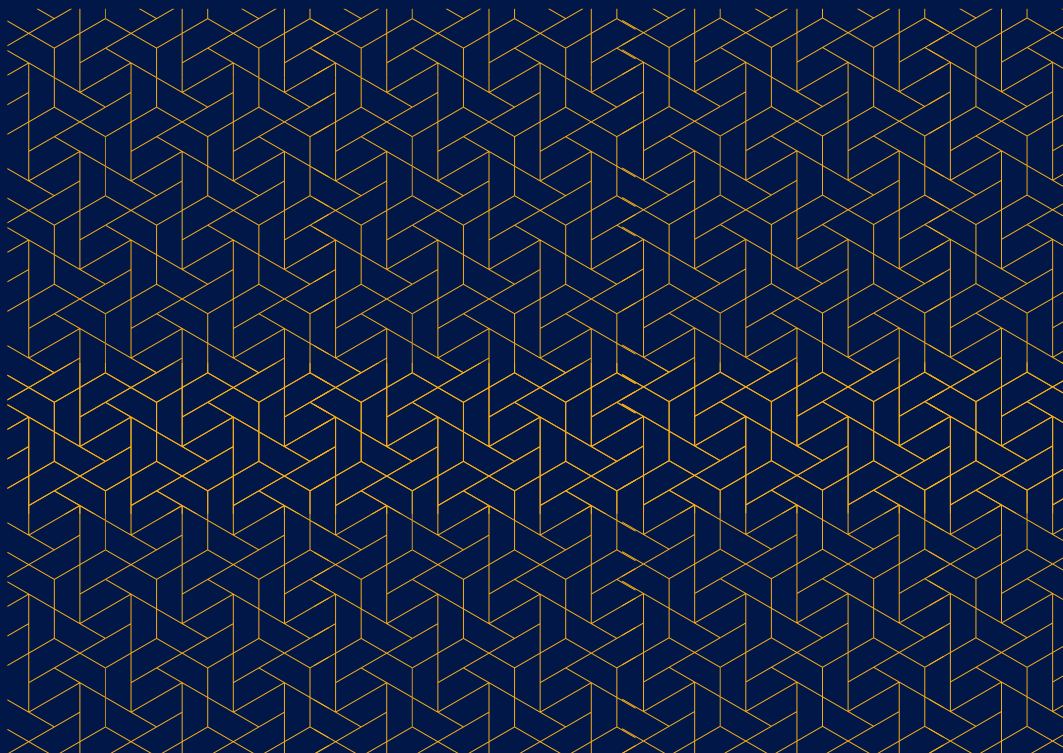
DCAF Geneva Centre for Security Sector Governance

ADMISSIBILITY OF (COUNTER-) INTELLIGENCE INFORMATION AS EVIDENCE IN COURT



About this Research Paper

This Research Paper was prepared by DCAF's Europe and Central Asia Division. DCAF would like to thank the Federal Department of Defence, Civil Protection and Sport (DDPS) of the Swiss Confederation and the Norwegian Ministry of Foreign Affairs for their generous support in making this publication possible.

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice, and supports capacity building of both state and non-state security sector stakeholders.

DCAF – Geneva Centre for Security Sector Governance

Maison de la Paix

Chemin Eugène-Rigot 2E

CH-1202 Geneva, Switzerland

Tel: +41 22 730 94 00

info@dcaf.ch

www.dcaf.ch

Twitter @DCAF_Geneva

Cite as: DCAF – Geneva Centre for Security Sector Governance. 2021. The Admissibility of (Counter-) Intelligence Information as Evidence in Court. (Geneva: DCAF).

Note

The opinions expressed in this publication are those of the authors and do not reflect the opinions or views of the Federal Department of Defence, Civil Protection and Sport of the Swiss Confederation or the Norwegian Ministry of Foreign Affairs.

Copy-editor: Alessandra Allen

Author: Andrej Bozinovski

Design & layout: DTP Studio

ISBN: 978-92-9222-630-5

Table of Contents

List of Abbreviations and Acronyms

EU European Union

ECHR European Convention on Human Rights

ECJ European Court of Justice

ECtHR European Court of Human Rights

FISA Foreign Intelligence Service Act

CIPA Classified Information Procedures Act

SIAC Special Immigration Appeals Commission

Introduction

Global security challenges – such as the war on terrorism, cybersecurity, the counter-proliferation of weapons of mass destruction, organized crime, corruption, and drugs trafficking – have transformed the objectives, nature, and instruments of criminal law. States have enacted measures based on the principle of the rule of law that allow investigators and prosecutors to use intelligence and sensitive law enforcement information as evidence in judicial proceedings in a manner that ensures not only the protection of sources and collection methods but also the defendant's right to a fair trial as a basic procedural guarantee. In the majority of European Union (EU) countries, evidence gathered by intelligence services (herein referred to as 'intelligence-gathered evidence') is used in judicial proceedings as general information only. General or steering information is defined as information that is shared by intelligence services with law enforcement authorities, or information from intelligence sources that can serve to instigate an independent police investigation. It is also referred to as information from intelligence sources that is used for 'lead purposes only'. This information can be used to instigate an independent investigation (case) – but not as evidence in court proceedings – or as special information[1] (Spain); it cannot serve as standard or crown[2] evidence or as the only evidence upon which the court renders a conviction. Notably, the legislations of Austria, Italy, and Croatia provide a clear distinction between the intelligence services and their competencies on the one side, and the law enforcement authorities and their competencies on the other. The United Kingdom and the Netherlands, on the other hand, follow a different approach and their respective procedural legislation allows for the direct use of such evidence in criminal procedures, and includes special proceedings (United Kingdom) concerning the use of evidence gathered by intelligence services in court. As a result of this diversity, an integrated and coherent approach is needed in Europe to facilitate cooperation and the exchange of information between law enforcement and intelligence services. Within the context of criminal law, such information can be used a catalyst to trigger investigations

1 The term special information was coined by the Supreme Court of Spain during the terrorism case of 2001 (STS 2084/2001), which influenced the evidentiary principles applied by the court. The court declared that reports by members of the Civil Guard could be considered intelligence reports and categorized as 'expert intelligence evidence' rather than testimonial evidence; however, this position was abandoned in 2005 during a similar case (STS 1029/2005). For more information, see: http://www.poderjudicial.es/search/index.jsp.

2 Crown evidence (as it is referred to in the jurisprudence of commonwealth countries) or key evidence is evidence produced before a court of law to prove or disprove a point in issue, such as the statements of witnesses, documents, and material objects.

of terrorist activities, organized crime, corruption, and other attempts to disrupt public order, while striking the right balance between privacy and security.

Given the complexity of this issue, this Thematic Brief aims to provide a comparative assessment of the admissibility, treatment, and practical ramifications of evidence obtained by intelligence services in court, through an analysis of European and international best practices – as well as applicable jurisprudence and human rights standards of the European Court of Justice (ECJ) and the European Court of Human Rights (ECtHR). Furthermore, it shows that evidence obtained by the intelligence services is not always considered inadmissible, and ultimately demonstrates that such evidence can serve to initiate investigations or facilitate ongoing investigations while respecting not only national security concerns but also the defendant's right to a fair trial.

This Brief is composed of three sections. The first section provides an overview of the standards and principles of the ECtHR and the ECJ of the European Union. The second part analyses the treatment of intelligence-gathered evidence in Europe, including national security cases, judicial assessment, evidentiary rules, and procedural safeguards. It demonstrates how intelligence-gathered evidence is admissible in court through the application of the 'proportionality principle' and highlights best practices observed through the prism of the Dutch, the UK, and several other jurisdictions. It describes the treatment of intelligence-gathered evidence in US legislation and jurisprudence, the integrated and coordinated approach of intelligence and law enforcement agencies to activities related to the prevention of terrorism and organized crime, and the implications of using evidence gathered through the application of the Foreign Intelligence Service Act (FISA) and the Classified Information Procedures Act (CIPA) in court. The conclusion summarizes the Brief's analysis of the use of intelligence-gathered evidence as well as their treatment and provides guidance for best practices in their use in proceedings.

