Commission and the Data Inspection Board is that the Commission focuses solely on cases regarding 'special crime-preventing activity' (Sveriges Riksdag 2007:980). In other words, the Commission only deals with information gathered through interception and surveillance and how this might violate individual integrity.

The military, and especially the Military Intelligence and Security Directorate (MUST), is monitored by Statens inspektion för försvarsunderrättelseverksamheten (Swedish Inspection of Defence Intelligence Services). The agency's main task is as follows:

"The Swedish Inspection of Defence Intelligence Services is instituted to control and monitor intelligence activity performed by those agencies who, according to Forordning 2000:131 on intelligence activities, conduct such activities. The Inspection should make sure that, with regards to surveillance undertaken, these agencies follow laws and regulations, and generally fulfil their obligations" (Sveriges Riksdag 2009b:969).

The Department of Defence also monitors the military, as the latter reports to the former annually. There is also oversight conducted by the Riksrevisionen (Swedish National Audit Office), which is responsible for oversight of all public institutions. The decisions for or against interception made by the Defence Intelligence Court are overseen by three different institutions: Justitieombudsmannen (Parliamentary Ombudsmen), Justitiekanslern (Chancellor of Justice) and Datainspektionen (Swedish Data Inspection Board).

3) The concept of national security: how is it framed and understood in your country? On what grounds do authorities in your country define national security and how is this connected to a right to secrecy in courts? Are there any secrecy claims that obstruct oversight?

According to Magnus Ranstorp, one of Sweden's most renowned experts on terrorism, the country has suffered a 'terrorism awakening'. In an article from 2011, he argues that after the suicide attack in central Stockholm in December 2010, Swedish intelligence services suffered a rude awakening, seeing that they had no previous files on the suicide bomber. Ranstorp argues:

"The debate climate about terrorist threat assessment in Sweden had been stifled by ideologically driven debaters who used the label of Islamophobia and racism to silence the issue. This is not possible anymore. The challenge for Sweden will be to debate the issues more frankly but sensibly, while simultaneously addressing the issue of countermeasures against extremism. For this, Sweden is looking toward Denmark, the Netherlands and the United Kingdom, which have had longstanding community-based 'experiments' in countering violent extremism" (Ranstorp 2011: 5).

However, there are other sides to the story. One could also argue that there has been a general trend of terrorism-awakening in Sweden since 9/11. As mentioned above, Sweden accepted a new terrorism law in 2003, based on the European Framework on combatting terrorism (European Council 2002). This law

granted more possibilities for Sweden's intelligence services since, in order to monitor individuals, the punishment for the crime must exceed a certain limit. In the 2003 terror laws, the punishment for crimes such as murder and other damages were increased if the crimes were also motivated by terrorism, that is, creating fear or destabilising the State (Sveriges Riksdag 2003). This has been heavily criticised, for instance, by Janne Flyhed, Professor of Criminology at Stockholm University, who argues that the current laws give too much power to the Police and the Security Police. In addition, he sees this as a direct consequence of 9/11 and how the concept of terrorism in Swedish legislation has been conflated with US and EU definitions (Flyghed 2007).

The new antiterrorism laws were later complemented with increased possibilities of surveillance, especially with what is in Sweden commonly referred to as the FRA law, implemented 1 January 2009. FRA (National Defence Radio Establishment) is the one body allowed to intercept wire communication (telephone, email, etc.). The FRA law designated a cluster of changes to the present legislation on surveillance and intelligence (Sveriges Riksdag 2008). It also allows FRA to store Internet traffic data, which in practice means that *all* Internet traffic in Sweden is stored for future potential investigations. The government bill which preceded the law (Regeringen 2006) claimed that Sweden was facing a new security reality in the wake of the 9/11 attacks. In the bill, it is strongly emphasised that current security threats are best handled in cooperation with other nations (ibid.), but that Sweden must be able to produce its own intelligence in order to keep its independence and neutrality.