1. Standards of the European Convention of Human Rights and Jurisprudence of the European Court of Human Rights

The ECtHR in Strasbourg has engaged with various issues affecting the relationship between national security, intelligence, and human rights judgments in intelligence surveillance cases. While the concept of national security has not been comprehensively defined, European case law provides some substance to the definition, stating that it 'most definitely includes the protection of state security and constitutional democracy from espionage, terrorism, support for

terrorism, separatism and incitement to breach military discipline'.[3] The jurisprudence of the court prescribes ex post assessments of whether states' actions that interfere with human rights on national security grounds conform to the European Convention on Human Rights (ECHR).[4] Three main standards must be fulfilled to determine the legality of the actions through:

- an assessment of whether the actions undertaken by the state are **lawful** and of the **quality of the national legislation**;
- an assessment of whether the actions are **necessary in a democratic society** and whether they adhere to the **principle of proportionality**; and
- an assessment of whether effective **legal remedies and judicial control** are present.

The standards of Article 6 of the ECHR provide details of the right to a fair trial, including the right to a public hearing before an independent and impartial tribunal within a reasonable time, the presumption of innocence, and other minimum procedural rights, such as the right to a defence; adequate time and facilities to prepare a defence; access to legal representation, translation, and interpretation; and the ability to challenge evidence and examine witnesses. The court cannot, however, determine the type of evidence allowed as states enjoy a margin of appreciation in drafting laws related to evidence and the admissibility of evidence gathered by the intelligence services and the assessment of such evidence.[5] More specifically, in the context of intelligence-gathered evidence, the testimony of intelligence officers is not always inadmissible as evidence. The court's jurisprudence also dictates that in the fight against terrorism, certain restrictions may apply to the rights of defendants. In Doorson v. the Netherlands, the court found that the use of anonymous witnesses to establish a conviction 'is not under all circumstances incompatible with the Convention' because the anonymous witness may be an intelligence officer deployed undercover and uncovering his or her identity may

3 European Court of Human Rights. 2013. 'National security and European case-law'. Division de la Recherche/Research Division, Council of Europe. Available at: https://rm.coe.int/168067d214.

4 The standards of states' interference in human rights were explained by judge and former Justice Minister of Slovenia, Ales Zalar at the DCAFs 11th Strategic Consultation on Admissibility of (counterintelligence information as evidence in Courts. Furthermore he also emphasized the issue of increased judicial oversight and the need to harmonize national legislation on the treatment of evidence gathered by intelligence services.

5 See: Handyside v. The United Kingdom, 7 December 1976, Application No. 5493/72, Series A, No. 24, p. 17, para. 48. For additional reading on the testimony of anonymous witnesses, see: Kostovski v. the Netherlands, 20 November 1989, Application No. 11454/85, Series A, No. 166, para. 42.

compromise his or her family, and may also impair his or her usefulness for future operations.[6] These exceptions can only be extended to the fight against terrorism when 'strictly proportionate to purpose, and compensatory measures to protect the interests of the accused must be taken so as to maintain the fairness of the proceedings and to ensure that procedural rights are not drained of their substance'.[7] The non-disclosure of certain evidence must be counterbalanced by the procedures followed by the judicial authorities. These procedures must be as adversarial as possible, preserve the principle of 'equality of arms', and be under judicial scrutiny at all times.[8]

2. Standards and Jurisprudence of the European Court of Justice

The ECJ jurisprudence focuses on two important issues: (1) the possibility of accepting secret evidence; and (2) the legality of executive interference with the right of the defence by intelligence activities in the scope of EU anti-terrorism policies. The United Kingdom's 'closed material procedure' (CMP), as part of the Justice and Security Act viewed through the case of ZZ. v. Secretary of State for the Home Department, provides the best example of the first issue.[9] In this case, the ECJ expressed concern that the national court was required 'to ensure that failure by the competent national authority to disclose to the person concerned, precisely and in full, the grounds on which a decision taken [...] and to disclose the related evidence to him is limited to that which is strictly necessary and that he is informed, in any event

6 See: Doorson v. the Netherlands, 26 March 1996, Application No. 20524/92, Reports of Judgments and Decisions 1996-II, para. 69. See also: A. and Others v. the United Kingdom, 19 February 2009, Application No. 3455/05, Reports of Judgements and Decisions 2009, para. 231 where the ECtHR states that 'the use of closed material gave rise to a breach of Article 6'. Here, the national proceeding also took place in the United Kingdom before the Special Immigration Appeals Commission (SIAC); the applicants claimed that the United Kingdom's derogation from Article 5(1) of the ECHR was lawful under the Anti-terrorism, Crime and Security Act (ATCSA) 2001. For more information, see: Coster van Voorhout, Jill E.B. 2006. '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) ECHR', Utrecht Law Review, Vol. 2, Issue 2, pp. 18-22.

7 Rowe and Davies v. the United Kingdom, 16 February 2000, Application No. 28901/95, Reports of Judgements and Decisions 2000-II, paras. 60-62.

8 Edwards v. the United Kingdom, 16 December 1992, Application No. 13071/87, Series A, No. 247-B, paras. 34 and 36; Bricmont v. Belgium, 7 July 1989, Application No. 10857/84, Series A, No. 158, p. 31, para. 89; and S.N. v. Sweden, 2 July 2002, Application No. 34209/96, Reports of Judgements and Decisions 2002-V, para. 44.

9 See: Case ZZ v. Secretary of State of the Home Department, 4 June 2013, C-300/11.

of the essence of those grounds in a manner which takes due account of the necessary confidentiality of the evidence'. The judgment resolved the preliminary ruling promoted by the Court of Appeal (England and Wales, Civil Division) relating to the decision to refuse an EU citizen admission into the United Kingdom on public security grounds. The prior appeal took place before the Special Immigration Appeals Commission (SIAC), where the Secretary of State invoked the confidentiality of material and its treatment as 'closed material'. Based on this case, the ECJ has also accepted the extreme measure of employing 'secret evidence' in the courtroom where intelligence information acquired for 'national security' purposes is concerned, while continuing to respect human rights standards. Regarding the second issue, the central case from the ECJ jurisprudence is the 'Kadi case'[10] or the Kadi trilogy.[11] The court ruled on whether a United Nations Security Council resolution should have primacy over EU law. The case is important because, despite criticism, the court indicated that it would allow Security Council measures to take precedence over EU law only if sufficient safeguards for human rights were established. With this in mind, the ECJ found an appropriate balance between the constitutional core values of the EU Charter of Fundamental Rights and effective international measures against terrorism. Furthermore, the developments following the Kadi case reiterated the importance of effective judicial protection as a key EU principle. The case's relevance stems from the ECJ's stance on the fundamental rights of the individual and the development of supranational standards regarding the use of 'intelligence information' in proceedings before European courts, which demonstrate that, irrespective of international obligations, respect for fundamental rights lies at the very foundations of the EU's legal order, including those enshrined in Article 6 of the Treaty on the European Union and the EU Charter.

10 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.

11 Kadi was identified by the UN Security Council as a possible supporter of Al-Qaida and therefore singled out for sanctions and, in particular, for his assets to be frozen. The EU transposed this UN sanction into a regulation that Kadi then attacked before the EU Courts. In the first instance, the General Court refused to review the EU regulation because this would constitute a review of a Security Council measure. The General Court did, however, examine whether the Security Council had respected jus cogens, in particular certain fundamental rights, but it did not find an infringement of this principle.

3. Treatment of Intelligence-gathered Evidence in Europe: National Security Cases, Judicial Assessment, Evidentiary Rules, and Procedural Safeguards

In most countries in Europe, there is a clear line between criminal law enforcement and intelligence gathering. By law, intelligence agencies have very restrictive power and detailed duties and responsibilities; they are strictly separated from law enforcement authorities and the information they are responsible for gathering serves a different purpose: the protection of national security. Of note, several European intelligence agencies, especially internal security services (for example, in Poland, Denmark, Ireland, and Latvia), have law enforcement competencies, particularly in relation to so-called crimes against the state or national security crimes (such as espionage, subversion, terrorism, or the disclosure of classified information). In these countries, transferring intelligence information related to these matters to the 'regular' law enforcement authorities, such as the police or the public prosecution office, to instigate criminal prosecution or for the information to be used in a trial is very difficult compared with the United States, the United Kingdom, or the Netherlands. Even common law countries specify the treatment and use of intelligence-gathered evidence in court. In Europe, the ECtHR's resistance to establishing stricter evidentiary rules is partly linked to ongoing differences between Council of Europe member states regarding the regulation of evidence in criminal cases.[12]

3.1. The use of intelligence-gathered evidence in court

Countries use different models to stipulate the use of intelligence-gathered evidence in court. In the first model, countries[13] have amended their respective codes of criminal procedure by expanding the scope of classic criminal investigations to include 'proactive criminal investigation', which includes the use of intelligence information to trigger an investigation.[14] The objective of these investigations is to

12 See: J. Bentham. 1988 (1781). The Principles of Morals and Legislation, Amherst, New York: Prometheus Books; J. Bentham. 1837. Principles of Judicial Procedure, The Works of Jeremy Bentham, vol. 2; and J. Bentham. 1827. Rationale of Judicial Evidence, The Works of Jeremy Bentham, Vol. 6.

13 Austria, Denmark, Germany, Slovenia, Serbia, and Spain.

14 Strictly speaking, a proactive criminal investigation responds to a situation that excludes clearly established indications of reasonable suspicion that a crime has been committed, is about the be committed, or that a specific act has taken place, nor are there any suspects.

prevent the preparation or execution of a serious crime and to enable the initiation of a criminal investigation against the organization and/or its members. As a result of these reforms, the mandate and competencies of the regular law enforcement authorities has shifted to make them more proactive (conducting more preventive investigations in response to high crime rates) and less reactive (carrying out fewer crime investigations), with the increased use of certain coercive measures such as special investigative measures, which still require prior authorization from the court.

In countries using the second model,[15] intelligence reform has led to changes in the mandate and power of intelligence services. This model aims to include intelligence agencies within the scope of law enforcement agencies under the jurisdiction of the specialized public prosecution office in the preliminary investigation. This approach empowers the intelligence agencies to implement coercive measures – the same as those enforced by the law enforcement authorities under the code of criminal procedure and relevant police laws – thus changing their nature and competencies. In this time frame, they are authorized to collect information and use certain coercive criminal procedure measures to prevent the preparation or execution of a crime. Hungary is one example of a country applying this model; it has expanded the regulations of the Public Prosecution Office, authorizing it to use the secret service and the law enforcement authorities (police, customs, and military police) to collect information. The secret collection of information has two separate regimes. The first category does not require a warrant and includes the use of informers and undercover agents, the general surveillance of persons and premises, and certain forms of wiretapping. The second category requires a warrant or the authorization of the Minister of Justice and includes the surveillance and searching of private homes and telecommunication interception. Secret information can continue to be gathered until the initiation of a judicial investigation. Once a judicial investigation is triggered, the judicial authorities can secretly obtain data by intercepting telecommunications, conducting searches, and so on; however, both sets of measures require a judicial warrant.[16]

In the third model – which is applied in countries like the United States, Belgium, the United Kingdom, and the Netherlands – the competencies of the law enforcement authorities and the intelligence agencies overlap. This refers to the open flow of information between the intelligence and law enforcement communities or the transfer of information between the law enforcement authorities and intelligence

15 Hungary, Sweden, Belgium, and Italy.

16 See: M. Damaška. 2001. 'Dokazno pravo u kaznenom postupku: oris novih tendencija, Pravni fakultet u Zagrebu; и Ž. Karas, Neke primjedbe o izdvajanju nezakonitih materijalnih dokaza, Policija i sigurnost', Vol. 21, No. 4, pp. 753-774.

community in both directions to initiate police investigations related to organized crime and terrorism. This exchange of information is facilitated through the establishment of shared databanks (such as the Counterterrorism Information Box – CT Infobox – in the Netherlands) and expert centres to deal with serious crimes or terrorism: l'Organe de coordination pour l'analyse de la menace (OCAM) in Belgium; the Nationaal Trainingscentrum (NCT) and the Financial Expertise Center (FEC) in the Netherlands; and the Joint Terrorism Analysis Centre (JTAC) in the United Kingdom. In the United Kingdom, JTAC is referred to in the context of the mandatory preparatory hearings under the 2006 Terrorism Act. These countries have a strong and coordinated intelligence community – with no significant organizational division between the intelligence community and regular law enforcement such as the police. For example, the US National Security Agency, the Defense Intelligence Agency, and the National Reconnaissance Office have intelligence units within the Department of State, the FBI, the Department of the Treasury, the Department of Energy, and the armed forces, but there are still strict distinctions with respect to objectives, methods, and control.

3.2. National experiences

Observed through the lens of evidentiary rules and the admissibility of evidence, some countries have more legal barriers than others affecting the use of intelligence-gathered evidence in court; certain countries only allow the use of intelligence-gathered evidence as legal evidence in proceedings after the completion of a 'proportionality' test between the protected public interest and the protected human right.[17]

Austria applies the rule of proportionality when assessing the admissibility of evidence obtained by the intelligence service. Nevertheless, the case of Austria is noteworthy in the context of removing barriers to the exchange of information between intelligence and law enforcement authorities in activities related to preventing terrorism or investigating organized crime. The judge applies the principle of proportionality by balancing the conflicting interests of a specific case; if they consider – for example, in organized crime cases – that the interests of the criminal prosecution outweigh other interests – for example, the right to privacy or similar – the judge

17 See: I. Martinović, D. Kos. 2016. Nezakoniti dokazi: teorijske i praktične dvojbe u svjetlu prakse Evropskog suda za ljudska prava, Hrvatski ljetopis za kaznene znanosti i praksu, br.2.; I. Bojanić, Z. Đurđević, Dopuštenost uporabe dokaza pribavljenih kršenjem temeljnih ljudskih prava, Hrvatski ljetopis za kazneno pravo i praksu (Zagreb), Vol. 15, broj 2/2008, str. 973-1003. See more at J.A.E. Vervaele. 2005. 'Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?', Utrecht Law Review, Vol. 1, Issue 1.

will allow the presentation of evidence obtained by the intelligence services.[18] Austrian intelligence and law enforcement agencies collect and process information to fulfil certain objectives (such as preventing corruption or protecting the constitutional public order). Traditionally, intelligence agencies cannot use standard intrusive measures of investigation in criminal procedures (such as search and seizure) or new ones (such as infiltration). They do, however, have general surveillance powers and can apply certain intrusive measures of a preventive nature (such as physical searches or the seizure of dangerous goods), and in serious crime investigation cases (such as organized crime or corruption) they can share intelligence information with the law enforcement agencies which can aid their investigation. The admissibility of the evidence shared by the intelligence agency is then scrutinized by the court using the principle of 'balancing or proportionality' to determine its admissibility.[19] Even in criminal investigations related to the prevention of terror-related crimes or crimes perpetrated by organized crime syndicates, which are prepared and/or executed by a criminal organization or a terrorist organization, the transfer of information between the intelligence and law enforcement authorities leads to the investigation being converted from a reactive criminal investigation into a proactive/ preventive one, to protect the interests of national security.