The law was heavily debated, and many public agencies, political parties, lawyers and foreign actors thought that it instituted a significant threat against individual integrity and was not justified based on threats against national security. It is notable that the actors who should be most interested in such a law were also deeply critical. For instance, the former director of the security police argued that the changes were not compatible with the Swedish ground laws (Dagens Nyheter 12/06/08). Duncan Campbell has claimed that this law was based on cooperation between the United States, Great Britain, and Sweden, and consequently meant that information was shared between the countries (Dagens Nyheter 2013-10-13; The Local 2013-10-13), saying that Sweden had as much intelligence exchange with the US as did Israel.

In concurrence with the FRA law, there were also changes made in the secrecy laws. Claims to national security play a central role when it comes to invocations of secrecy. This is described in the Public Access to Information and Secrecy Act (OSL) (Sveriges Riksdag 2009a), which ensures access to public information, but also regulates when secrecy can be invoked. OSL was implemented on 30 June 2009. For some time, there had been concerns about whether the current Secrecy Law (from 1980) was up to date with important changes in society. Among these we can count privatisation of previously public services and the increase of digital material (Regeringen 2008: 380). There was a concern that the principle of publicity (which is very strong in Sweden) was not sufficiently guarded. In addition, the new law was supposed to be more user-friendly and less formal. Some of the main changes concerned freedom of speech and whistle-blowing. The new law stated that private companies working for the public sector should also have to make material public (Regeringen 2008: 271). In addition, the law was made "technology neutral", meaning that regardless of the format used for public information, it should be accessible to the general public.

There is a section devoted to the right to invoke secrecy based on national security concerns, and it refers to any sort of information which can harm the country (OSL Section IV). This section interferes with freedom of speech and freedom of the press. The changes in the new secrecy law are not very different from the previous ones: previously, invocations of national security for secrecy were also possible. However, it now also encompasses digital materials. With regards to court proceedings and secrecy, all court rulings are normally supposed to be made public. However, this can be kept secret with reference to national security:

"Secrecy for a statement in a trial…ceases to exist if the statement is included in a court ruling. The first section is not applicable if the court in its ruling has decided that the secrecy shall remain. The decision that secrecy shall remain cannot include the final court ruling, unless with reference to national security or to another interest of outstanding character. If the trial regards the civil rights or obligations or accusation of any crime of or against an individual, decisions to invoke further secrecy are only allowed if the nation is at war or in the immediate threat of war or if there are other extraordinary circumstances induced by war" (Sveriges Riksdag 2009a: Chap. 43, §8).

As seen above, there are severe restrictions on keeping court rulings secret, even though the previous content of the trial has been kept so. This means that the courts can keep information secret with reference to national security, but it is very difficult to keep court rulings away from the public.

With regards to oversight, there are special regulations in the Public Access to Information and Secrecy Act (OSL) which stipulate how bodies of oversight shall handle secret information. According to the inspecting agencies (Swedish Inspection of Defence Intelligence Services and the Swedish Commission on Security and Integrity Protection) there are no obstructions to oversight, even if the information is classified (Sveriges Riksdag 2009b; Sveriges Riksdag 2009a: Chap. 10, §17).

In a recent report by the government (Statens Offentliga Utredningar 2013:42), questions are raised regarding the oversight of the Police and the Security Police. The report states that the Police and the Security Police now have more tools to deny the rights of citizens, especially with regards to surveillance. This requires a high level of trust from the public, says the report, a trust that may not be present today, due to the recent debates about integrity. It is especially problematic that the main oversight of the police is still internal, and the report suggests that a completely external body of oversight should be instituted (ibid. 123).

4) What are the procedural guarantees and the protection standards for the rights of the defence, the freedom of the press and the protection of whistle-blowers in your country concerning the use of secret evidence in courts?