Belgium has taken a more moderate approach by increasing intelligence-led investigations and cooperation between the intelligence services and the law enforcement authorities by providing a double file.[20] A double file is consisted of a classified file which contains the modus operandi of the proactive investigation methods undertaken by the law enforcement authorities and a non-classified file, opened to the public with the results of the proactive investigation. In contrast with the Netherlands and Spain, the classified file is under complete judicial scrutiny and available only to the court, the second file is part of the adversarial procedure and it is available to all the parties of the procedure; while the results of the investigation can be used as evidence, the judgment cannot be based exclusively on this evidence'.[21]

18 D. Novosel. 2017. 'Use of Classified Data in the Criminal Procedure- Experiences and Method of Work in the Republic of Croatia', Journal of Criminal Law and Criminology, No. 2. Available at: www.journal.maclc.mk.

19 Code of Criminal Procedure of Austria. Available at: https://www.legislationline.org/download/id/8549/file/Austria_CPC_1975_am122019_de.pdf (Accessed on 14 July2021).

20 European Union Agency for Fundamental Rights. Presumption of innocence, procedural rights in criminal proceedings (accessed 14 July 2021). Available at: https://fra.europa.eu/sites/default/files/fra_uploads/belgium-2021-country-research-presumption-innocence_en.pdf.

21 J. Vervaele. 2005. 'Terrorism and information sharing between the intelligence

Croatia's criminal justice system has also undergone a major reform, shifting from the inquisitorial to the adversarial model of procedure. While Croatia's intelligence services do not have law enforcement or coercive powers (power of arrest), they are authorized to use special measures to collect information – sometimes referred to as 'coercive measures' (such as communication intercepts or secret surveillance). Their tasks include the prevention of terrorism and organized crime, and they have the competence to secretly collect data.[22] Nevertheless, the intelligence service must follow a specific warrant procedure determined by the Supreme Court of Croatia to use certain measures stipulated in Article 33 of the Law on the Security and Intelligence System. These measures include covert surveillance of the content of communications, postal and other items, and the inside of homes.[23] (The intelligence service does not have to acquire a Supreme Court warrant to use the other special investigative measures.[24]) The warrant has to be issued by a Supreme Court judge; however, the standard of proof for obtaining this warrant is not based on reasonable suspicion. The intelligence agency only needs to indicate the persons and/or organizations subject to surveillance, the purpose of the surveillance, and the necessary surveillance measure.[25]

The case of Dragojevic v. Croatia illustrates the need for detailed judicial scrutiny in applying such measures. The orders issued by the investigating judge were based only on a statement referring to the requests of the public prosecutor's office and the assertion that 'the investigation could not be conducted by other means', without any details of whether less intrusive means were available.[26] The investigating judge's approach was endorsed by both the Supreme Court and the Constitutional Court. 'In an area as sensitive as the use of secret surveillance, the [ECtHR] had difficulties accepting such an interpretation of the domestic law, which envisaged and required prior detailed judicial scrutiny of the proportionality of the use of secret surveillance measures.'[27] It can be argued that the domestic

and law enforcement communities in the US and the Netherlands: emergency criminal law?', Utrecht Law Review, Vol 1, Issue 1, p. 8.

22 See: M.O. Damaska, Mješanju inkvizitornih i akuzatornih procesnih formi, Hrvatski LJetopis za Kazneno Pravo I praksu, br. 2/1997.

23 Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske, NN 79/06, 105/06. Available at: https://www.zakon.hr/z/744/Zakon-o-sigurnosno-obavje%C5%A1tajnom-sustavu-Republike-Hrvatske.

24 See: Đudevic, Z. Osvrt na rezultate rada radne skupine Ministarstva pravosuđa za usklađivanje Zakona o kaznenom postupku s Ustavom Republike Hrvatske, Hrvatski LJetopis za Kazneno Pravo I praksu, br. 1/2013.

25 Ibid.

26 See: Dragojevic v. Croatia, Application No. 68955/11 (accessed 16 July 2021). Available at: https://cyrilla.org/api/files/1580906744825830sv0rpwyq.pdf.

27 ECtHR. 2015. 'Insufficient reasons given by Croatian courts when ordering telephone tapping of drug-trafficking suspect', press release.

courts' retrospective justification for circumventing this requirement opened the door to arbitrariness and did not provide adequate safeguards against potential abuse.[28] Most importantly, the ECtHR reiterates that the relevance of evidence, excluding the contested evidence, will depend on the circumstances of each individual case. In this particular case, where the substance of the recordings provided accurate and reliable evidence, the need for supporting evidence was correspondingly weaker. In view of the above, the court found nothing to substantiate the allegation that the applicant's defence rights were violated based on the evidence adduced or that the domestic courts' evaluation of the evidence was arbitrary. The court concluded that '... the use of the impugned recordings as evidence did not deprive the applicant of a fair trial.' There was therefore no violation of Article 6, paragraph 1 of the Convention. Although the standards from this case can be applied to other intelligence cases involving judicial scrutiny in applying special investigative measures, mutatis mutandis can be directly applied to this case.

Interestingly, the German doctrine of measuring or balancing has also been adopted in Croatian legislation. Thus, the fundamental rule for excluding evidence is set forth in the Croatian Constitution; Article 29, paragraph 4 envisages that '[e]vidence obtained illegally may not be admitted in court proceedings'. The absolute character and unclear definition of this rule in the constitution resulted in it being transposed into Article 9 of the Law on Criminal Procedures of Croatia of 1997; however, this led to many practical problems (such as limiting the efficiency of the criminal prosecution in cases of organized crime and corruption in Croatia).

The second most important reform of the procedural legislation – considering that enhancing the efficiency and effectiveness of criminal prosecution was one of the main conditions for the integration of Croatia into the European Union – was the fundamental change to the rules on excluding evidence from criminal procedures. The 2008 Law on Criminal Procedure therefore introduced for the first time the model of 'balancing' or 'measuring'; this approach was to be applied to all types of evidence, excluding evidence that is considered a part of the private (intimate) sphere according to German doctrine, i.e. evidence obtained by torture or any other inhuman or degrading treatment. This provision was, however, annulled by the Constitutional Court of

28 For more information, see: DCAF – Geneva Centre for Security Sector Governance. 2019. Benchbook on the Implementation of the Measures for Interception of Communications. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/ENG%20Benchbook%20on%20implementation%20of%20measures%20for%20interception%20of%20communication%20e-book.pdf. See also: Columbia Global Freedom of Expression. n.d. 'Dragojević v. Croatia' (Accessed on 21 September 2021). Available at: https://globalfreedomofexpression.columbia.edu/cases/dragojevic-v-croatia/.

Croatia, with the reasoning that the rule of 'balancing' or 'measuring' and the proportionality test must not be applied in cases of violations of human dignity.[29] After the adoption of the amendments to the Law on Criminal Procedure of Croatia, the relevant provisions were amended; in practice, the application of this doctrine is regulated by dividing illegal evidence into four categories. The first category comprises evidence obtained by torture or any other inhuman or degrading treatment. The second category comprises evidence obtained by violating the defendant's rights to defence of the defendant; damaging their reputation or honour; or infringing upon the principle of the inviolability of their personal and family life – except in cases involving evidence obtained for serious crime cases in which the interests of the criminal prosecution prevail over the violated right. While this theoretically opens the possibility of allowing intelligence information (for example, from communication intercepts) to be used in Croatia's criminal proceedings, other obstacles exist. For example, while judges may be granted access to classified information, there is no legal basis for including classified content in a judicial ruling or for providing the defendant with access to classified content, as classified information is protected under law (Law on Classified Information). If the producer/owner of the classified information were to declassify the information, however, it would open the possibility of allowing it to be used in a court proceeding. Nevertheless, in the context of this category of evidence, the principle of proportionality may be applied with regard to evidence obtained by torture or any other inhuman or degrading treatment, provided the judgment is not exclusively based on such evidence (Article 10, para. 4 of the Law on Criminal Procedure). The third category of illegal evidence consists of evidence obtained by violating provisions governing the criminal procedure; in these cases, the doctrine of 'balancing' cannot be applied, since the legislator that proscribed the provisions of the criminal procedure has already weighed out these interests. The fourth category of illegal evidence is evidence derived from the 'fruit of the poisonous tree' doctrine, the application of which, according to Croatian literature and the case law of the Supreme Court of Croatia, is rather limited.[30]

In **Germany** and Central and South-east European countries the admissibility of evidence is primarily regulated by law, with procedural laws containing strictly defined provisions. The present-day Federal Law on Criminal Procedure in Germany completely prohibits the use of evidence obtained through torture or any other inhuman and

29 See: Constitutional Court of Croatia, Ruling, 19 July 2012, Case No. U-I-448/2009, U-I-602/2009, U-I1710/2009, U-I-18153/2009, U-I5813/2010, U-I-2871/2011.

30 See: Kalajdziev, G., Arifi, B., Marsavelski, A., Bozhinovski, A. 2018. Inadmissible Evidence in the Criminal Procedure – Legal Analysis, OSCE Mission to Skopje publication.

degrading treatment that violates the defendant's fundamental rights.[31] Regarding intelligence-gathered information pertaining to the prevention of terrorism and organized crime, however, the German law invokes the so-called measuring or balancing theory (Abwägungslehre), i.e. the 'proportionality' test. According to this doctrine, minor legal violations concerning the gathering of evidence will be tolerated in more serious criminal cases. The principle of proportionality is supported by the need to ensure a balance between the protection of human rights and freedoms, on the one hand, and effective criminal prosecution, on the other.[32] Thus, in accordance with the principle of proportionality, the intensity and nature of the violation of rights is far less significant than the gravity of the crime in terms of proving whether the evidence obtained by violating such rights is permitted. Violations by intelligence services of the proscribed procedure for obtaining and presenting evidence are therefore not always considered grounds for declaring this evidence illegal. The evidence is instead assessed on a case-by-case basis. Even today, Germany does not have a fully comprehensive system of legal rules governing the issue of excluding intelligence-gathered evidence as inadmissible evidence. In fact, most of the standards have been developed under the case law of German courts, which has rejected the automatic legal prohibition of the use and presentation of intelligence-gathered evidence, as determined by law, and introduced a new approach to this issue. The reasons for this relate to the differing purposes of the exclusionary rules of 'illegal' evidence;[33] in the accusatory system of Anglo-Saxon law, rules excluding evidence from a criminal procedure are primarily aimed at preventing law enforcement bodies from obtaining evidence in an illegal manner while the German procedure prioritizes enabling the court to establish the material truth.

Italy has a dualist legal system, which includes not only the standard criminal procedure law but also special criminal legislation against the Mafia. The country has an elaborate set of proactive criminal law instruments. Individual preventive measures are envisaged under the Italian Law on Criminal Procedure including special surveillance by the police, limited free movement, and house arrests.[34] The measures are not based on reasonable suspicion but on suspected ties to organizations linked to organised crime.

31 German Code on Criminal Procedure (Strafprozeßordnung), available at: https://www.gesetze-im-nternet.de/englisch_stpo/englisch_stpo.html

32 See: Šečić v. Croatia, 31 May 2007, Application No. 40116/02. For additional reading, see: I. Bojanić/Z. Đurđević, p. 974.

33 See: I. M. Schaal. 2002. Beweisverwertungsverbot bei informatischer Befragung im Strafverfahren, Tenea, p. 66.

34 See: Italian Code of Criminal Procedure, 124/2007.

Over time, the preventive measures were extended further to include anti-terrorism measures after the ratification of the EU Framework on the European Arrest Warrant. These preventive measures – aimed at gathering information to prevent serious crimes – require no warrant, even to search private homes without significant evidence that a serious crime has taken place, and have longer durations.[35] To implement these measures in relation to not only terrorist acts but also ordinary criminal investigations, it is sufficient to demonstrate that indications of a crime exist, based on reasonable suspicion. Intelligence agencies are mandated to intercept communications under the authorization of the Public Prosecution Office, but the information obtained through such intelligence gathering cannot be used in the pre-trial or trial procedure.[36] The Italian Code of Criminal Procedure has a very open and unique solution for the treatment of intelligence information as evidence in court. The law imposes a partial rather than an absolute ban on the use of intelligence as evidence in court. The existing provisions allow the source of intelligence-gathered evidence to be heard and cross-examined in court. Furthermore, the Code of Criminal Procedure stipulates that the raw data gathered by intelligence services can only be used to trigger judicial investigations; the information cannot form part of the pre-trial or trial procedure. The Italian Supreme Court also decided that the blacklisting of terrorists or terrorist organizations cannot be used as evidence in court.[37]

The Netherlands stands out in this regard as a country that comprehensively introduced the new concept of proactive enforcement in its Law on Criminal Procedure. To understand the use of intelligence-gathered evidence in trials in the Netherlands, it is important to examine two key laws: the Code of Criminal Procedure[38] and the Act on Shielded Witnesses.[39] In 1999, the Code of Criminal Procedure of the Netherlands introduced special investigative techniques, such as

35 M. Nino. 2007. 'The Abu Omar Case in Italy and the effects of CIA renditions in Europe on Law Enforcement and Intelligence Activities', Revue Internationale de Droit Pénal, Vol. 78 (1-2), pp. 113-141.

36 Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske, NN 79/06, 105/06. Available at: https://www.zakon.hr/z/744/Zakon-o-sigurnosno-obavje%C5%A1tajnom-sustavu-Republike-Hrvatske.

37 For more information, see: D. Pulitano, 2009. 'Sicurezza e diritto penale'. Rivista italiana di diritto e procedura penale 52(2), pp. 547-568; K. Nuotio. 2013. 'Security and Criminal Law: A Difficult Relationship', in M. Fichera and J. Kremer, eds. Law and Security in Europe: Reconsidering the Security Constitution (Cambridge, Antwerp, and Portland: Inersentia).

38 Dutch Code of Criminal Procedure (accessed 15 July 2021). Available at: https://www.legislationline.org/download/id/6416/file/Netherlands_CPC_am2012_en.pdf. Articles 226g-226m are relevant to the protection of intelligence officers.

39 Shield Witnesses Act, Kamerstukken II 2003-2004, 29 743, no. 1; Kamerstukken II 2003-2004, 29 743, no. 2; Kamerstukken II 2003-2004, 29 743, no. 3; Kamerstukken II 2003-2004, 29 743, No. 4, Wet afgeschermde getuigen.

observation, infiltration, wiretapping, and systematic and electronic surveillance, to combat organized crime and terrorism. These measures can be used only after the examining judge has verified whether the legal prerequisites for such an intrusive measure have been met. The reform of the Code of Criminal Procedure introduced new procedures to allow, in cases of criminal investigations of terrorist crimes, intrusive measures to be lawfully applied against a person based on reasonable suspicion – rather than in response to indications of the perpetration and/or planning of a terrorist offence. The threshold for the use of these measures depends on indications of a terrorism-related crime in addition to a reasonable suspicion of a crime being committed or a reasonable suspicion that crimes are being plotted or committed in an organized context.[40]

Dutch intelligence officers have no jurisdiction to investigate criminal offences.[41] The exchange of information between the Dutch Intelligence Service and the law enforcement agencies is strictly regulated. Cooperation is a one-way process: intelligence services can provide information or a lead to the police regarding a criminal investigation, but they are not obliged to inform law enforcement agencies. On the other hand, the police and the prosecution have a duty to inform the intelligence services.[42] The Dutch Law on Criminal Procedure envisages that the special units of the Dutch police may gather criminal intelligence concerning organized crime and terrorism. Separate regional police departments have their own special unit, but similar units also exist at the national level – for instance, the National Criminal Investigation Department, the military police, the Governmental Investigation Department, and the Revenue Department. Reports/information from the Dutch Criminal Intelligence Unit (CIE) may be used as a tip-off for criminal investigations and may give rise to 'reasonable suspicion', initiating a prosecution.[43] The Dutch Law on Criminal Procedure also allows threatened witnesses[44]

40 J.A.E. Vervaele. 2005. 'Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?', Utrecht Law Review, Vol. 1, Issue 1, pp. 1-27. For more information, see: Jill E.B. Coster van Voorhout. 2006. 'Intelligence as 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) ECtHR', Utrecht Law Review, Vol. 2, Issue 2, pp. 18-22.