In 2013, Transparency International criticised Sweden for having insufficient support for whistle-blowers. They meant that privatisation has had a profound effect on such protection and that, though it might be strong in the public sector, it is very deficient in the private sector (Transparency International 2013). At the time of the report, there had already been some discussion in Sweden on the insufficiency of the protection. Dennis Töllborg, Professor of Law at the University of Gothenburg, has in several reports and investigations pointed to the practice of loyalty and fear of exclusion, mostly within the Swedish judiciary forces such as the police, but also the army (Töllborg 2012: 91). Töllborg argues that other countries, such as the UK and Denmark, have much stronger mechanisms for protecting whistle-blowers, and not as strong codes of silence as in Sweden (Töllborg 2012: 101)

Sweden has had a few cases of whistle-blowing, most recently when a corruption scandal was revealed in Gothenburg where municipality officials, against a small remuneration, gave large construction contracts to their private friends. The whistle-blowers then lost their positions within the companies. Transparency International has concluded that there had been some political willingness to change the situation, with the criminalisation of employers punishing whistle-blowers in 2011 (Svenska Dagbladet 6/11/13; Sveriges Riksdag 1949: Chap. 2 and 3; Sveriges Riksdag 1991: Chap 2; Regeringen 2009). Indeed, there has also been a government bill, suggesting a range of improvements for the rights of whistle-blowers.

The bill argues that the support is indeed too weak, and compares Sweden's situation to that of other European countries. Just like Transparency International, they conclude that the protection is quite good if you are employed in the public sector, but much weaker when employed in the private sector (Statens Offentliga Utredningar 2014:31: 74). The Swedish ground laws protect freedom of the press and freedom of speech. In addition, there is a clause which prohibits any (public) employer from further investigating who the whistle-blower is (Statens Offentliga Utredningar 2014:31: 68). In other words, the right to anonymity is quite strong in the public sector. The government bill suggests that this should also be valid for the private sector, but the bill has yet to be approved by Parliament.

Whilst the support and protection for whistle-blowers is quite strong for public employees, and is very well protected in the ground laws, there are also several clauses which prohibit this with reference to national security. If, in any way, the material leaked could be harmful to the nation, the protection ceases to exist and the whistle-blowing becomes a criminal offence, for instance, when the information leaked leads to "[a] crime against national security and other crimes directed against the state (espionage, treachery, sedition, negligence with classified material, or unauthorised dealing with classified material)" (Statens Offentliga Utredningar 2014:31: 288).

Another case where the protection ceases is if the whistle-blower shares classified information. The relationship between freedom of speech, freedom of the press (both regulated in Sweden's fundamental laws)[274] and secrecy is described in the Public Access to Information and Secrecy Act (OSL). This stipulates that freedom of speech (YGL) and the freedom of the press (TF) are suspended if the publication of information could "put the safety of the state in danger or seriously harm the country" (Sveriges Riksdag 2009a: Chap 15, par. 6), as was the case of Jan Guillou and Peter Bratt (described below under question 5). However, it should also be noted that there is a possibility of publishing information in, for instance, a newspaper and it is "in certain cases allowed to disclose secret information verbally for publication in, for instance, a newspaper, but that it is never allowed to disclose the secret official document which contains this information nor to disclose information if one thereby commits such a crime as referred to in the said fundamental laws" (Ministry of Justice 2009: 32). This structure makes it possible for public officials to share secret information without committing a criminal offence. They are allowed to share things to enhance debate among the general public "if they consider that the interest of public access to the authorities' operations weighs more heavily in the balance than the interest to be protected by the secrecy" (Ministry of Justice 2009: 32).

5) In your view, how do the current debates over the issue of digital surveillance affect the use of secret evidence in courts as regards the practices of intelligence services that have been denounced?

The topic of digital surveillance and national security has indeed been heavily debated since the terror attacks in 2001. However, one must remember that Sweden has a long tradition of neutrality; it is politically sensitive to argue that we must help the "West" in achieving a secure world. Therefore, the debate has been centred on integrity as such, whereas questions of national security are often met with silence.

One of the highest profiles in the debates is Jan Guillou, one of Sweden's most famous authors. However, one should also note that he was one of the journalists who revealed the so called IB affair in 1973. Along with his colleague, Peter Bratt, Guillou revealed that Sweden had a secret intelligence unit, IB, which not even the Parliament knew about. The unit conducted surveillance and collected intelligence from both abroad and domestically, and they also had a large registry of left-wing activists. They conducted espionage abroad, and had also broken into the Egyptian embassy in Stockholm. The information came from Håkan Isacson, who was previously employed by IB. Giullou, Bratt and Isacson were all arrested from crimes against national security, and they were sentenced to one year each in prison (Sveriges Radio 02/05/2013).