41 Dutch Code of Criminal Procedure (accessed 15 July 2021). Article 9.

42 Article 17 and Article 15(2) of the Police Files Act (Wet op de politieregisters). See also: J. Vervaele. 2005. 'Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?', Utrecht Law Review, Vol. 1, Issue 1, p. 6.

43 Article 27 of the Law on Criminal Procedure of the Kingdom of the Netherlands (Accessed on 21 September 2021). Available at: https://www.legislationline.org/download/id/6416/file/Netherlands_CPC_am2012_en.pdf.

44 The protection of threatened witnesses was first addressed by the courts, and

and informants of the special police units to be heard anonymously or through the use of protective measures in court. The final report of the special units, however, has no probative value[45] and may not be adduced as evidence at trial. Nevertheless, Dutch judicial practice allows the heads of regional special police units to testify before the court, and their testimony is admissible as evidence. They reserve the right to not answer any questions that might reveal the source, even where informers are concerned. The court may require the defence not to ask any questions that might reasonably endanger ongoing investigations. When it comes to the direct use of intelligence as evidence in court, however, the Dutch jurisprudence has moved away from its earlier stance that grounds for reasonable suspicion may not be based exclusively on evidence gathered from intelligence services.[46] Dutch courts were very careful to examine intelligence-gathered evidence in depth in cases of gross human rights violations to prevent unfair trials. Under the new paradigm of anti-terrorism legislation, however, the Supreme Court of the Netherlands ruled that intelligence can be used as evidence in criminal proceedings, but only under the presumption that there is no stipulated legal norm/rule prohibiting the use of such intelligence as evidence.[47] A legal basis must therefore exist in order to use items or information as evidence. Rather than identifying a legal rule that enables the use of intelligence as evidence, it states that the courts have a duty to investigate, on a case-by-case basis, whether intelligence may be adduced as evidence, and that it must fulfil the fair trial requirements of Article 6 of the ECHR.[48]

The second important and sui generis legal solution in the Dutch legal

subsequently laid down and extended in the Witness Protection Act (Wet getuigenbescherming, Wet van 11 November 1993, Staatsblad 603) after the ECHR judgment in Kostovski v. the Netherlands, 20 November 1989, ECtHR. For further reading, see: J. Vervaele. 2005. 'Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?', Utrecht Law Review, Vol. 1, Issue 1, p. 6.

45 Probative value, or the value of the evidence, can be defined as evidence that is sufficiently useful to prove something important in a trial. Whether some evidence has a probative value can only be determined by the presiding judge in the case.

46 Supreme Court of the Netherlands, LJN No. AF2141, case no. 10/150080/0

47 Supreme Court of the Netherlands, LJN No. AV4122 and LJN No.AV4144 (accessed 14 July 2021). Available at: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2006:AV4122. For more information, see: Jill E.B. Coster van Voorhout. 2006. 'Intelligence as 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) ECHR', Utrecht Law Review, Vol. 2, Issue 2, pp. 18-22.

48 J. Vervaele. 2005. 'Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?', Utrecht Law Review, Vol. 1, Issue 1, p. 6.

system is the Act on Shielded Witnesses.[49] This piece of legislation made certain changes to key provisions of the Law on Criminal Procedure.[50] The Act empowers the pre-trial judge to legally withhold any evidentiary material (usually the testimony from an intelligence officer or the heads of special police units) from the public – including other participants of the criminal procedure – for the protection of national security. The intelligence officer testifies before the pre-trial judge and must give their written consent to the transcript of the testimony being provided to the defence and the prosecution as parties to the procedure and being used as evidence. The trial judge also receives the transcript and testimony documents for which the intelligence officer provided consent. Furthermore, the pre-trial judge can be summoned as a witness to corroborate the testimony, but this Act restricts them from providing any details that may compromise the intelligence officer's identity. Written or hearsay evidence (de auditu) is allowed in the Netherlands. The transcript of the intelligence officer is therefore permitted as evidence in court if it fulfils two legally stipulated criteria: (1) the witness (intelligence officer) was heard following the criminal procedure; and (2) the crime for which the defendant is prosecuted is a high crime with a minimum jail sentence of five years.[51]

The **Serbian** Law on Criminal Procedure stipulates the widest encompassing exclusionary rule of illegal evidence, compared to other countries in the Western Balkan region. There is no law or clear rule regulating the use of intelligence-gathered evidence. According to Article 16, paragraph 1 of the Law on Criminal Procedure, '[c]ourt decisions may not be based on evidence that is, directly or indirectly, in itself or by the manner in which it was obtained, in contravention of the Constitution, this Code, other statute or universally accepted rules of international law and ratified international treaties, except in court proceedings in connection with the obtaining of such evidence'.[52] The use of intelligence-gathered evidence, however, amounts to a relative rather than an absolute violation of the provisions of the criminal

49 English version of the Act on Shielded Witnesses (accessed 14 July 2021). Available at: https://zoek.officielebekendmakingen.nl/kst-29743-7.html.

50 Amendments to Articles 187d, 226g-226m, 226b, 178a, 226a of the Dutch Code of Criminal Procedure.

51 Kamerstukken II 2003-2004, 29 743, no. 2, Kamerstukken II 2004-2005, 29 743, the Heads of the public prosecution office, available at: www.om.nl/files; T. Prakken. 2004. 'Naar een cyclopisch (straf)recht', Nederlands Juristenblad, No. 45; Y. Buruma and E.R. Muller. 2003. 'Wet TerroristischeMisdrijven in perspectief', Nederlands Juristenblad, No. 40, available at: publicaties/rechtsbescherming_op_de_helling.pdf.

52 Law on Criminal Procedure of Serbia. Available at: https://www.legislationline.org/download/id/3560/file/Serbia_2011%20CPC%20English_.pdf.

procedure.[53] Under Article 438, paragraph 1, sub-paragraph 1, the law explicitly envisages an exception according to which there shall be no substantive violation of the provisions of the criminal procedure despite the fact that the judgment is based on inadmissible evidence, in accordance with the provisions of the Law on Criminal Procedure. This means that the court may issue a judgment based on inadmissible evidence if other evidence also supports the facts of the case.

According to the **Slovenian** Law on Criminal Procedure, '[t]he court may not base its decision on evidence obtained in violation of human rights and basic freedoms provided by the constitution, nor on evidence which was obtained in violation of the provisions of criminal procedure and which under this Law may not serve as the basis for a court decision, or which were obtained on the basis of such inadmissible evidence'.[54] The first part of this provision may be interpreted as permitting the application of the proportionality test. The second part of this provision only excludes the use of evidence obtained in contravention of the provisions of the Law on Criminal Procedure, which the judgment may not be based on according to the Act; in principle, this allows for the use of other evidence, in spite of the same procedural violations related to obtaining such evidence. It is also important to consider the preceding paragraph of the same article, which states that the right of the court 'to evaluate the facts presented shall not be bound, or limited by any specific formal rules of evidence'. Thus, Article 18, paragraph 1 of the Law on Criminal Procedure potentially allows flexibility with respect to the admissibility of evidence.

In **Spain**, despite the considerable number of amendments to the Criminal Code and the Code of Criminal Procedure, no regulation on the use of intelligence information in court exists. The law on intelligence includes a provision that defines cooperation between intelligence and law enforcement services, as well as the admissibility of intelligence as evidence under the scope of the Council's Framework decision on simplifying the exchange of information and intelligence between law enforcement agencies.[55] Although there are no specific provisions in the Spanish Code on Criminal Procedure, in judicial practice, intelligence reports are frequently considered as expert

53 Advokatska komora Srbije, Projekat reforme krivičnog zakonodavstva: konačan izvještaj 2016 godina, Beograd, p. 48.

54 Article 18, para. 2 of the Law on Criminal Procedure of Slovenia. Available at: https://www.legislationline.org/download/id/9233/file/SLOV_CPC.pdf.

55 Spanish Code on Criminal Procedure 11/2002, 6 May, on the regulation of the National Intelligence Centre. See also: Mar Jimeno Bulnes. 2017. 'The use of intelligence information in criminal procedure: A challenge to defence rights in the European and the Spanish panorama', New Journal of European Criminal Law, Vol. 8, No. 2, June, pp.171-191.

evidence with additional special features.[56] In judicial practice, intelligence reports are categorized in the same way as testimonial and expert evidence. The defence is, however, unable to cross-examine the intelligence officer, therefore does not fully comply with the principle of contradiction and rules on confrontation during proceedings.[57] Such unwillingness to disclose intelligence sources to the accused is justified on the grounds of protecting national security, which is argued to be of overriding importance to fundamental rights. However, in its ruling, the Spanish Supreme Court stressed the importance of police reports that referred to intelligence work, since they contribute specific technical knowledge (expertise) to criminal procedures. Its decision implied the use of intelligence information, qualified as expert evidence, in terrorism-related cases.[58]

The United Kingdom has specific legislation for ramification of classified intelligence information as evidence in criminal proceedings. Intelligence services can share their intelligence with the law enforcement authorities. However the law enforcement authorities cannot directly use this intelligence, but are required to conduct their own investigation and build an eventual case, as direct intelligence was not admissible in court.[59] Closed material procedures and the admissibility of written testimony by intelligence officers in court envisaged in the Justice and Security Act of 2013 are important components for the admission of intelligence-gathered evidence in court.[60] Firstly, the closed material procedures are secretive, but the judge and the security-cleared special advocates are given access to sensitive intelligence materials. The judge has the power to decide, at the request of the government, whether to present evidence to the court in secret without the defendant being granted access to that

56 R. Castillejo Manzanares. 2011. 'La prueba pericial de inteligencia', Diario La Ley, 16 December, No. 7756. Available at: http://diariolaley.laley.es. See also: Mar Jimeno Bulnes. 2017. 'The use of intelligence information in criminal procedure: A challenge to defence rights in the European and the Spanish panorama', New Journal of European Criminal Law, Vol. 8, No. 2, June, pp.171-191.

57 See: Alonso R. Peña Cabrera Freyre. 2013. 'El Derecho penal del enemigo y su influencia en la legislacio´n penal', Jueces para la democracia, No. 77, pp. 49–72. See also: C. Walker. 2010. 'Conscripting the Public in Terrorism Policing: Towards Safer Communities or a Police State?', Criminal Law Review, No. 6; and Mar Jimeno Bulnes. 2017. 'The use of intelligence information in criminal procedure: A challenge to defence rights in the European and the Spanish panorama', New Journal of European Criminal Law, Vol. 8, No. 2, June, pp.171-191.

58 See the Supreme Court search form. Available at: http://www.poderjudicial.es/search/index.jsp. See also: Mar Jimeno Bulnes. 2017. 'The use of intelligence information in criminal procedure: A challenge to defence rights in the European and the Spanish panorama', New Journal of European Criminal Law, Vol. 8, No. 2, June, pp.171-191.

59 Ibid.

60 Justice and Security Act. Available at: www.legislation.gov.uk/ukpga/2013/18/contents/enacted/data.htm.

information. The Justice and Security Act therefore acted to codify the use of closed material procedures in any civil case in which it is argued that disclosure of the material would harm national security. The use of such procedures was first introduced by the Special Immigration Appeal Commission Act 1997,[61] which permitted the government to rely on closed material in seeking to justify deportation on national security grounds. Apart from the criminal law component, closed material procedures are envisaged in:[62]

- the Anti-Terrorism, Crime and Security Act 2001[63] which, although no longer in force, permitted the permanent detention of foreign nationals suspected of being terrorists;
- the Prevention of Terrorism Act 2005[64] and the Terrorism Prevention and Investigation Measures Acts 2011, which permitted restrictive measures to be imposed on those suspected of involvement in terrorism;
- the Counter-Terrorism Act 2008, which grants the UK Treasury the opportunity not to disclose material if contrary to the public interest;[65] and
- the Justice and Security Act of 2013 mentioned above, which extends the use of closed material procedures to the main civil courts, for example, for claims for damages concerning extraordinary rendition and alleged torture cases.[66]

During closed material procedures, when permitted, evidence may be subject to cross-examination, possibly by a special advocate – a specially appointed barrister who handles cases involving classified security information and is instructed to represent a person's interests concerning material that is kept secret from that person and his or her ordinary lawyers. The court always decides upon the admissibility of evidence in jury trials.[67] Secondly, concerning the use of anonymous

61 Special Immigration Appeal Commission. Available at: https://www.legislation.gov.uk/ukpga/1997/68/contents.

62 European Parliament Directorate General for Internal Policies – Policy Department C. 2014. National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges – Study for the LIBE Committee. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf.

63 Anti-terrorism, Crime and Security Act 2001. Available at: www.legislation.gov.uk/ukpga/2001/24/contents.

64 Prevention of Terrorism Act 2005 (repealed). Available at: www.legislation.gov.uk/ukpga/2005/2/contents.

65 Ibid.

66 Counter-Terrorism Act 2008. Available at: www.legislation.gov.uk/ukpga/2008/28/pdfs/ukpga_20080028_en.pdf.

67 'Law Commission No. 245, para. 3.37' in B. Fitzpatrick. 2002. 'Tinkering or transformation? Proposals and principles in the White Paper, "Justice for All"', Web

testimony in a trial, the Crown Prosecution Service allows intelligence officers to give evidence from behind a screen, and even grants anonymity in some cases. Nevertheless, this is only likely to be allowed if the court is satisfied that delivering the testimony in this way will not affect the truthfulness of the witness in the case, and will not prevent cross-examination from taking place. Moreover, it has been accepted in the United Kingdom that even if the evidence from anonymous witnesses might have been decisive in the case, this does not render the conviction unsafe.[68] In the United Kingdom, all relevant evidence is generally considered admissible unless it falls within one of the exclusionary rules: hearsay statements, public interest, and the very discretion of the court to exclude evidence.[69] Concerning the latter, the pre-trial testimony may, in principle, be admitted in court when it is found to be relevant; however, the court has the discretionary power to exclude evidence under common law and Section 78 of the Police and Criminal Evidence (PACE) Act 1984. The court's discretion to exclude evidence based on fairness is a long-standing judicial power that has its roots in the common law.[70] The presentation of (highly) sensitive intelligence may be excluded from the disclosure duty under public interest immunity based on the decision of the court, not that of the intelligence officer. As explained in a study commissioned by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), despite the United Kingdom's 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, 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 are properly scrutinized by judicial authorities'.[71]

However, despite the restrictive and extensive legal doctrines on the treatment and use of intelligence-gathered evidence, given the rise

Journal of Current Legal Issues. Available at: http://www.bailii.org/uk/other/journals/WebJCLI/2002/issue5/fitzpatrick5.html.

68 See: R v. Taylor and Crabb (1995) and Cooper and Schaub (1994). In R v. Taylor, the Court of Appeal set out some guidelines to assist courts in cases where the names of witnesses are withheld.

69 Under the Criminal Justice Act 1988, the court had to exercise judicial discretion based on the interest of justice before admitting hearsay evidence.

70 C. Walker. 2004. 'Terrorism and Criminal Justice: Past, Present and Future', Criminal Law Review, Supplement for the 50th Anniversary, p. 315.