As expected, Guillou has a very contentious relationship with Swedish intelligence. He has, not surprisingly, been a fierce debater on the recent terrorism cases (cf. Question 1). Guillou argues that the 2003 terrorism laws completely set the Swedish judiciary system out of place, since all proceedings are held *in camera* (Guillou 2008). As also mentioned under Question 1, the civil rights organisation Charta 2008 has compared Sweden to several authoritarian regimes, saying that the 2003 terror laws are merely an expression of anti-Muslim propaganda. Lawyer Tomas Olsson – who has worked as a defender in several terrorist cases – has said that the terror laws cannot be applied the way they previously have been due to the difficulty of determining what is "terrorism" in states such as Somalia (Proletären 16/12/2010). In addition, the Helsinki Committee (now known as Civil Rights Defenders) argued that the laws on terrorism did not uphold the legal motto of equality before the law, since the laws on extradition made it easier for Sweden to deport individuals suspected and sentenced for terrorism (Swedish Helsinki Committee for Human Rights 2003).

[274] Sweden does not have a formal constitution but, instead, four fundamental laws. Two of these regulate freedom of speech (YGL), and freedom of the press (TF), respectively. To change a ground law, the Parliament needs to vote twice, with absolute majority, in favour of the change. Between the votes, there needs to be a national election (Sveriges Riksdag 2013).

However, the most heated debates have been over the use of new surveillance methods and the breaches of personal integrity. Indeed, the laws implemented in 2008 did give the FRA almost a *carte blanche* to intercept Internet and telephone conversations. The law was implemented by the conservative government, but there was severe disagreement within the coalition. Sweden also suffered criticisms from Privacy International, which argued that the security police now have "unprecedented possibilities" to collate intelligence (Privacy International 2014). As also identified by Duncan Campbell, Sweden was more prone than other countries to give more capabilities to the Security Service (European Parliament 15/09/2013). Mark Klamberg, Lecturer in Law at Uppsala University, claimed in an article in 2009 that the system would not be legally sound without a court decision giving permission for interception (Klamberg 2009: 540). He also pointed out that the real danger with the new laws was not the interception, but rather the storing and archiving of *all* Internet traffic data.

However, there are also voices that claim the threat from the new laws is exaggerated. For instance, William Agrell, Professor of Intelligence Analysis at Lund University, argues that FRA conducting interception over the Internet is not really a major change, because since it is possible in countries such as the UK and Germany, it should also be possible in Sweden (Dagens Nyheter 10/07/2008). Similarly, Dennis Töllborg argues that intelligence and interception are international; if Sweden does not intercept communication, someone else will, and it should be better that the country remains in control (ibid.).

Indeed, there have been some changes due to the heavy criticism. Most of all, as mentioned above, preserving personal integrity has been revisited and the new laws are thus more restrictive in the use of interception. The biggest changes lie in the creation of a court which must obtain permission for interception, and of a body of oversight, the Swedish Commission on Security and Integrity Protection (Regeringskansliet 25/09/2008; SOU 2006:98). However, the Swedish Pirate Party – which is working for increased integrity protection – argues that even though there were changes made to the initial laws, FRA practice has not changed. According to the Party, the restrictions implemented, which should only give the Government Cabinet and the Parliament the right to order this type of interception, are heavily compromised. As the Snowden documents have shown, the material given to the NSA by Swedish intelligence services was extensive (Piratpartiet 31/07/2014).

On a final note, one can linger on the point that what is most heavily debated in Sweden is the production of evidence and information, rather than the handling thereof. The agency that has been most heavily criticised is the FRA. This leaves the actual analysis of the material almost untouched. As mentioned above, MUST is the branch of military intelligence which analyses threats, even if they do not collate evidence. In the debate, this agency is largely absent. This also relates to the discovery made by Guillou and Bratt in 1973 of a previously completely secret agency. As such, intelligence is something which does not suffer much public scrutiny in Sweden. How can that be? Bo Rothstein, Professor of Politics at the University of Gothenburg, has argued that trust in public offices is very high in Sweden. Swedes rarely think that public officials would do anything wrong, and there is a strong myth of the infallible public servant (Rothstein 2003). Dennis Töllborg has made a similar argument, saying that the public trust in the Swedish police is indeed very great, but, in fact, the tradition of loyalty within the Swedish police is highly dangerous to a transparent public system (Töllborg 2012: 19).

References

Dagens Nyheter (12/06/08), "Förre Säpochefen kritiserar förslaget", http://www.dn.se/nyheter/politik/forre-sapochefen-kritiserar-forslaget/, Retrieved 08/09/2014.

Dagens Nyheter (10/07/08), "Professor: Snedvriden debatt i Sverige", http://www.dn.se/nyheter/politik/professor-snedvriden-debatt-i-sverige%5C, Retrieved 08/09/2014.

Dagens Nyheter (2013/10/13), "Sverige samarbetade med USA om FRA-lagen", http://www.dn.se/nyheter/sverige/sverige-samarbetade-med-usa-om-fra-lagen/, Retrieved 01/09/2014.

European Council (2002), "Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)", *Official Journal of the European Communities*, L 164, pp. 3-7.

European Courts of Human Rights (2006), CASE OF SEGERSTEDT-WIBERG AND OTHERS v. SWEDEN, http://hudoc.ECHR.coe.int/sites/eng/pages/search.aspx?i=001-75591#{"itemid":["001-75591"]}, Retrieved 28/08/2014.

Flyghed, Janne (2007), "Internationaliseringen av kriminalpolitiken", *Nordisk Tidskrift for Kriminalvidenskab*, 94(1), pp. 74-88.

Försvarsmakten (2013), "Militära underrättelse- och säkerhetstjänsten, MUST", http://www.forsvarsmakten.se/sv/organisation/hogkvarteret/militara-underrattelse-och-sakerhetstjansten/, Retrieved 28/08/2014.

Försvarsunderrättelsedomstolen (2014), "Om försvarsunderrättelsedomstolen", www.undom.se, Retrieved 04/09/2014).

Guillou, Jan (2008), "Rättssäkerhet sätts ur spel under hemliga rättegångar", Aftonbladet, March 2.

Hulten, Göran – Sonne, Lena (2011), *Terroristjaktens svarta bok*, Falun: Scandbook.

Klamberg, Mark (2009), "FRA:s signalspaning ur ett rättsligt perspektiv", *Sveriges Juristtidning*, pp. 519-541.

Ministry of Justice (2009), *Public Access to Information and Secrecy Act Information concerning public access to information and secrecy legislation, etc.*, Stockholm: Government Offices.

Piratpartiet (31/07/2014), "FRA-lagen", http://www.piratpartiet.se/fra/, Retrieved 14/08/2014.

Privacy International (2014), "Sweden Country Report", https://www.privacyinternational.org/reports/sweden/ii-surveillance-policies, Retrieved 18/08/2014.

Proletären (16/12/2010), "Säpo vann mot rättssäkerheten", http://www.proletaren.se/inrikes/sapo-vann-mot-rattssakerheten, Retrieved 05/09/2014.

Ranstorp, Magnus (2011), 'Terrorism awakening in Sweden?', CTC Sentinel, 4(1), pp. 1-5.

Regeringen (2006), *En anpassad försvarsunderrättelseverksamhet Prop. 2006/07:63*, Stockholm: Regeringskansliet.

Regeringen (2008), *Regeringens proposition 2008/09:150: Offentlighets- och sekretesslag*, Stockholm: Regeringskansliet.

Regeringen (2009), *Grundlagsskydd för digital bio och andra yttrandefrihetsrättsliga frågor prop. 2009/10:81*, Stockholm: Regeringskansliet.

Regeringskansliet (25/09/2008), "Alliansen enig om stärkt integritet, tydligare reglering och förbättrad kontroll i kompletteringar till signalspaningslagen", http://www.regeringen.se/sb/d/10911/a/112332, Retrieved 18/08/2014.

Rothstein, Bo (2003), *Sociala fällor och tillitens problem*, Stockholm: SNS förlag.

Statens Offentliga Utredningar (SOU) (2006), *Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel m.m.*, Stockholm: Elanders Sverige AB.

Statens Offentliga Utredningar (SOU) (2013), *Tillsyn av polisen*, Stockholm: Elanders Sverige AB.

Statens Offentliga Utredningar (SOU) (2014), *Visselblåsare: Stärkt skydd för arbetstagare som slår larm om allvarliga missförhållanden*, Stockholm: Elanders Sverige AB.

Stockholms Tingsrätt (2005-05-12), "Dom i mål B 2965-04".

Svenska Dagbladet (06/11/2013), "Svenskt skydd för visselblåsare får underkänt", http://www.svd.se/naringsliv/nyheter/varlden/svenskt-skydd-for-visselblasare-far-underkant_8694156.svd, Retrieved 01/09/2014.

Sveriges Radio (02/05/2013), "40 år sedan IB-affären exploderade", http://sverigesradio.se/sida/gruppsida.aspx?programid=2151&grupp=16181&artikel=5522466, Retrieved 05/09/2014.

Sveriges Riksdag (1949), *Tryckfrihetsförordning (1949:105),* Stockholm: Svensk Författningssamling.

Sveriges Riksdag (1991), *Yttrandefrihetsgrundlag (1991:1469),* Stockholm: Svensk Författningssamling.

Sveriges Riksdag (2003), *Lag om straff för terroristbrott SFS 2003:148*, Stockholm: Svensk Författningssamling.

Sveriges Riksdag (2007), *Lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet*, Stockholm: Svensk Författningssamling.

Sveriges Riksdag (2008*), Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet*, Stockholm: Svensk Författningssamling.

Sveriges Riksdag (2009a), *Offentlighets och Sekretesslagen SFS 2009:400*, Stockholm: Svensk Författningssamling.

Sveriges Riksdag (2009b), *Förordning (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten*, Stockholm: Svensk Författningssamling.

Sveriges Riksdag (2013), "Grundlagarna", http://www.riksdagen.se/sv/Sa-funkar-riksdagen/Demokrati/Grundlagarna/, Retrieved 10/09/2014.

Sydsvenskan (12/02/2006), "Kiosken var en terrorbank", http://www.sydsvenskan.se/sverige/kiosken-var-en-terrorbank/, Retrieved 21/08/2014.

Säkerhetspolisen (2014), "Nationellt centrum för terrorhotbedömning", http://www.sakerhetspolisen.se/kontraterrorism/nationellt-centrum-for-terrorhotbedomning.html, Retrieved 28/08/2014.

The Local (13/10/2013), "Sweden worked with USA on FRA law" http://www.thelocal.se/20131013/50760, Retrieved 28/08/2014.

The Swedish Helsinki Committee for Human Rights (2003), Alternative report to "Comments by the Government of Sweden on the Concluding Observations of the Human Rights Committee" (CCPR/CO/74/SWE), Stockholm: Swedish NGO Foundation for Human Rights.

Transparency International (2013), "Whistleblowing in Europe – Legal protection for whistleblowers in the EU", http://www.stt.lt/documents/soc_tyrimai/2013_WhistleblowingInEurope_EN.pdf, Retrieved 28/08/2014.

Töllborg, Dennis (2012), *Älska din navel: Om illiojal maktanvändning, den offentliga lögnen och skydd för whistle-blowers*, Gothenburg: Gothenburg Research Institute.

ABOUT CEPS

Founded in Brussels in 1983, the Centre for European Policy Studies (CEPS) is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world.

Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today,
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process, and
- Provide a regular flow of authoritative publications offering policy analysis and recommendations,

Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts,
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach,
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals.

Programme Structure

In-house Research Programmes

Economic and Social Welfare Policies
Financial Institutions and Markets
Energy and Climate Change
EU Foreign, Security and Neighbourhood Policy
Justice and Home Affairs
Politics and Institutions
Regulatory Affairs
Agricultural and Rural Policy

Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)

Research Networks organised by CEPS

European Climate Platform (ECP)
European Network for Better Regulation (ENBR)
European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)