71 European Parliament Directorate General for Internal Policies – Policy Department C. 2014. National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges – Study for the LIBE Committee. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf.

of domestic and international terrorism, states should have targeted mechanisms in place to allow the sharing of intelligence information between the intelligence and law enforcement community. Intelligence should be used in criminal investigations and prosecutions in a manner that respects the rule of law under both domestic and international law, in particular international human rights law.[72] However, as seen above in some countries' approaches to intelligence, a thorough reform of the legal and institutional capacities is needed to increase the efficiency of justice, protect the public interest, and at the same time guarantee procedural rights and liberties.

In the **United States**, the events of 9/11 have dramatically altered the traditional approach to terrorism-related offences by shifting the paradigm from the ordinary criminal justice system to an extraordinary model based on the interests of national security.[73] The division between intelligence and criminal enforcement is not as strict in the United States as it is in Europe; both intelligence and criminal investigations are generally deployed as preventive counter-terrorism strategies. Nevertheless, information is generally not shared – not internally in the intelligence community nor externally with law enforcement agencies. The CIPA[74] regulates the use of classified information in regular criminal trials;[75] it provides for ex parte proceedings for both parties for the use of classified information. After 9/11, the FISA[76] once again gained momentum as provisions that had been rejected earlier were adopted in the USA Patriot Act.[77] In addition to this, the Detainee Treatment Act of 2005

72 The Rabat Memorandum of Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector. Available at: https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2016%20and%20before/GCTF-Rabat-Memorandum-ENG.pdf?ver=2016-09-01-115828-653.

73 See: Fred Manget. 2006. 'Intelligence and the Criminal Law System', Stanford Law and Policy Review, Vol.17, pp. 415-436.

74 Classified Information Procedures Act (CIPA). Available at: https://www.justice.gov/archives/jm/criminal-resource-manual-2054-synopsis-classified-information-procedures-act-cipa.

75 See United States v. Truong Dinh Hung which examines the importance of CIPA's primary purpose test in gathering and presenting intelligence information in court. The court opined that so long as the primary purpose of the surveillance was the collection of national security information relating to activities of a foreign power, the resulting information could be used in the criminal case.

76 James G. McAdams, III. n.d. Foreign Intelligence Service Act (FISA): An Overview (Accessed on 25 September 2021). Available at: https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf.

77 The Patriot Act explicitly authorized law enforcement agencies to share with the intelligence community any foreign intelligence information identified as Rule 6(e) grand jury information or Title III electronic, wire, and oral interception information that had been generated by a criminal investigation.

and the Military Commissions Act of 2006[78] also offer an alternative track for investigation, prosecution, and adjudication procedures. These pieces of legislation improved the information flow between law enforcement agencies and the intelligence community and opened up new possibilities for the use of secret procedures and intelligence – generally as classified evidence – in criminal cases. In the same way that investigatory powers have been extended considerably, the grounds for using these powers have also become broader. Moreover, it is now possible to significantly restrict defence rights in the interests of national security. Nevertheless, the judiciary still sets strict requirements for these restrictions and the principle of due process has been significantly reinforced.[79] Regardless of the evidence obtained, however, all classified evidence is generally scrutinized by judges.

Conclusion

European countries have certainly made substantial changes to their criminal justice systems in response to the anti-terrorism paradigm shift, transforming the objectives, nature, and instruments of criminal law. States are nevertheless still trying to identify the appropriate model for the use of intelligence as evidence in court – one that strikes a balance between fair trial guarantees and the protection of specific interests (such as national security and public order), while conforming to the standards and principles of the ECtHR and the ECJ. Some countries have introduced measures during the trial phase to protect the identity of a witness or intelligence agent, allowing the court and defence lawyers to carry out interrogations behind a screen while ensuring anonymity. Other countries, such as the Netherlands, have adopted a different approach to the admissibility of intelligence-gathered evidence and do not prohibit it from being used as evidence in court The United Kingdom's strong judicial oversight and assessment of such information offers a positive example of how to ensure a clear balance between the public security interest and the right to a defence council, allowing intelligence information to be classified as sensitive without preventing the accused from being represented by a special advocate in closed material proceedings. Despite the backlash to the special advocate provisions, a lawyer is at least present to

78 The Military Commissions Act's primary purpose was 'to authorize trial by Military Commission for violations of the law of war and for other purposes'. It is an Act of Congress and was drafted right after the US Supreme Court's decision on the case Hamdan v. Rumsfeld in 2006 (Opinion of the Supreme Court in Hamdan v. Rumsfeld).

79 See: A. Bozhinovski. 2015. 'The Influence of Magna Carta Libertatum in the Development of the Principle of Rule of Law', SEEU Review, Special Edition, Vol. 11, Issue 1.

oppose the intelligence officer at the material proceedings. Each state must identify its own appropriate method of admitting intelligence-gathered evidence in judicial proceedings, according to their respective legal tradition and practice. Nevertheless, all legislation must comply with the three main standards of the ECHR and the criteria for a fair trial. Each legal solution must guarantee that (a) special measures have only been used as a last resort; (b) the defence has had the opportunity to examine the evidence and question witnesses; and (c) trial judges have been able to examine the evidence to ensure a fair trial. Ultimately, regardless of the measures implemented to protect witnesses or fight terrorism, the chosen model must not under any circumstances infringe criminal procedural rights.

Concerning the judicial assessment of evidence, however, the ECtHR's jurisprudence on this issue clearly indicates that, in executing the judgments of the ECtHR, the court assesses whether the overall criminal procedure was fair; in this context, evidence gathered by intelligence services through the interception of communications or the violation of citizens' privacy rights does not automatically lead to the presumption that the procedure of implementation of special investigative measures against them has been unfair. In these circumstances, the court applies the proportionality test to decide whether the infringement of a particular right guaranteed under the domestic law, constitution, or convention may be justified. With regard to Article 8, the margin of appreciation varies according to the circumstances, the case, and its background; the decision is guided by two sets of circumstances: (1) whether the infringement of a particular right is justified, necessary, and proportionate to the public interest; and (2) whether the state has undertaken sufficient measures to honour its obligations.

In examining the nature of the established violation of the convention, the court considers whether the use of intelligence information obtained by violating Article 8 (privacy) as evidence renders the trial unfair and whether it is contrary to Article 6 (fair trial), taking into consideration the circumstances of the case. The court also assesses whether the applicant's right to defence has been respected and the quality and significance of the evidence in question (i.e. its relevance to the interests of criminal justice). In the context of the right to privacy, the court has on several occasions established that this right is of secondary importance compared with the right to a fair trial and the principle of protecting the public interest, which is always the number one priority. Thus, the reform of procedural laws and other related legal solutions must incorporate the public interest as a criterion for assessing intelligence-gathered evidence in a criminal procedure. This addition would make it possible to easily establish the relevance of the infringement upon the right to privacy, particularly when evidence is linked to the perpetration of a crime. Hence, intelligence-gathered

evidence which discloses that terrorism-related crimes are being planned or committed, or have been committed by persons who seek to disrupt public order, may be used as evidence in criminal procedures before the court.

As elaborated above, most criminal procedure laws relating to the legality of intelligence-gathered evidence emphasize the manner of obtaining evidence, and not whether such evidence is in the interest of justice. When drafting future legal reforms, and in order to protect both the public interest and the rights of the accused person, legislators should primarily consider the German doctrine of 'measuring or balancing' by applying the 'proportionality test', which accepts evidence gathered by the intelligence service in certain situations, but also ensures sufficient protection of the human rights of the defendant. Different solutions could be developed to enable the application of the proportionality test and to help establish the truth in criminal procedures by expanding the rules on admissible evidence. In any case, the right to privacy and the privilege against self-incrimination do not exclude the application of unauthorized communication interception. These human rights, widely recognized in contemporary legal systems, do not incorporate a general prohibition that would preclude certain statements of the defendants from being used against them.

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva