# INTERNATIONAL TERRORISM: THE FUTURE UNCHAINED?

**Editors**
Steven W. Becker
Adjunct Professor of Law, DePaul University College of Law, Chicago
Davor Derenčinović
Professor of Law, Faculty of Law, University of Zagreb

Zagreb, 2008.

**John A. E. Vervaele**[1]

# INFORMATION SHARING BETWEEN INTELLIGENCE AND LAW ENFORCEMENT AUTHORITIES IN COMBATING INTERNATIONAL TERRORISM[2]

## 1. Introduction

The 11-S and 11-M attacks in New York, Madrid and London have raised many questions concerning the position of information of the intelligence services and concerning the possible use by them of coercive measures for the prevention and repression of terrorist offences. In many countries, the events have led to a tide of criminal law legislation to restrain terrorism. This is not only the case in the US, with its USA Patriot Act,[3] but also in Europe, both at EU level and in the Member States. The EU terrorism framework decision, imposing harmonisation of the offence of terrorism in the Member States, illustrates this trend.

The criminal prosecution of terrorism and guaranteeing security in a state under the rule of law give rise to fundamental questions concerning the constitutional freedoms and criminal law guarantees in times of crisis.

From the mid-1990s there has been a clear tendency to broaden the scope of criminal law enforcement by including pro-active enforcement. The triggering of criminal procedure and coercive measures no longer depends on the reasonable grounds to believe or suspect or on the probable cause that a crime has been committed, but on the potential danger for society arising from certain behaviour or even from certain ways of thinking. Both open and secret information gathering on societal targets have become aims of pro-active criminal investigation. In addition, the statutes of the intelligence services have been reshaped in some Member States, in order to provide the agencies with coercive powers (such as tapping, infiltration, etc.). The dividing line between the intelligence authorities and the law enforcement authorities is becoming blurred and the Chinese walls between their functioning and the data which they have at their disposal are played down for functional cooperation.

---

[1] Professor of economic and financial criminal law at Utrecht University, Professor of European criminal law at the College of Europe at Bruges.

[2] This article is an updated (up to 15 May 2007) and rewritten version of J.A.E. Vervaele. Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law? *International Review of Penal Law*, AIDP, 2005, nr. 3-4, 409-446.

[3] J.A.E. Vervaele. The anti-terrorist legislation in the US; inter arma silent leges? *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 13/2, 2005, 201-254.

Just after the coming into force of the Treaty of Amsterdam, the Heads of State elaborated a Master Plan for the Area of Freedom, Security and Justice, the Tampere Programme,[4] which was followed up in 2005 by a second term Master Plan, the Hague Programme,[5] elaborated by the EU Ministers of Justice, the Interior and Migration end approved by the Council of Ministers in November 2004. This Programme for strengthening the area of freedom, security and justice contains, besides mutual recognition, a new key concept, the principle of availability of information between law enforcement authorities. The free flow of law enforcement information became a key element in the Action Plan which was elaborated for the execution of the Hague Programme. The fight against serious crime and terrorism calls for finding the right balance between the right to privacy and the right to security. In this conceptual approach, the principle of availability becomes an executive principle of the right to security, shaped as a fundamental right. Of course, it is not conceived here as a right of individuals, but as a duty for law enforcement authorities when securing the citizen.

Information gathering, information stocking and information exchange between law enforcement authorities have become key topics in combating serious crime and international terrorism. The EU is not only aiming at the free movement of evidence in the common area of freedom, security and justice, but also at the free movement of law enforcement information and at intelligence-led criminal procedure and criminal justice.[6]

In this contribution, we concentrate on a special aspect, which is, however, on the whole illustrative of these fundamental questions. The question of what role the information gathered by intelligence services can and may play in the criminal proceedings has become topical in the investigation, prosecution and trial of suspects and accused of terrorist offences. The EU has foreseen a green paper on this topic in 2008 and as aiming at streamlining this topic in the domestic legal order of the Member States. The discussion in the EU Member States on the use in criminal proceedings of information gathered by intelligence services already dates from before 11-S. That such information can be used as a lead for initiating criminal investigations is hardly contested. Much more of a problem is, however, whether this information per se is able to give rise to reasonable suspicion or form a sufficient basis for the use of coercive measures under criminal law. It is also disputed whether such information can be used as legal proof in criminal proceedings. The question in the event of its use is also what the consequences are for the public nature and the position during the trial of the defence. In most countries there is little case law concerning this question and the discussion, both academic and practical, has yet to get into stride.

This article aims to contribute to this discussion by giving a legal analysis of the problem in the US and in Europe. Much experience has been gathered in the US in the field of intelligence sharing between intelligence and police services. There is also some interesting case law available, including Supreme Court decisions. There is very little case law in the

[4] Tampere Conclusions, 15 e 16 Octobre 1999, http://ue.eu.int.

[5] http://www.libertysecurity.org/article264.html.

[6] See point 5.

European countries on this issue and the academic debate on this topic has yet to start. In Italy, however, there has been a decision by Judge Forleo, a preliminary proceedings judge of a Milanese tribunal,[7] who on 24 January 2005 declared all foreign intelligence information inadmissible as evidence in criminal proceedings. However in another case, judge R. Spano, a preliminary proceedings judge at a Brescia tribunal decided otherwise in his decision of 31 January 2005. In any event, there is a specific rule in Italian criminal procedure concerning the production of evidence before a court. Article 203 of the Code of Criminal Procedure does not exclude the use of intelligence as evidence in court, but does submit it to the strict condition that the source of the information (including secret agents or their informants) can be heard and cross-interrogated in court at the trial hearing. Such a provision of an adversarial trial nature concerning intelligence information is quite unique in Europe. It does not, for instance, exist in Germany, where the Oberlandesgericht of Hamburg decided to make use of information of the secret services of the United States in the Motassadeq terrorist case, even without the presence of the agents as witnesses at the trial.[8]

The Netherlands is one of the few countries in the EU where the topic has become the focus of political scrutiny by the government and the parliament since the beginning of the 1990s[9] and has also led to case law and legislative proposals. Do the intelligence services[10] have a discretionary power to determine which intelligence will be provided? What is the relationship between this discretion of the intelligence services and the corresponding legal duty of secrecy on the one hand and the rights of the defence and the judicial review of the lawfulness of that information? Can criminal prosecutors blindly trust the discretionary judgment of the intelligence services and the lawfulness of the means by which the information has been gathered? Is it up to the prosecuting authorities to decide whether such intelligence is used as secret evidence? After 11-S, these questions have been partly at issue in a number of Dutch criminal cases. The Rotterdam District Court's decision at the end of 2002[11] where it was held that intelligence may serve as a lead in criminal investigations, but not as the exclusive basis for determining reasonable suspicion has been heavily criticized in the US.[12] By an expedited procedure, Minister Donner has submitted a legislative proposal concerning shielded witnesses.[13] The proposal was recently adopted by Parliament .[14] Does

[7] N. 28491/04 R.G., G.I.P.; N. 5774/04 R.G. G.I.P.

[8] OLG Hamburg, sentenza del 14 giugno 2005, IV-1/04.

[9] See L. van Wifferen (2004). Het gebruik van AIDV-informatie in het strafproces, *Justitiële Verkenningen*, no. 3, 2004, 139-140; and L. van Wifferen (2003). Intelligence in het strafproces, *NJB*, no. 12. Already in 1992, the Minister of Justice sent a Note to Parliament concerning the question whether *BVD* intelligence could form legal evidence, *Kamerstukken II*, 1991-1992, 22 463, no. 4.

[10] As of the new Intelligence and Security Services Act [*Wet op de inlichtingen- en veiligheidsdiensten (Wiv)*] of 2002, the *BVD* has been renamed the General Intelligence and Security Service [*Algemene Inlichtingen- en Veiligheidsdienst (AIVD)*].

[11] See discussion under 5.2.

[12] L. Vidino & E. Stakelbeck (2003, July 7). Dutch Lessons. *The Wall Street Journal Europe*: "This is a distressing example of the limitations placed on Dutch authorities in fighting and preventing terrorism, as intelligence agencies' efforts are all too often thwarted by liberal courts and inadequate laws."

[13] Wijziging van het Wetboek van Strafvordering in verband met het treffen van een regeling inzake het

this mean that the paradigm of security doctrine has further eroded the classic embeddedness of criminal law in the rule of law? Is the use of secret intelligence evidence an example of the Americanization of Dutch criminal (procedural) law? The comparison with the US is interesting, as precisely in the US much experience has been gained over the past 20 years in conducting the movement of information between intelligence and police services. It is also especially the US which urges European authorities to bring about a smoother flow of information within Europe. However, the comparison between the US and Europe requires a few words of explanation concerning the historical context of the cooperation between the intelligence and police services.

## 2. Information sharing between the Intelligence Community (IC) and the Law Enforcement Community (LEC): the historical background

The intelligence services have the task of recognising, based on a strong position of information, future or current threats to the democratic legal order and to alert the competent authorities thereof. The police, in the framework of its judicial function, have the task of gathering information concerning offences with a view to their eventual settlement by a criminal court. The intelligence services do not have the objective of investigating offences, while the police do not have the objective of gathering information in order to ensure a strong position of information. The tasks which the different services have been set and the manner in which they perform them are quite different and a dividing wall has been erected between the two. Information of intelligence services is principally secret. Police information is subject to judicial testing as criminal evidence in the publicly accessible courtroom.

Nevertheless, the historical distinction has to be viewed in perspective, as both the intelligence services and the police services are not ancient institutions and furthermore their relatively young existence has been politically marked. The turbulent political developments explain the differences in the relationship between intelligence and police services in the US and Europe. In Europe, the experience with the totalitarian regimes and their political police forces in Nazi Germany, in Russia, etc. has greatly influenced the organization after WW II. The intelligence services went back to being separate organizations with their own statute. The police were removed from direct political control and made into an agency, and operational police duties and intelligence work were formally split up. In principle, information was no longer to be shared. Attempts after 11-S to revise this flow of information, for example in the framework of Europol's Counter Terrorism Task Force have ended in fiasco. In the US, the political threat at home and abroad was exactly the argument inducing President Roosevelt to expand the FBI from a classic federal police service into an organization with a dual function, namely to act as a federal police service and a federal

verhoor van afgeschermde getuigen en enkele andere onderwerpen (afgeschermde getuigen), *Kamerstukken II* 2003-2004, 29 743, no. 2.

[14] http://www.eerstekamer.nl/9324000/1/j9vvgh5ihkk7kof/vhfifl1fmyx9/f=y.pdf.

intelligence service, initially just limited to national security, but later also endowed with tasks abroad, despite the establishment of the CIA which was specialized in this area. In short, in the US it is not exactly sensational that the regular federal police do not just occupy themselves with investigation, but also with intelligence work, including counter-intelligence operations. For this reason, the IC in the US not only consists of the CIA, the National Security Agency, the Defense Intelligence Agency and the National Reconnaissance Office, but also of the intelligence units of the Department of State, of the FBI, of the Department of Treasury, of the Department of Energy and of the armed forces. The fact that there is no organizational division between the IC and the LEC - both the CIA and parts of the FBI belong to the IC - is not to say that there are no strict distinctions in respect of objectives, methods and control. Both evidently have to act in accordance with the Constitution and federal laws, but it is obvious that the IC is much more regulated by executive orders from the President and is only subject to political parliamentary control. Due to the scandals which occurred in the 1970s over political espionage, the relationship between the IC and the LEC remained factually frozen for a decade, but starting from the mid-1980s cooperation was resumed, due to the fact that Presidents Ford and Reagan assigned special tasks to the IC by executive order in the fight against drugs and terrorism. Certainly after 11-S and the mounting criticism heaped onto the intelligence services counter-terrorism cooperation has intensified considerably.

## 3. Analysis of information sharing between the IC and the LEC up to 11-S

### *3.1. The development toward security-orientated criminal law*

Since the beginning of the twentieth century, searches and tapping and surveillance operations are being carried out without a judicial warrant, also for the purpose of investigating and prosecuting criminal offences. Since the 1960s, judicial control over the use of powers of investigation has been a recurring theme in the case law of the Supreme Court, especially as regards the Fourth Amendment (warrant clause). The Fourth Amendment expressly states that a warrant can only be issued when there is probable cause. In *Katz vs. US*,[15] the Supreme Court decided that a warrant is needed for bugging, unless a matter of national security is involved. In Berger vs. New York,[16] the Supreme Court stated that the warrant for wiretapping must be sufficiently specific with respect to the target, the method and the duration. In 1986, the legislator regulated this topic in Title III of the Omnibus Crime Control and Safe Street Act. The conditions for obtaining a warrant are laid down in legislation. The enforcement agencies must be able to show probable cause[17] in an affidavit.[18] As a rule, therefore, a warrant is required, but there are numerous exceptions.[19]

[15] Katz vs. US, 389 U.S. 347 (1967).

[16] Berger vs. New York, 388 US 41 (1967).

[17] The enforcement agencies must thereby have reasonable grounds to believe that the information to be obtained is relevant for the investigation.

[18] The affidavit may be based on information from an informer whose identity is not revealed, on the

In case of tapping without a warrant, however, the action taken may not be unreasonable and there must be probable cause in the mind of the investigating officer. The Act also expressly states that 'the statute does not limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts by foreign powers, to obtain foreign intelligence information deemed essential to the security of the US, or to protect national security information against foreign intelligence activities'.[20] In short, tapping without a warrant is always possible in national or international investigations for the purpose of protecting national security. In 1972, the Supreme Court decided in Keith[21] that the Constitution makes a warrant compulsory if the investigation concerns 'domestic individuals' and has 'no significant connection with a foreign power'. The legislator got the message and in 1978 the by now infamous FISA surveillance[22] was introduced, which makes it possible to bug and tap foreign powers and their agents, foreign networks or persons or terrorist activities[23] without a warrant. For the tapping or bugging of related US citizens or US residents a warrant must be issued by a secret FISA court. The investigative acts involved are always secret and persons concerned are not informed of them either before or afterwards.

### *3.2 Information sharing between the IC and the LEC before 11-S*

In the US, the discussion concerning the transfer of intelligence for use as criminal law evidence mainly focuses on FISA intelligence. Nevertheless, the principles are the same for information obtained from classical intelligence operations. First of all, the compulsory notification by the IC has to be pointed out. For example, the FBI, if it involves itself with foreign intelligence (FI) or foreign counterintelligence (FCI), must immediately inform the Criminal Division of the Attorney General's Office (AG) when "facts or circumstances are developed in an FI or FCI investigation that reasonably indicate that a significant federal crime has been, is being, or may be committed". This threshold is below the probable cause requirement in criminal cases. The crimes concerned are serious and include terrorism and material support to terrorism. When FISA is involved, the Office of Intelligence Policy and Review of the Department of Justice must be consulted beforehand. In case of doubt or disagreement the final decision is made by the AG.[24] The other way around, the procedure for access by criminal prosecutors to IC information in ongoing criminal investigations is also strictly regulated. The prosecuting authorities must indicate quite precisely the

condition that the police officer has been questioned and heard about this.

[19] See T.P. Metzler, et al. (2001). Warrantless searches and seizures, 89 *Geo L. J.*, 1084, and S.M. Beck (2001). Overview of the Fourth Amendment, 89 *Geo. L. J.*, 1055.

[20] 18 U.S.C. para. 2511 (3).

[21] US vs. US District Court (Keith), 407 US 297 (1972).

[22] Foreign Intelligence Surveillance Act, http://www4.law.cornell.edu/uscode/50/ch36schI.html..

[23] FISA (50 U.S.C. para. 401(a)). It does not have to be shown with probable cause that these persons or activities are involved.

[24] See http://www.epic.org/privacy/terrorism/FISA/08_2002_mem.html.

information related to facts and individuals which it wishes to access and why. The permission of the Internal Security Section of the Criminal Division of the Attorney General's Office is required. Furthermore, the officials of the Public Prosecutor's Office who will inspect the documents have to be screened beforehand for reliability.

Sec. 1806 and Sec. 1825 of the FISA Act include specific provisions concerning the use of FISA intelligence as evidence in criminal cases. The permission of the person concerned is not required, but he/she does have to be informed. The permission of the AG is always required, implying that information cannot be shared directly between the IC and LEC. The person concerned may request the court in the preliminary stage or at the hearing to declare the evidence inadmissible for having been unlawfully obtained or because the procedural requirements applicable in FISA investigations have not been fulfilled. The AG may request the court by means of an affidavit under oath to hear the case in camera and ex parte if disclosure of the evidence would harm national security.[25]

In transferring IC information to the LEC mandatory use must be made of what is termed the minimization procedure.[26] Minimization aims to limit the acquisition, retention and dissemination of information concerning US citizens as much as possible. Only where such information is crucial for the assessment of foreign intelligence may it be stored and used. It is also provided that evidence of criminal offences which have been committed, are being committed or may be committed are exempted from minimization. A classic component of minimization is the information-screening wall, which means that an official from the Department of Justice, who is not directly involved in the IC or the LEC, screens the FISA intelligence and only selects the parts that are relevant as evidence. The starting point of the 1995 memorandum by AG Janet Reno[27] is the prohibition of any direct exchange of information between the IC and the LEC. All information has to pass through the Criminal Division first for screening. The transfer of information is possible whenever there is a "legitimate and significant criminal law enforcement concern". The Criminal Division may also assist the FBI in order to preserve the option of criminal prosecution, although "the Criminal Division shall not, however, instruct the FBI on the operation, continuation, or expansion of FISA electronic surveillance or physical searches. Additionally, the FBI and Criminal Division should ensure that advice intended to preserve the option of criminal prosecution does not inadvertently result in either the fact or appearance of the Criminal Division's directing or controlling the FI or FCI investigation toward law enforcement objectives".[28] In short, the 1995 memorandum principally allows the use of FISA intelligence in criminal case. US courts also allow the use of FISA intelligence as evidence in criminal cases, provided, of course, that FISA requirements have been fulfilled and that the information has not been laundered. In many court proceedings it has been attempted to declare the fruits of FISA surveillance as unlawful evidence, but to no avail, given that the

[25] See further under 3.3. for a discussion of CIPA.

[26] See 50 U.S.C. Sec. 1801(h), Sec. 1806(a) and Sec. 1825(a) of the FISA Act.

[27] See http://www.epic.org/privacy/terrorism/fisa/ag_1995_mem.html.

[28] See http://www.epic.org/privacy/terrorism/fisa/ag_1995_mem.html, under 7.

prevailing opinion in case law is that the FISA rules form a constitutionally sound balance between the rights of the defence and the interests of national security, which renders the use of FISA intelligence as legal evidence in criminal cases lawful.[29]

In addition, the 1995 memorandum restricts contact between the IC and the LEC by providing for steering by the Department of Justice and the AG (also known as the chaperone requirement) and by the reporting duties which have to be open for testing by the FISA court. Especially in complex cases, such as, for instance, the bombings of US embassies in Africa, the FISA court performed such testing. The FISA court's task in this is: "to preserve both the appearance and the fact that FISA surveillances and searches are not being used sub rosa for criminal investigations" and has "routinely approved the use of information screening 'walls' proposed by the government in its applications".[30] However, it has emerged from a recent memorandum opinion of the FISA court that in 75 cases information submitted by the FBI or the Department of Justice has proved to be erroneous, omitted or false in applications for the extension of secret judicial authorization for secret tapping operations or searches, without this having been sufficiently explained by the organizations in question.[31] By this, the FISA court recognizes that the screening wall was deliberately circumvented.

### *3.3 Balance between national security and the fundamental rights of due process of persons involved in criminal proceedings*

In 1980, the Classified Information Procedures Act (CIPA) was adopted under regular federal criminal procedural law. Essentially, it is decided in a pre-trial conference, in camera, what information will be used during the hearing, while a protective order (secrecy) is imposed on the defence which has access to the information. The government may also ask the court not to make the secret evidence available, but to replace it with summaries of or excerpts from the reports. To this end, the government must convince the court that this will not undermine the position of the defence. In case the court refuses, the AG may contest the disclosure by means of an affidavit. If the court nevertheless persists in disclosure and the government fails to respond to the court's subpoena, the court may exclude the evidence or take these circumstances into account in sentencing. CIPA primarily aims to prevent secret information from still leaking out at the trial or placing the government in the dilemma of either disclosing or withdrawing the evidence. There is much debate in the US concerning the relationship between CIPA and the constitutional freedoms.

---

[29] See US vs. Megahey, 553 f. Supp 1180, 1189-90 (E.D.N.Y. 1982); US vs. Falvey, 540 F. supp 1306, 1310-11 (E.D.N.Y/ 1982); US vs. Duggan, 743 F. 2d 59, 75-78 (2d Cir. 1984); US vs. Pelton, 835 F 2d 1067 (4th Cir. 1987) and Bin Laden, 126 f. Supp 2d at 278.

[30] See http://www.epic.org/privacy/terrorism/fisa/fisc_opinion.html.

[31] See http://www.epic.org/privacy/terrorism/fisa/fisc_opinion.html.

There is not much case law in the US concerning unlawfully obtained evidence with respect to evidence in criminal proceedings which relies on information derived from intelligence. Reference is routinely made to *Truong*,[32] but this case dates from before the FISA Act. Truong was suspected of espionage for Vietnam and pending criminal investigations was tapped without a judicial warrant by the FBI and the CIA. The evidence that was the result of the tapping was excluded. Nevertheless, Truong was still convicted, as there was also evidence relying on intelligence gathered against agents of a foreign power at a time when there was not yet a suspect or a criminal investigation. This case is an indication of the fact that courts have to be watchful for circumventions of the legal guarantees through the deployment of intelligence surveillance by another route.

## 4. Information sharing between the IC and the LEC and the new approach under the Patriot Act

### *4.1 The provisions of the Patriot Act*[33]

After 11-S, new anti-terrorism legislation was elaborated in the US, resulting in the USA Patriot Act.[34] First of all, it has to be emphasized that the Patriot Act has considerably expanded the regular powers of investigation, especially in the field of electronic and digital surveillance, while at the same time it has weakened judicial control. Secondly, the Patriot Act has ensured that FISA security criminal law can be used on a much wider scale. Before the Patriot Act, a primary purpose standard had to be met, which meant that in the case of an investigative interest the use of FISA powers was only allowed for primary foreign intelligence purposes. The Patriot Act has made it sufficient that the purpose is significant. It is allowed to pursue investigative purposes, as long as a significant purpose of the surveillance is to obtain foreign intelligence information.[35] Thirdly, the Patriot Act has opened up the flow of information from the LEC to the IC and vice versa by breaking down the existing legal dividing wall. Sec. 203 of the Patriot Act amends the Federal Rules of Criminal Procedure.[36] Sec. 203(a) grants the LEC permission to share information from criminal investigations derived from matters occurring before the Grand Jury with other federal agencies (such as the Immigration Service) and the intelligence and security services,

[32] United States vs. Truong Ding Hung, 629 F. 2d 908 (4th Cir. 1980).

[33] See J.W. Whitehead & S. H. Aden (August 2002). Forfeiting "Enduring Freedom" for "Homeland Security": A constitutional analysis of the USA Patriot Act and the Justice Departments anti-terrorism initiatives. *American University Law Review*, 51, 1081; A.A. Bradley (December 2002). Extremism in the defense of liberty?:The Foreign Intelligence Surveillance Act and the significance of the USA Patriot Act. *Tulane Law Review*, 77, 465 and J.C. Evans (Summer 2002). Hijacking Civil Liberties: the USA Patriot Act of 2001, *Loyola University of Chicago Law Journal*, 33, 953.

[34] http://www.evergreen.edu/library/govdocs/hotopics/usapatriotact/patriot-act.pdf . J.A.E. Vervaele (2005).The anti-terrorist legislation in the US; inter arma silent leges? *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 13/2, 201-254.

[35] 50 U.S.C. paras. 1804 (a) (7)(B), 1823 (a) (7)(B).

[36] See also http://www.usdoj.gov/olp/section203.pdf for the memorandum of the AG Office thereon.

in case the information is of an FI or FCI character. Sec 203 (b) also grants the LEC permission to share criminal investigative electronic, wire and oral interception information with other federal agencies and the intelligence and security services, in case the information is of an FI or FCI character. Neither requires judicial authorization. In this way, the CIA is increasingly gaining control over the use of FISA. The Patriot Act provides that the director of the CIA may elaborate regulations for the collection of information under the FISA and that he may assist the AG so as to ensure that the FISA information is used efficiently and effectively for foreign intelligence work.[37] Based on Sec. 905(a) and Sec. 905(b) of the Patriot Act further rules were specified in memoranda of the Attorney General's Office of September 2002.[38] Specific Memoranda of Understanding, which have not been published, have also been negotiated between the services involved.

Sec. 504, conversely, regulated the flow of information from the IC to the LEC. The FBI intelligence services which are authorized to use the secret FISA tapping powers are allowed to consult with the LEC in order to coordinate efforts to investigate or protect against attacks, hostile acts, sabotage, international terrorism or clandestine intelligence activities by a foreign power, agent, network or person. This means that the Patriot Act neither prohibits nor conditions this flow of information. Matters have been further elaborated in the recent NSI guidelines from the AG for FBI national security investigations and foreign intelligence collection.[39] These do not leave any doubt that FI or FCI, either obtained through FISA or not, may be used in the investigation and prosecution of serious offences, such as terrorism. It becomes clear from the guidelines that the FBI has a duty to inform other components of the IC and the competence to inform the LEC. If the information is not personal, it may be supplied at all times. If it is personal, the information has to be necessary to guarantee the safety of persons or property, to prevent crime or "to obtain information for the conduct of a lawful investigation by the FBI". The IC and the LEC may also consult with a view to coordinating their different tasks.

### *4.2 Further regulation by the AG concerning intelligence sharing*

In the Patriot Act's wake, AG Ashcroft issued a new memorandum in March 2002 concerning intelligence-sharing procedures for foreign intelligence and foreign counterintelligence investigations conducted by the FBI,[40] which is to replace the 1995 memorandum. In the field of information-sharing powers the memorandum distinguishes between disseminating information and providing advice. Under the dissemination of information clause[41] the LEC is given access to all FI and FCI information, unless the FISA court or the AG imposes restrictions. This access also concerns personal information and

[37] 50 U.S.C.A. para. 403-3(d)(1) (Supp. 2002).

[38] See http://www.usdoj.gov/olp/section905a.pdf en http://www.usdoj.gov/olp/section905b.pdf.

[39] See http://www.usdoj.gov/olp/nsifactsheet.pdf en http://www.usdoj.gov/olp/nsiguidelines.pdf.

[40] See http://www.epic.org/privacy/terrorism/FISA/ag_mem_03_2002.html.

[41] Based on 50.U.S.C. pars. 1801 (h), 1806(a) and 1825(a).

modus operandi. The FBI has a duty to inform the Criminal Division of the Attorney General's Office concerning FI and FCI information "that is necessary to the ability of the US to investigate or protect against attack, sabotage, terrorism, and clandestine intelligence activities". The wording has thus been broadened as compared to the 1995 memorandum. The use as evidence in criminal proceedings of FI or FCI information requires permission of the AG. Under the provision of advice clause far-reaching cooperation procedures are established concerning coordination between the IC and the LEC in areas such as investigation strategy, the use of coercive measures by the IC and the LEC, interaction between the IC and the LEC and "the initiation, operation, continuation, or expansion of FISA searches or surveillance". The latter were still expressly excluded in the 1995 memorandum. Finally, the possibilities for forwarding IC and FCI information directly to lower levels within the Public Prosecutions Office are enhanced considerably, although the Criminal Division of the Attorney General's Office still has to be notified and the AG still has to approve the use of the information as evidence in criminal proceedings. The outcome of these provisions is that the prosecuting authorities are given an important role in the management of secret FISA tapping surveillance and searches, from the very beginning to the inclusion of the results in the criminal file. Due to the considerable broadening of the scope of application of the FISA and thereby of secret investigative acts little threatens to remain of the classic criminal law guarantees against coercive measures.

These facts have not escaped the notice of the FISA court which formally has to approve the memorandum.[42] Because of its years of experience with FISA authorizations, the court is fully aware of the fact that IC and LEC investigations may overlap or that FI/FCI and investigative interests may overlap within the same FISA surveillance or regular criminal law investigations. According to the FISA court, AG Ashcroft's extensive interpretation of the provisions of the Patriot Act do not constitute a reasonable balance between the intelligence purposes of FISA and the rights and freedoms of the citizen. The FISA therefore rejects the competence of criminal prosecutors to give guidance to FBI intelligence in respect of "the initiation, operation, continuation, or expansion of FISA searches and surveillance" and thus also rejects the direct access of criminal prosecutors to IC information: "A fair reading of those provisions leaves only one conclusion - under sections II and III of the 2002 minimization procedures, criminal prosecutors are to have a significant role directing FISA surveillances and searches from start to finish in counterintelligence cases having overlapping intelligence and criminal investigations or interest, guiding them to criminal prosecution (...) If criminal prosecutors direct both the intelligence and criminal investigations, or a single investigation having combined interests, coordination becomes subordination of both investigations or interests to law enforcement objectives". The FISA court fears that the stricter requirements and broader legal guarantees of regular criminal procedural law will be circumvented by means of the FISA, which is why it has deleted these passages and replaced them with wording that is in line with the 1995 memorandum. The FISA court does, however, approve of the clause concerning the movement of information and applies the minimization procedure to it in order to prevent information concerning US

[42] See http://www.epic.org/privacy/terrorism/fisa/FISC_opinion.html.

citizens from ending up with the investigative authorities. This decision is remarkable on two accounts. The FISA court is known as a loyal government ally and for this reason is sometimes laconically called "rubber stamp". This time, however, it pulled the government up short and moreover published its opinion.

The AG has appealed[43] to the US Foreign Intelligence Surveillance Court of Review, which is unique in history. It is interesting to note the positions chosen by the AG in defence of the memorandum. The starting point is that the Patriot Act enables a complete exchange of information between the IC and the LEC. The information-screening walls are torn down. FISA surveillance may be used for serious offences, including terrorism, in order to obtain criminal law evidence: "Prosecution of spies and terrorists is not merely an incidental by-product of a FISA search or surveillance; rather, obtaining evidence for such a prosecution may be the purpose of the surveillance; the use of FISA within those investigations, may be 'designed' for a law enforcement purpose". The AG does not hesitate to make clear that due to the Patriot Act a primary intelligence purpose is no longer needed from now on and that a significant intelligence purpose suffices. FISA surveillance means that the FISA may be used primarily for a law enforcement purpose. The former dichotomy between the IC and the LEC is history, according to the AG, who adds that another consequence is that comparisons no longer have be made between the interests of the IC and those of the LEC and that it therefore no longer needs to be determined whether the legal guarantees under criminal law play a role either. In other words: out with the Truong test (no IC surveillance after suspicion). This is also the reason why the screening walls and the chaperone requirements may be abolished. In its first decision in its 23 years of existence, the Court of Review has reversed the decision of the FISA court and approved Ashcroft's 2002 memorandum after all.[44] The Court is of the opinion that the FISA legislation was never intended to limit the use of IC intelligence in criminal proceedings and that the 1995 memorandum was therefore a much narrower interpretation than was legally necessary. The Court is further of the opinion that the Truong test is based on an erroneous starting point. Whenever there is a case of criminal suspicion and criminal investigation, this does not mean that policy interests with respect to foreign intelligence just cease to exist. The construction in Truong was based on the organic division within the Department of Justice and erected a dividing wall between the components. According to the Court, this interpretation belies the fact that effective counterintelligence consists of a combination between the IC and the LEC and therefore requires their cooperation: "A standard which punishes such cooperation could well be thought dangerous to national security (...) Indeed, it was suggested that the FISA court requirements based on Truong may well have contributed, whether correctly understood or not, to the FBI missing opportunities to anticipate the September, 11, 2001 attacks". On the other hand, the Court rejects the opinion of the AG that the dichotomy between the IC and the LEC has ceased to exist and that FISA can be used for primary enforcement purposes. Nevertheless, this does not result in a different outcome, given that the Court holds significant purpose to mean that there must be a significant FI or FCI

[43] See http://www.epic.org/privacy/terrorism/fisa/doj_fisc_appeal.html.

[44] See http://www.cadc.uscourts.gov/common/newsroom/02-001.pdf.

purpose; for this, it is immaterial how significant the investigative purpose is, nor does it require a comparison anymore. Only in cases where there is no significant FI or FCI purpose, would there be insufficient grounds for FISA surveillance. NGOs and the National Association of Criminal Defense Lawyers have submitted amicus curiae briefs in which it was argued that the 2002 memorandum constitutes a violation of various constitutional guarantees, among which the warrant clause of the Fourth Amendment. To the question of whether abandoning the primary purpose requirement for FISA surveillance constitutes a violation of the Constitution the Court laconically replies that, after a thorough examination of the case law: "We acknowledge, however, that the constitutional question presented by this case has no definitive jurisprudential answer (...) Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly, applying the balancing test drawn from Keith, that FISA as amended is constitutional because the surveillances it authorizes are reasonable".

### *4.3. Equality of arms after 11-S?*

The far-reaching possibilities for criminal prosecutors to use intelligence as evidence in criminal proceedings and also to direct the process of obtaining intelligence naturally raises questions as to the position of the defence. Many of these points were already reviewed under 3.3. A question which became extremely topical after 11-S is whether the suspect/accused may also use FI or FCI as evidence in criminal proceedings in order to prove his innocence. One of the problems involved is that the government uses its constitutional prerogatives to shield information.[45] That this issue can lead to extremely complex situations in the US may best be illustrated by the case concerning Zacarias Moussaoui,[46] a French national of Moroccan birth who was detained in August 2001, i.e. before the attacks, on suspicion of a breach of immigration law. At that time, he was taking flying lessons. After the attacks, he was connected with Al-Qaeda and the terrorist acts of 9/11. Moussaoui is accused of being the twentieth hijacker whose detention prevented him from boarding and of being jointly guilty of the death of 3 000 people. He has pleaded not guilty, and is risking the death penalty on four of the six charges against him.[47] For this reason, he wishes to have Bin Al-Shibh questioned as a witness. The problem is, however, that Bin Al-Shibh, who was arrested in Pakistan, is suspected of being the intermediary between Moussaoui and the 9/11 command and is being held as an enemy combatant overseas, presumably in Guantánamo. His statements are classified and can therefore not be contested. Both the District Court and the US fourth Circuit Court of Appeals have recognized Moussaoui's Sixth Amendment right to subject the witness Bin Al-Shibh to

[45] Executive Order 13292, Classified National Security Information, 68 FR 15315.

[46] For all relevant information, see:
http://news.findlaw.com/legalnews/us/terrorism/cases/index.html#moussaoui.

[47] See http://www.usdoj.gov/ag/moussaouiindictment.htm for the charges.

questioning, as one of the fundamental rights of a fair trial.[48] In this case, District Court Judge Brinkema in January 2003 ordered that the testimony be recorded on video and that the video be made available to the jury or that the witness be heard by teleconference. AG Ashcroft continued to underline the fact that this would result in "the unauthorized disclosure of classified information". The AG refused to implement the court decision, which was formally confirmed in a secret affidavit in mid-July 2003.[49] The court could hold the government in contempt of court, but could also declare the Moussaoui case inadmissible, exclude part of the evidence or instruct the jury unfavourably for the government, preventing a death sentence. Judge Brinkema opted to exclude the death penalty and to strike the part of the indictment related to 9/11, as in her view there could be no fair trial under these circumstances. The part of the indictment concerning conspiracy to commit the Al-Qaeda actions remained intact. The government lodged an appeal against the decision with the US 4th Circuit Court of Appeals,[50] which is known to be conservative, and which on 22 April 2004[51] decided to set aside the exclusion of evidence and of the possibility of a death sentence. On the other hand, the three-judge panel also decided that Moussaoui could not be deprived of the right to question detained Al-Qaeda members as witnesses and that he was entitled to present their testimony to the jury. Judge Brinkema was ordered to elaborate a compromise which would allow the witnesses to be questioned in a way which would not prejudice their questioning by the government in the framework of the war against terrorism.[52] On March 2005 The Supreme Court[53] rejected Moussaoui's attempt to directly question Al-Qaeda prisoners and cleared the way for a trial of the only US defendant charged in connection with the September 11 attacks. The ruling allows the government to proceed with plans to seek the death penalty if Moussaoui is convicted of participating in an Al-Qaeda conspiracy that included the 2001 airplane hijackings. In April 2005 he suddenly decided to plead guilty to all six counts of conspiracy to engage in terrorism.[54] It is not excluded that he did so in order to avoid transfer to a military procedure and thus military consignment.

[48] See Brady vs. Maryland, 373 US 83 (1963).

[49] US will defy court's Order in Terror Case, New York Times, 15 July 2003.

[50] See http://news.findlaw.com/hdocs/docs/moussaoui/usmouss102403gbrf.pdf for the government's petition in which references to concrete facts or documents have been regularly blackened out, as these, according to the government, concern confidential information in the protection of national security.

[51] See Westlaw, 2004 Wl 868261 (4th Cir. (Va.)).

[52] For a list of all pleadings, orders and opinions filed in the case, see: http://notablecases.vaed.uscourts.gov/1:01-cr-00455/DocketSheet.html

[53] http://news.findlaw.com/hdocs/docs/moussaoui/usmouss21005cert.pdf

[54] N.A. Lewis (2005, April 24). Surprise Terror Leaves Unresolved Issues. *The New York Times*.

*4.4. Interim conclusion*

Already before 11-S there was much room in the US for letting intelligence flow through to criminal proceedings. FISA security criminal law has promoted this development. Before 11-S the minimization procedure and the chaperone requirements had to ensure that personal information concerning US citizens was only used in criminal proceedings if they were relevant as evidence for the prosecution. In addition to the screening walls, it was also guarded against that the investigative authorities did not direct the secret surveillance in their own interest. It was clear, however, that secret intelligence information from criminal investigations could be interesting, not just as leads in criminal investigations, but also as evidence. All this has led to complex legal structures concerning secret evidence and the secret furnishing of proof in ex parte and in camera proceedings and in a number of cases even to secret trials and secret judgments. After 11-S the security paradigm has further eroded the classical criminal law guarantees. Secret investigations and the free flow of the information derived there from into criminal proceedings have become possible. The administration of criminal justice is becoming less and less public and the decision making concerning the acquisition and use of evidence takes place within an ever wider margin of discretion. National security is the government's argument not to apply the legal guarantees which are perceived as obstacles. This has led to legal action on principle concerning the applicability of the constitutional guarantees in the fight against terrorism.

## 5. State of the art at EU level

As stated in the introduction, the EU in the Hague Programme for the Area of Freedom, Security and Justice introduced the principle of availability, including the transnational flow of law enforcement information.[55]

Already at the end of March 2004, the European Commission submitted a draft third-pillar proposal concerning exchange of information and cooperation to combat terrorism.[56] More important for our topic is the Communication from the Commission concerning the enhancement of access to information by law enforcement agencies[57] and the Swedish proposal for a Framework Decision concerning the exchange of intelligence between the enforcement authorities of the Member States.[58] The Commission Communication has as its

[55] See G. Vermeulen e.a. (2005). Availability of law enforcement information in the European Union. Between mutual recognition and equivalent right of access. Antwerp/Apeldoorn: Maklu.

[56] COM (2004) 221 final, 29 March 2004.

[57] Communication from the Commission to the Council and the European Parliament - Towards enhancing access to information by law enforcement agencies (EU information policy) - (COM (2004) 429 final, 16 June 2004).

[58] Draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU, in particular as regards serious offences including terrorist acts, Council of the EU, 10215/04, 4 June 2004.

starting points the mutual recognition and free movement of information between the competent authorities of the Member States. Police work and judicial activity should also be based more on intelligence. In passing, without any further explanation, it is remarked that the intelligence services could play an important role in this. The Swedish proposal works out in greater detail what is stated in the Communication from the Commission, but as regards the topic under discussion it keeps all options open. The basic idea is indeed the free movement of information between the competent enforcement authorities. A competent authority is a: "national police, customs or other authority, that is authorized by national law to detect, prevent or investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities". Such a broad definition does not exclude national intelligence services. The definition of "information and intelligence" is also quite broad: "any type of existing information or data (...) that could be used in crime investigation or a criminal intelligence operation to detect, prevent or investigate a crime or a criminal activity". This means that intelligence from the intelligence services also falls within its scope. According to the Explanatory Memorandum, the broad definitions have to ensure that free movement is not frustrated by differences in national organization. With respect to our topic, Article 1 (objective and scope) hastens to determine expressly that the Framework Decision does not imply any obligation to exchange information to be used as evidence in criminal proceedings. In the event that the receiving state wishes to use that information in this way, the prior consent of the providing state is required and it may be necessary to go down the road of judicial assistance. On the other hand, the proposal Framework Decision does not prohibit use as evidence either, nor does it restrict it by setting certain conditions as to selection or legal protection. The usefulness is determined exclusively by the provider. In accordance with Article 9(4), the provider of information may set certain conditions with respect to its use. The conditions are not defined further, although Article 9(3) makes it clear that the purposes of use are determined quite broadly, ranging from prevention to prosecution, and for trying offences, but also for enforcing migration rules, for example. It is notable that the various proposals all pay lip service to the European Convention of Human Rights (ECHR) and the legal protection of the suspect, but that this dimension is not fleshed out in concrete terms.

During the negotiations on the Swedish proposal for a framework decision on the exchange of information between law enforcement authorities, 7 Member States[59] preferred to agree on an instrument outside the structure of the EU. The so-called Prüm Treaty is an intergovernmental agreement on the stepping-up of cross-border cooperation, particularly in combating terrorism, cross-border and illegal immigration. It includes an important section on the exchange of law enforcement information, by giving reciprocal access to national databases concerning DNA profiles, fingerprints and vehicle registration data. It is not entirely clear whether this was an initiative to sideline the EU initiative on the principle of availability, but the overlap is obvious. However, there are also some differences. The Prüm Treaty deals with a more narrow range of data and is not based on direct access to databases, but on indirect access through reference data.

[59] Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria.

The agreement of the 7 States has been criticized for breaching EU loyalty, for not having been reached making use of the EU possibilities of enhanced cooperation within the EU Treaty and for having set aside the link between an EU instrument of exchange of information and an EU instrument on protection of personal data in the third pillar.[60] Only quite recently, the House of Lords' European Union Committee has made public its severe criticism of the agreement[61] and insisted upon a parallel agreement on the integration of the Prüm Treaty and on a Framework Decision setting high standards for the protection of data across the third pillar.

At the end of 2006, the Member States of the Union finally agreed upon a Council Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.[62] The objective and the scope of the Framework Decision is limited to the exchange of existing information, not information that has to be gathered by investigation, for the purpose of conducting criminal investigation or criminal intelligence operations. This means that law enforcement information must be exchanged at all stages of law enforcement, from the stage of pro-active intelligence information to the execution of the sanctions. However, agencies or units dealing especially with national security issues are not covered by the concept of competent law enforcement authorities. Which intelligence units will fall within its scope depends on the declarations by all individual Member States defining at national level the authorities that are covered by the concept of law enforcement authority for this instrument. Included in any case is information or data held by private entities (service providers) which is available to law enforcement authorities without the use of coercive measures.

Article 5 is somewhat misleading on the finality of the exchange, by stating that "Information and intelligence may be requested for the purpose of detection, prevention or investigation of an offence where there are factual reasons to believe that relevant information and intelligence is available in another Member State. The request shall set out those factual reasons and explain the purpose for which the information and intelligence is sought and the connection between the purpose and the person who is the subject of the information and intelligence". This is misleading, as Article 8 on data protection deals more with finality than it does with data protection. Indeed, Articles 8 (3-4) extend finality far beyond the boundaries set by Article 5. Article 8 (3) provides for three legitimate forms of use:

1. for the purposes of the Framework Decision;
2. for preventing an immediate and serious threat to public security;
3. for other purposes.

[60] COM (2005) 475 final and SEC (2005) 1241.

[61] House of Lords, European Union Committee, 18th Report of Session 2006-2007, Prüm; an effective weapon against terrorism and crime? May 9th, 2007.

[62] Council framework decision 2006/960/JHA, OJ L 386/89, 19.12.2006.

In the latter case, use is dependent upon the prior authorization of the communicating Member State and both the national laws of the communicating and receiving Member State. It is quite clear that the threat to public security can be used as a Pandora's box for intelligence and information exchange.

Interesting is also that Article 8 (4) provides the possibility for the communicating Member State to impose conditions upon the use of this information for the purposes of the Framework Decision (not for preventing an immediate and serious threat to public security!), but that these binding conditions can be set aside in the receiving Member State "in the specific case where national law lays down that the restrictions on use be waived for judicial authorities, legislative bodies or any other independent body set up under the law and made responsible for supervising the competent law enforcement authorities". In this case only prior consultation with the communicating Member State is mandatory, not prior consent. Finally, if these authorities want to use the information as evidence before a judicial authority, then Article 1(4) provides that the communicating Member State must consent to this.

It is clear that this exchange of information under the availability principle can replace the classic mutual legal assistance framework and that police intelligence authorities, judicial authorities and law enforcement authorities can dispose transnationally of large amounts of intelligence and information. The Framework Decision does not elaborate on the possible privileges or professional secrecies of the authorities involved. Article 9 only deals with confidentiality for the requirements of investigation secrecy. That means that the national rules on possible secrecies of the bodies involved are set aside. Finally, the Framework Decision only contains references to national data protection rules and the rules of the Council of Europe. Any reference to the proposal for a Framework Decision on data protection in the third pillar has definitely been avoided.

Meanwhile the German Presidency has clearly opted for a stepping up cross-border police cooperation by transposing the Prüm Treaty into the legal framework of the EU. A number of 15 Member States[63] submitted a proposal to this effect to the Article 36 Committee, which means that the contents of Prüm will not be the subject of negotiations in the working groups of the EU Council of Ministers. Integration can take place by means of a unanimity decision or under the EU provisions on enhanced cooperation. The integration of the Prüm Treaty has not been combined with data protection provisions in the third pillar. In April 2006,[64] the European Data Protection Supervisor submitted a very critical ex officio opinion on this topic, stating that the adoption of a specific third-pillar instrument for data protection is a conditio sine qua non for the exchange of personal data by law enforcement initiatives. Unfortunately, the latest version of the German Presidency on data protection in the third

[63] Belgium, Bulgaria, Germany, Spain, France, Luxembourg, the Netherlands, Austria, Slovenia, Slovakia, Italy, Finland, Portugal, Romania and Sweden.

[64] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-04-04_crossborder_cooperation_EN.pdf .

pillar has further weakened the content of the proposal and can be qualified as a low common denominator that does not go beyond the minimum imposed by the Council of Europe instruments.[65]

The state of the art in the EU clearly shows that the principle of the availability of information has been pushed through[66] and in no way strikes the right balance with human rights.[67] In this way, the use of intelligence in criminal proceedings has been increased, but the use of intelligence as evidence and the intelligence-led criminal procedure is still beyond the scope of this evolution. On this topic we must await the Commission study on the cross-border use of intelligence as evidence scheduled for 2008.

## 6. Analysis of the sharing of intelligence and investigation information in the Netherlands

### *6.1. Legal framework*

The Netherlands has a long tradition of obtaining, storing and processing criminal intelligence.[68] Criminal Intelligence Services [Criminele inlichtingendiensten (CIDs)], which have now been renamed Criminal Intelligence Units [Criminele inlichtingen eenheden (CIEs)], have the task of providing information in the context of the performance of police functions in the field of serious and/or organized crime. Much intelligence is supplied by informers, civilian infiltrators and tip-offs and stored in CIE files. In 2003, for example, an additional CIE was established at the law enforcement agency of the Internal Revenue (FIOD-ECD).[69] Intelligence may of course also be provided by the General Intelligence and Security Service [Algemene Inlichtingen- en Veiligheidsdienst (AIVD)] or the Military Intelligence and Security Service [Militaire Inlichtingen- en Veiligheidsdienst (MIVD)], which obtain information by information gathering and processing and through the use of

[65] For the EDPS opinion on the proposal on data protection in the third pillar, see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-04-27_3dpillar_3_EN.pdf.

[66] See EDPS opinion, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2006/06-02-28_availability_EN.pdf.

[67] See EDPS opinion, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2006/06-02-28_availability_EN.pdf.

[68] M. van Stratum (2001). Criminele inlichtingen en het recht op kennisneming. *Delikt en Delinkwent*, 174-191.

[69] Decision of 28 July 2003 establishing the criminal intelligence unit at the law enforcement agency of the Internal Revenue of the Ministry of Finance and its functions [*Instellingsbesluit van 28 juli 2003, houdende de inrichting van de criminele inlichtingen eenheid bij de Belastingdienst/ FIOD-ECD van het Ministerie van Financiën en de vaststelling van de werkzaamheden*], Decree of 28 July 2003, no. DGB2003/3877M, Staatscourant no. 151.

special powers. Under the Intelligence and Security Services Act [Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv 2000)] the AIVD's power to snoop has been extended considerably, also in the field of the integrity of public administration and threats to computer networks. Articles 19 to 33 of the Wiv provide for far-reaching tapping and searching powers, infiltration, etc., which are to be as effective as the special investigative measures provided in the Code of Criminal Procedure. Despite the fact that the AIVD does not have the power of judicial investigation (Article 9(1) Wiv) and that police officers who perform tasks for the AIVD are not allowed to carry out their criminal investigative powers in that capacity (Article 9(2) Wiv), the AIVD from an information-gathering point of view can certainly compete with the police and judicial authorities. Article 14 Wiv stipulates that the storing of AIVD information must be strictly separated from the CIE. The stronger the AIVD's position of information is, the more interesting it becomes for the Public Prosecutions Department to allow this information to flow through and perhaps also direct the acquisition of such information. Based on Article 62 Wiv, the police has the duty to supply information which is relevant for the intelligence services. The police may also at the request of the AIVD supply information in accordance with Article 17 Wiv and Article 15(2) of the Police Files Act [Wet op de politieregisters]. The provision of information by the AIVD to internal and external channels is phrased in the Wiv as a competence and takes place in the framework of a closed provision regime. The AIVD may, for instance, disclose information to the Public Prosecutions Department in case it has information which may be relevant to the investigation or prosecution of offences (Article 38 Wiv). The AIVD, as opposed to the police, is under no obligation to do so, and will only do it to prevent threats to vital national interests.[70] Remarkable is the lack of any provision based on which the police or the Public Prosecutions Department could request information from the intelligence and security services of their own accord. The transfer of AIVD information takes place through two national terror officers of the national public prosecutor's office in the shape of an official report. The report does not reveal sources or describe the modus operandi. Based on Article 38(3) Wiv, the officer is competent to inspect the underlying documents in order to verify the correctness and lawfulness of the facts reported. He decides whether the information is supplied to the public prosecutor handling the case in question through an ex officio report of the national police (KLPD), possibly after consultations with the Board of Procurators General (Article 61(2) Wiv). Both the AIVD officers and the public prosecutor handling the case are bound to secrecy (Articles 85-86 Wiv), extending to the trial.

On 6 January 2003 the interdepartmental working group on legislation concerning information exchange published a report concerning Information Exchange and the Fight against Terrorism[71] to implement point 43 of the Action Plan on Security and Fighting Terrorism.[72] The report argues in favour of thematic files to complement the serious crime

[70] That this term is broadly interpreted is demonstrated by the fact that the AIVD has concluded an agreement with the Immigration and Naturalization Service, see Staatscourant, 19 June 2003, no. 115, p. 13.
[71] *Kamerstukken II*, 2002-2003, 27 925, no. 82.
[72] *Kamerstukken II* 2001-2002, 27 925, no. 10.

file (CIE file) and the preliminary and temporary files. The information in the thematic files could be stored for five years and its use would be less limited. The report does not pay any attention to the use of this information in criminal proceedings. In practice, this transfer of information is institutionalized. The Board of Procurators General has drawn up Guidelines for information supply to and from the AIVD and MIVD [Handleiding informatieverstrekking aan en door de AIVD en MIVD]. Intelligence and information from criminal investigations are submitted to the Technical Evaluation Commission, now renamed Evaluation Consultation [Evaluatie Overleg], which is a committee of representatives of Ministries (the Ministry of the Interior and Kingdom Relations, the Ministry of Justice and the Ministry of Defence) and operational services (KLPD, AIVD and MIVD).[73] The Unit for Fighting Terrorism and for Special Tasks [Unit Terrorismebestrijding en Bijzondere Taken] of the KLPD's Criminal Investigations Service [Dienst Recherche Onderzoeken] carries out threat analyses and the AIVD carries out analyses. However, the information supplied by the AIVD for the purpose of these analyses may not be used by the police for operational purposes or investigation purposes. The outcomes of the analyses are discussed in the Evaluatie Overleg and recommendations are made to the Evaluation Triangle [Evaluatie Driehoek] consisting of the Directorate General for Public Order and Security [DG Openbare Orde en Veiligheid] of the Ministry of the Interior and Kingdom Relations, the Directorate General for Law Enforcement [DG Rechtshandhaving] and the Special Directorate General for Security and Crisis Management [Project DG Beveiliging en Crisisbeheersing], both of the Ministry of Justice. The ultimate responsibility lies with the Security Council [Raad voor Veiligheid], which has been established as a sub-council of the Council of Ministers. It is assisted by the Joint Committee for Combating Terrorism [Gezamenlijk Comité Terrorismebestrijding], consisting of representatives from the civil service and the Public Prosecutions Department. The flow of information is therefore much more directed than would appear from the legislation and analysis and operational information is easily mixed. Research by the Netherlands Court of Audit has meanwhile shown that the KLPD's organization of information concerning terrorism still leaves much to be desired.[74] How do the Dutch criminal courts interpret the balance between the protection of national security and the corresponding confidentiality of sources, identities, modus operandi on the one hand and the public administration of criminal justice and the corresponding legal protection of the suspect on the other?

[73] In the Netherlands, exchange of information has been much experimented with, e.g. as between the financial supervisory authorities, the Public Prosecutions Department, the police, the tax authorities and the *AIVD*, among others in the field of fighting the financing of terrorism. See Nota Integriteit financiële Sector en terrorismebestrijding, *Kamerstukken II* 2001-2002, 28 106, no. ??? and M.J.J.P. Luchtman, e.a. (2002). *Informatie-uitwisseling in het kader van het Financieel Expertise Centrum.* Utrecht, ISBN 90-73272-32-7.

[74] Rekenkamer, Uitwisseling van opsporings- en terrorisme-informatie, *Kamerstukken II* 2002-2003, 28 845, nos. 1-2. In practice, information from the AIVD is used as a lead to initiate criminal investigations or as part of the criminal file and thus as evidence.

*6.2. The use of AIVD intelligence in the administration of criminal justice: Quid juris?*

On 18 December 2002, the three-judge criminal section of the Rotterdam District Court rendered a remarkable judgment[75] in a case in which persons whom the press qualified as the Dutch branch of Al Qaeda were suspected of forgery under ordinary law and of acts in preparation or support of terrorist activity (attacks on the American embassy in Paris and/or an American army base in Belgium). The charges were based on two official reports of the BVD, the AIVD's predecessor, which had obtained information by continuous surveillance and by the use of an informer/infiltrator. Now that sources and modus operandi are not disclosed, it was impossible to verify whether the information was the BVD's own or whether it had been supplied by a foreign sister organization. In this case the question therefore arose whether the Public Prosecutions Department could regard the suspect as a suspect as referred to in Article 27(1) of the Code of Criminal Procedure based on the information supplied by the BVD to the Public Prosecutions Department alone. The District Court answers this question in the negative, now that the gathering of intelligence by the security service did not take place in the context of criminal investigations – which as such are subject to criminal law guarantees – for the purpose of gathering evidence incriminating the suspect, but instead took place in the framework of the duties assigned to the service under the Wiv, which is the gathering of intelligence for the purpose of national security. The District Court considered that the legislator intended the strict separation of intelligence gathering for the purpose of national security and the investigation and prosecution of offences. It therefore held that although the intelligence could be used as a lead to initiate criminal investigations it could not serve as the exclusive basis for meeting the requirements of the concept of suspect under Article 27(1) of the Code of Criminal Procedure. The District Court did not decide to declare the case inadmissible, but to exclude the evidence and then to acquit the accused due to lack of evidence. The Court added that even without the exclusion of evidence the case would have resulted in an acquittal now that insufficient basis had been provided for the charge of preparing an attack.

In a similar case of 31 December 2002 concerning a petition for termination of the pre-trial detention, the Rotterdam District Court sitting in camera reached a different conclusion.[76] The Court considered the testing of the official reports by the national public prosecutor, even if only marginal, a sufficient guarantee to accuse a suspect in accordance with Article 27(1) of the Code of Criminal Procedure based on AIVD intelligence. The decision was not reasoned any further. On 17 January 2003, this judgment was upheld on appeal by the Hague Court of Appeal sitting in camera.[77] The official reports were considered sufficient grounds for a reasonable suspicion of guilt as referred to in Article 27 of the Code of Criminal Procedure or for a reasonable suspicion that organized offences are being committed or plotted as referred to in Article 132a of the Code of Criminal Procedure, now that the source of information may be any third party, including the AIVD, and the

[75] LJN-no. AF2141, case no. 10/150080/01.
[76] LJN-no. AF2579, case no. 10/000109-02.
[77] LJN-no. AF3039, case no. 1000013402.

information therefore does not necessarily need to originate in the framework of criminal investigations in which criminal law guarantees automatically apply. The information does, however, have to yield sufficient concrete facts or circumstances to justify charging.

On 25 April 2003, the Hague Court of Appeal rendered a precedent-setting interlocutory decision as a result of counsel's petition for the hearing of witnesses, the addition of files to the case file and the making available of a CD-rom of tapped telephone conversations.[78] The whole case revolved around official BVD reports and the way in which the information was obtained. To what extent can the acquisition and supply by the BVD of intelligence be made subject to judicial control? The Court emphasized that the duty of secrecy under the Wiv is a legal duty which also applies to the provision of information to the judicial authorities. Waiver of the duty of secrecy is only possible by a joint decision in writing of the Ministers of the Interior and Kingdom Relations and the Minister of Justice. Given the political control of the permanent parliamentary Committee on intelligence and security services and the supervisory committee established under the Wiv 2002 and the strict separation which the legislator intended of the supervision of intelligence duties on the one hand and criminal justice duties on the other, the Court found that the testing of the lawfulness of the acquisition of information that had been supplied to the judicial authorities by the AIVD could only be limited: "It shall have to be limited to cases in which there are strong indications that the information has been obtained through (gross) violations of fundamental rights. To that extent the Court is of the opinion that a good faith principle should apply in the relationship between the (now) AIVD and the judicial authorities in the same way as this applies in extradition law and treaty-based judicial assistance in criminal matters, which implies that the judicial authorities may assume that the information supplied by the BVD/AIVD has at least been obtained lawfully".[79] The Court still added, however, that in addition to assessing lawfulness, the evaluation of the information should also take account of its content, especially when this information could be used as evidence in court: "If the trial is to be fair, (...) the court (...) at some point will have to consider carefully to what extent this information may be regarded as legal evidence".[80]

On 5 June 2003 the three-judge section of the Rotterdam District Court decided an interesting similar case, clearly inspired by the interlocutory decision of the Hague Court of Appeal. Based on official BVD reports, criminal investigations were started, searches were made and persons were arrested in two cases. Afterwards, the information was carelessly compiled, so that it could no longer be verified which acts had been performed in which case. The three-judge section was of the opinion that judicial authorities may in principle assume that information supplied by the AIVD has been lawfully obtained. Only where (gross) violations of fundamental rights appear to have occurred should the principle of good faith between the judicial authorities and the AIVD be deviated from. In the case in question, there had been carelessness, but no gross violations. The District Court was also of

[78] LJN-no. AF7798, case no. 2200076103.
[79] Under 2.4.
[80] Under 2.6.

the opinion that the intelligence could result in a reasonable suspicion of guilt as referred to in Article 27 of the Code of Criminal Procedure and thereby reached the opposite conclusion from the one arrived at in the District Court decision of 18 December 2002. However, the District Court had some difficulty assessing the evidence in the framework of a fair trial, given the duty of secrecy of the AIVD and the national public prosecutor, which makes it impossible to make statements concerning the source of the information. According to the Court, this makes it impossible for the defence to test the origin and factual correctness of the official reports and the Court adds: "the Court cannot find any support in the law for a different way of reasoning, which would stipulate that as the seriousness of the offence of which the suspect has been accused increases, the evidence collected for the purpose of proving the offence needs to meet fewer requirements". This led to the exclusion of evidence and acquittal.

On 21 June 2004, the three-judge section of the Hague Court of Appeal rendered a judgment on appeal against the judgment of the three-judge section of the Rotterdam District Court of 18 December 2002.[81] The Court largely followed the reasoning in the interlocutory decision of 25 April 2003. The starting point is the principle of good faith. Unless there is manifest doubt (concerning (gross) violations of human rights) the Court does not have any duty to test. The legislator has compartmentalized the powers of the AIVD on the one hand and of the judicial authorities on the other. This strict separation does not, however, mean that the AIVD would have to stand back if the judicial authorities start an investigation (or take other action). It does mean that the AIVD and the judicial authorities must keep on exercising their powers exclusively with a view to carrying out their own functions "and it is not appreciated, for instance, that the judicial authorities circumvent the boundaries which have been imposed on its own investigative powers by letting the BVD exercise its powers for the purpose of the criminal investigation and subsequently having the outcome of this included in the criminal proceedings through the national public prosecutor for terrorism."[82] The conclusion is that AIVD intelligence cannot just serve as leads, but may also contain facts or circumstances which produce a reasonable suspicion of guilt as referred to in Article 27 of the Code of Criminal Code, or a reasonable suspicion as referred to in Article 132a of the Code of Criminal Procedure. The Court of Appeal does not discuss the question of the circumstances under which this information could be used as evidence, because the evidence was supported by other evidence. Appeal in cassation has meanwhile been lodged against this decision.

It emerges from this analysis of case law that the initial decision of the Rotterdam District Court has not survived. It is now accepted in case law that AIVD intelligence can be used not just as a lead to initiate criminal investigations, but that the facts and circumstances it contains can also produce a reasonable suspicion of guilt. It also emerges from the case law that courts are extremely cautious in deciding to regard AIVD information as legal evidence, the more so because there are grave doubts as to the possibilities for the defence to test the

[81] LJN-no. AP2058, case no. 2200071403.
[82] Under 4.3.8.

correctness of this information. The duty of secrecy from the Wiv and the marginal testing by the courts will in practice often lead to unfair trials. It is therefore not surprising that, despite the case law, it has still been decided to intervene legislatively.

### *6.3. The Donner Bill concerning the use of AIVD information in criminal proceedings*

Justice Minister Donner has long defended that amendments to the legislation were not necessary to solve the problem and had promised parliament an extensive Note on the matter. However, partly under pressure from parliament the Minister revised his position and on 29 April 2004 the cabinet approved a legislative proposal.

The Bill centres around three themes: the non-disclosure by the examining magistrate of certain information in the interest of national security; the hearing of witnesses as shielded witnesses and an amendment of the law of criminal evidence. The government has rejected and reasoned its rejection of the advice of the Council of State on a number of essential issues.

#### *6.3.1. Preventing disclosure of certain information (Art. 187d Code of Criminal Procedure)*

In the Netherlands witnesses in criminal cases have a duty to appear and give testimony (Art. 342 of the Code of Criminal Procedure). There are exceptions to this main rule, however. Based on Article 293 of the Code of Criminal Procedure, the court can allow witnesses not to answer questions that are not relevant to the case or that may work to the witness's disadvantage and the examining magistrate has the power to exclude answers to questions from the hearing report (see Arts. 187 et seq. and the rules concerning threatened witnesses). It is also possible that certain personal details concerning the witness are not disclosed in connection with nuisance or obstacles to his/her profession, thus providing for limited anonymity. It is proposed to extend the provisions of Article 187 with a view to the hearing of witnesses where the interest of national security is at stake. In this way, details of the modus operandi may be kept secret. This not to be made public information is subsequently kept out the case file and is not disclosed to the Public Prosecutions Department, the suspect/accused, counsel or the trial judge. This also means that certain answers to questions by the defence will not be revealed to the parties either.

#### *6.3.2. (Anonymous) shielded witness (Arts. 226g-226m Code of Criminal Procedure)*

A separate procedure, ex parte and in camera, is introduced for the shielded witness. Like the threatened witness, the shielded witness does not have to appear at the hearing anymore either. The decision is taken by the examining magistrate at the request of the Public Prosecutions Department, the suspect, the trial judge or ex officio. The possibility of hearing

the witness anonymously has also been provided for, namely in case disclosure of the witness's identity could endanger the witness him/herself or national security. The examining magistrate him/herself, however, must be aware of the witness's identity. If possible, the hearing shall take place in camera, but not ex parte. This means that the parties to the proceedings may be present and that the witness is disguised or shielded. It is assumed in the legislative proposal that as a rule such hearings will not only take place in camera, but also ex parte, which means that the parties are only allowed to have questions asked and cannot be present. The report of the hearing is only submitted to the parties with the consent of the witness. Further to the report, the parties may ask further questions. The report may only be added to the case file with the consent of the shielded witness. This implies a break in the examining magistrate's monopoly to assemble the case file.

### *6.3.3. Law of criminal evidence (Art. 344 Code of Criminal Procedure)*

Official AIVD reports may from now on serve as legal evidence in criminal proceedings and not just as documents which may only serve as evidence in connection with the contents of other evidence. This rule is also extended to documents from foreign investigating officers and officials in the service of international institutions. The new rule does not alter the assessment of evidence by the courts. Furthermore, the principle that a suspect/accused cannot be convicted solely on the basis of his/her own testimony (Art. 341(4) Code of Criminal Procedure) and the rule that convictions may not be based on the testimony of one witness alone are maintained. In addition, further evidence is required to support statements from anonymous, shielded witnesses.

### *6.3.4. Advice of the Council of State and government position*

In its expedited advice the Council of State enumerates a number of essential points of criticism. The Council states that this regulation does not necessarily make 'hard' information, i.e. usable in criminal proceedings, out of 'soft' information. The government holds that the rules precisely aim to test hard information without endangering national security. The Council also argues in favour of an in principle in camera, although not ex parte organization of the procedure for questioning the shielded witness, namely from the point of view of the principle of immediacy. The government agrees, but underlines that this situation will mostly be the exception rather than the rule. The interests of national security will in practice nearly always lead to ex parte procedures. The Council further criticizes the partial cancellation of the examining magistrate's exclusive competence in the compilation of the case file. The Council pleads against granting the witness the right to consent. The government does not agree and argues that "with respect to making a decision to hear a witness as a shielded witness, it cannot be asked of the examining magistrate that he makes an assessment on the merits as to whether the interest of national security requires it. He is

not in a position to do so".[83] The Council also has doubts concerning the amendments to the law of evidence as to what constitutes legal proof. The current minimum standard of evidence, especially with regard to AIVD official reports, may, given the limited possibilities for control, actually serve as a guarantee, according to the Council. The government distances itself from this point of view. Finally, the Council is of the opinion that the test of lawfulness does not receive sufficient attention. Thereto, the government underlines the significance of the principle of good faith.

Due to the fact that the procedure was expedited the Dutch Public Prosecutions Department was not consulted. However, it has recently emerged during the discussion of the Bill in Parliament that the Public Prosecutions Department has severely criticised the proposal in a letter to the Minister.[84] Nevertheless, the proposal has recently been approved by Parliament.[85]

## 7. The ECHR and the use of intelligence in criminal proceedings

At first glance, the ECHR is only of limited relevance, now that it is established case law that the European Court of Human Rights (ECtHR) does not decide on the admissibility of evidence and whether information constitutes legal evidence, as this is regarded as a matter of national law, but only deals with the question of whether the procedure in its entirety, including therefore the collection and use of evidence, fulfils the requirements of a fair trial.[86] Of course, the ECtHR has on occasion tested the use of evidence at trial, for instance, with respect to the anonymous witness as the exclusive source of evidence.[87] The Court has also rendered judgments concerning the use of certain investigative techniques in connection with violations of, for example, Article 8 ECHR. From this it follows that judicial control may be ex parte, but "(...) that it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights (...) The rule of law implies, inter alia, that an interference by the executive authorities with an individual's right should be subject to an effective control which should normally be assured by the judiciary, at least in last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure".[88] As regards our topic of discussion, the case law of the ECtHR has dealt with two interesting aspects: 1. the legal testing of intelligence which forms the basis for reasonable suspicion, and 2. the use of secret evidence in ex parte procedures.

---

[83] *Kamerstukken II*, 2003-2004, 29 743, no. 5 p. 4.

[84] Over gebruik van informatie AIVD. OM botst met Donner over nieuwe wet. (2005, April 22) *NRC Handelsblad*.

[85] http://www.eerstekamer.nl/9324000/1/j9vvgh5ihkk7kof/vhfifl1fmyx9/f=y.pdf.

[86] See Van Mechelen et alia v. Netherlands, ECHR, 23 April 1997, NJ 1997, 635.

[87] See Kostovsi v. Netherlands, ECHR, 20 November 1989, A 141, NJ 1990, 245.

[88] Klass v. Germany, ECHR, 4 July 1978, A 28, AA 1979, under 55.

The basis for suspicion and arrest and judicial control have been the subject of various IRA cases. In Fox, Campbell and Hartley[89] v. UK the question is whether, and if so, which information the authorities have to disclose in order to enable a test of the lawfulness of the arrest in the event that it was based on confidential intelligence. In the UK, reasonable suspicion is no longer required for terrorist offences and a lower threshold, that of genuine and bona fide or honest suspicion, now applies. Further, a concrete indication of the offence which is suspected to have been committed no longer needs to be given either. The ECtHR is aware that in the case of terrorism intelligence is often used that cannot be made public, not even in a court of law, without endangering the source. The Court is also understanding of the view of the UK that the practical definition of the term reasonable suspicion may depend on the type of crime, but immediately adds: "Nevertheless, the exigencies of dealing with terrorist crime cannot justify stretching the notion of "reasonableness" to the point where the essence of the safeguard secured by Article 5(1)(c) is impaired (...). Nevertheless, the Court must be enabled to ascertain whether the essence for the safeguard afforded by Article 5(1)(c) has been secured. Consequently, the respondent Government has to furnish at least some facts or information capable of satisfying the Court that the arrested person was reasonably suspected of having committed the alleged offence. This is all the more necessary where, as in the present case, the domestic law does not require reasonable suspicion, but sets a lower threshold by merely requiring honest suspicion". In this case, the facts were not furnished by the UK and the Court decided that there had been a violation of Article 5(1)(c). From a later decision in Murray v. UK,[90] however, the Court does accept that, despite the lower threshold for suspicion in the Northern-Irish anti-terrorism legislation, the requirements for reasonable suspicion were nevertheless fulfilled, as this emerged from additional facts and circumstances. The facts and circumstances in question were derived from the court decisions in the civil damages suit which Murray had started against her arrest. In O'Hara v. UK,[91] where the claimant had been arrested on suspicion of terrorism based on statements by four informers, the ECtHR also held that the requirement of reasonable suspicion was fulfilled. In this case, the reasonable suspicion (not the honest suspicion) was based on statements by four separate informers. The reasonable suspicion was tested by three different UK courts, which in itself is a guarantee against arbitrary arrest. The suspect in these trials did not make use of his right to call into the question the good faith of the police officers who made the arrest. The reasonableness of any suspicion depends on the circumstances of each individual case. In this case, the circumstances put forward result in reasonable suspicion. In his dissenting opinion, judge Loucaides states that here must be a reasonable suspicion in the minds of the enforcement authorities at the moment of arrest and they have to be able to furnish proof of this upon judicial control. These criteria were not met in this case. In Chahal v. UK[92] the ECtHR clearly states that the protection of national security by the use of secret evidence does not render judicial control inoperative: "The Court recognizes that the use of confidential material may be unavoidable

[89] Fox, Campbell and Hartley v. UK, ECHR, 26 June 1990, A 182, p. 15, 28.
[90] Murray v. UK, ECHR, 28 October 1994, NJ 1995, 509.
[91] O'Hara v. UK, ECHR, 16 October 2001, Reports of Judgments and Decisions 2001-X.
[92] Chahal v. UK, ECHR, 15 November 1996, NJ 1997, 301.

where national security is at stake. This does not mean, however, that the national authorities can be free from effective control by the domestic courts whenever they choose to assert that national security and terrorism are involved".[93] Panels without judicial competence are an insufficient guarantee.

In the UK, the use of intelligence as evidence in criminal cases is principally subject to the classic rules of evidence. Under common law, the prosecution has a duty to disclose to the defence all evidence which supports the position of the accused. However, the Attorney General's Guidelines from 1981 made the duty to disclose subject to a discretionary power of the Crown Prosecution Service to withhold sensitive information (national security, identity of an informer, etc.). In this, the Crown Prosecution Service must seek a balance between the measure of sensitivity and the significance of the evidence to the defence. If the result would be a very serious violation of the rights of the defence, the case will just have to be dismissed. UK Courts of Appeal have rendered many decisions on this issue. In R. v. Ward (1992)[94] it was held that it is up to the court, not the prosecution, to weigh the interests. In R. v. Davis, Johnson and Rowe (1993)[95] the Court of Appeal developed three options for the procedure of testing: 1. the test takes place in ordinary adversarial criminal proceedings where only the type of material is indicated, or 2. the test takes place in an ex parte procedure, where the type of material is not disclosed (secret information), or 3. the test takes place in an ex parte procedure, which is not disclosed to the defence as its disclosure would reveal the nature of the evidence (secret information and secret procedure). In R. v. Turner (1994)[96] the Court of Appeal warns that R. v. Ward has led to too many requests for disclosure of confidential evidence: "We wish to alert judges to the need to scrutinize applications for disclosure of details about informants with very great care (...) Even when the informant has participated, the judge will need to consider whether his role so impinges on an issue of interest to the defence, present or potential, as to make disclosure necessary". The ex parte procedures have resulted in several cases before the ECtHR. In Jasper v. UK[97] the person concerned was kept under observation, tapped and subsequently arrested on drug charges on the basis of intelligence. The prosecution applied for non-disclosure of the evidence based on public interest immunity. The defence was informed of the application and the ex parte hearing, but was not given any information concerning the sources and means of evidence and was not informed of the court's reasoning either. The ECtHR emphasized the importance of the free exchange of evidence between the parties, but also recognized that the right to disclosure of evidence is not an absolute right and may conflict with other interests, such as national security, the protection of witnesses and of

[93] See hereon E. Myjer (2003). Rechten van de mens en bestrijding van terrorisme; enige opmerkingen over de Europese aanpak en over de rol van de officier van justitie, *Trema*, 336-342 and C. Warbrick (2002). The Principles of the European Convention on Human Rights and the Response of States to Terrorism, *European Human Rights Law Review*, 287-314.

[94] The Weekly Law Reports 1993 (1) p. 619-692.

[95] The Weekly Law Reports 1993 (1) p. 613-618.

[96] All England Law Reports 1995 (3) p. 432-436.

[97] Jasper v. UK, ECHR, 16 February 2000, 27052/95.

sources of evidence, modus operandi, etc. The Court accepts secret evidence provided that this limitation of the rights of the defence "be counterbalanced by the procedures followed by the judicial authorities (equality of arms)". In the case in question, the Court was of the opinion that this balancing had been successful, now that the furnishing of proof had been tested by the trial judge and because the secret information was not part of the case file, but a lead obtained from a phone tapping operation.[98] In a collective dissenting opinion, six magistrates sharply protested against this decision and argued that the fact that the defence was not informed concerning the type of evidence and material and the fact that the outcome of the ex parte procedure was not reasoned were contrary to the nature of adversarial proceedings to such an extent that this could not be rectified by the trial judge. In Edwards and Lewis v. UK,[99] a drug case where use was made of agents provocateurs, a similar ex parte procedure was applied in which the defence was not informed of the type of evidence. However, in this case the material in question was used as evidence at the trial. Moreover, the undercover police officer, who was the only witness called during the hearing, was questioned anonymously. It was crucial for the defence to be able to verify whether this constituted entrapment by the police. It also emerged at the trial that intelligence had been submitted in the ex parte procedure concerning the accused's involvement in drug offences in the past without the defence having been notified of this so that they could have contested these facts. In this case the Court established a violation of Article 6(1). This was also the outcome of Dowsett v. UK[100] as the trial judge had failed to perform the necessary judicial control and this could not be remedied on appeal.[101] How important this judicial control is also becomes clear from Tinnelly & Sons and others and McElduff and others v. UK,[102] a case in which it was decided, based on intelligence, to reject a tender in a public procurement project in Northern Ireland. The applicants were refused public work contract or the security clearance necessary to obtain those contracts on account of their religious beliefs or political opinions. The refusal was based on a certificate, being conclusive evidence, from the Secretary of State relying on intelligence. The ECtHR holds that the lack of independent and full scrutiny by a judicial authority violates art. 6 ECHR.

[98] Along the same lines P.G. and J.H. v. UK, ECHR, 25 September 2001, NJ 2003, 670.
[99] Edwards and Lewis v. UK, ECHR, 22 July 2003, 39647/98 and 40461/98.
[100] Dowsett v. UK, ECHR, 24 June 2003, 39482/98.
[101] In G.M.R and A K.P. v. UK, decision of 19 September 2000, the Court held that the appeal procedure did offer sufficient guarantees.
[102] Tinnelly & Sons and others and McElduff and others v. UK, ECHR, 10 July 1998, Reports 1998-IV.

## 8. Conclusion

From the comparative law analysis (USA, EU, the Netherlands, UK and ECHR) it clearly emerges that the use of intelligence in the administration of criminal justice touches upon the foundations of a fair trial and can therefore not be reduced to a detail of criminal prosecution. The public administration of criminal justice[103] is essential to the legality of the dispensation of justice as a public matter. The internal public nature of criminal justice proceedings requires that the participants in the proceedings may be present in the performance of acts of procedure or that they are informed thereof, that they have access to the evidence and that they can have this evidence tested in a fair trial. The external public nature of the proceedings requires that cases are not heard ex parte and in camera. Exceptions to this public nature, both internal and external, are of course conceivable, not in the least in the interest of the suspect/accused or witnesses, but also in the interest of national security. The ECtHR not only accepts that information from intelligence services may be used as a secret lead for criminal investigations, but also that this intelligence is able to produce a reasonable suspicion of guilt. These exception must, however, be defined in such a way that it is not the discretionary power of the intelligence services and/or the enforcement bodies to decide on the use of secret evidence under criminal law. Experience in the US has shown that the screening walls and the chaperone requirements are necessary filters in the movement of information between the intelligence services and the investigative authorities. According to the ECtHR, the decision concerning the use of secret information as the basis for suspicion or as evidence in criminal cases must be subject to independent judicial control whereby the court must be competent to assess the lawfulness and reliability of the information and the sources. In my view, the starting point here cannot be an assumption of lawfulness and reliability and marginal judicial testing. However, it is not appropriate to speak of the free movement of information in this context either. The principle of good faith between the AIVD and the investigative authorities as elaborated by the Hague Court of Appeal – no testing, unless there are indications of the (gross) violation of human rights – must also be considered a dangerous feat of reasoning. Belief in the reliability of the AIVD as a partner (such as exists between nations in the case of extradition) is not the essential factor, but the rule-of-law function of the courts with respect to secret evidence that the suspect/accused is by definition unable to assess. In short, in a fair trial, judicial control is a fundamental counterbalance against the restriction of the rights of the defence. The idea that the court would be unable to perform any testing or only marginal testing due to the fact that the legislator desired the compartmentalization of the relationship between the AIVD and the criminal justice authorities is untenable. Information flow has to be accompanied by judicial information control. How important judicial testing is becomes clear from the Classified Information Procedures Act which has been elaborated as part of the federal law of criminal procedure in the US and from the case law of the ECtHR. Testing the lawfulness of the intelligence evidently also concerns the possible direction of the gathering of information by the AIVD. The possibility must be guarded against that the AIVD, either in cooperation with police and judicial authorities or not, employs its far-

[103] A. Beijer, e.a. (ed.) (2002). Openbare rechtspleging. Deventer: Kluwer.

reaching secret powers of investigation for the main purpose of criminal law objectives and in so doing circumvents the guarantees of criminal justice. Parallel investigations are conceivable, but information laundering - whereby information is produced by a different body than the one which gathered it - wrapped in the veil of confidential sources and the duty of secrecy under the Wiv is not allowed. So far, the powers under the Wiv have only been used in the Netherlands for strengthening the position of information and the possible additional yields of surveillance, i.e. information which could also be of interest to the criminal justice authorities. The discussion in the US concerning the difference between primary and significant intelligence purpose indicates that the use of Wiv powers also for criminal justice purposes cannot be reduced to mere additional yields. The court exercising judicial control must also have the power to order disclosure of the evidence. If this is refused, the prosecution may still withdraw the evidence or dismiss the case. This means that the Donner Bill still leaves some issues for regulation. The duty of secrecy under the Wiv has to be reviewed in respect of the supply of information to the judicial authorities and the test before the court. The filters between the AIVD and the judicial authorities have to be formalized. Furthermore, the conditions under which the defence may compel the prosecution and the AIVD to submit secret evidence in criminal proceedings require regulation.

A second point of interest is the organization of the procedure for judicial control itself. In many cases, judicial control cannot be exercised at a public hearing, but often not in camera and inter partes either. The opportunity for the defendant and his counsel to inspect documents or directly question incriminating witnesses is therefore limited or non-existent. In the interest of national security the rights of the defence can be limited, provided that sufficient compensatory measures are taken. The Donner Bill formulates rules under which the examining magistrate is informed of all relevant facts and gives a reasoned assessment of the reliability of the information supplied. The examining magistrate has a duty to investigate the reliability of the statement (person, circumstances, etc.) and a duty to reason his/her decision. The question is, however, whether the examining magistrate can qualify as an independent and impartial court. The Bill restricts investigations into the lawfulness of the information to exceptional cases of gross violations of human rights in the acquisition of the information. As a starting point, the principle of good faith applies. Investigations into the reliability of the information are also marginal in character, judging from the Explanatory Memorandum: "with respect to making a decision to hear a witness as a shielded witness, it cannot be asked of the examining magistrate that he makes an assessment on the merits as to whether the interest of national security requires it. He is not in a position to do so".[104] Appeal against the examining magistrate's decision to apply the procedure for the shielded witness is also ruled out, as "this is connected with the marginal character of the evaluation framework: the decision whether to grant shielded witness status will often solely depend on rather objective criteria for assessment (whether the person in question is in the service of the AIVD, what his/her function is, etc.)".[105] The fact that the shielded witness determines

[104] *Kamerstukken II*, 2003-2004, 29743, no. 5 p. 4.
[105] *Kamerstukken II*, 2003-2004, 29743, no. 3, p. 13.

whether the hearing report is submitted to the parties or whether it is added to the case file (double consent of the shielded witness) undermines the independence and impartiality of the examining magistrate. Also important in the conduct of a fair trial is the degree to which the trial judge has reasoned the use and reliability of the evidence. The Explanatory Memorandum states that the trial judge may always freely assess the findings of the examining magistrate, but in fact the information needed for this at his/her disposal is quite limited. The proposed rules make the trial judge too dependent upon the examining magistrate. As opposed to under the general rules for protecting witnesses, the trial judge cannot order the shielded witness to appear at the hearing. The prosecution can prevent the giving of testimony at the hearing. The trial judge does not have access to all the sources used by the examine magistrate either. He does not have access to non-public material. In testing reliability and lawfulness, the trial judge has to rely completely on the marginal assessment of the examining magistrate.

The third and final point concerns the evidentiary quality of and the extent to which AIVD intelligence can serve as legal evidence. On this point, there is no decisive ECHR case law. The procedure and rules proposed in the Donner Bill concerning legal proof run parallel to the regulation of the procedure involving the anonymous witness in the Code of Criminal Procedure.[106] It has become clear from ECHR case law concerning the anonymous witness[107] that convictions may not rely to a decisive extent on anonymous information. The degree to which supporting evidence is needed depends on the degree to which the right to question is limited. In the case of AIVD intelligence, these limitations will mostly be considerable, implying a by definition limited role for this evidence in criminal proceedings. Provisions that AIVD evidence cannot be exclusive evidence do not meet the ECHR standard. Of further relevance here are Articles 344(a) and 344(3) of the Code of Criminal Procedure. Article 344(3) provides that an anonymous written statement may not be used as evidence, unless the ruling on the evidence is to an important degree supported by other evidence and the accused has not claimed the right to hear the witness. If, however, the accused has claimed this right, the statement may be regarded as testimony in accordance with Article 295 of the Code of Criminal Procedure, but the minimum rules of Article 344a must be respected at all times. This means that this is only possible for serious violations of legal order and on the condition that the witness has been heard by the examining magistrate, in accordance with the rules concerning the threatened witness in Articles 266(c) to 266(f) of the Code of Criminal Procedure.

It remains to be seen whether the Donner Bill, which was inspired by the rules concerning the anonymous witness, will be able to pass the ECHR test. The Explanatory Memorandum is non-committal in this respect: "Following the procedure for the shielded witness does not guarantee that this means that the requirements of Article 6 ECHR are adequately met under

[106] See hereon also J.W. Fokkens (2004). Strafrecht en terrorisme. *NJB*, 1347-1351.

[107] Unterpertinger v. Austria, EHRM, 24 November 1986, NJ 1988, 745; Kostovsi v. Netherlands, EHRM, 20 November 1989, A 141, NJ 1990, 245; and Lüdi v. Switzerland, EHRM 15 June 1992, A 238, NJCM-bulletin 1992, 810.

all circumstances. Every criminal case conducted in accordance with the proposed rules will in addition have to be tested (by the court) against the treaty provision referred to".[108] It is also questionable whether these rules do not undermine the so urgently desired separation between the functions of the intelligence services and those of the investigative authorities. There is a risk that from now on, in cases touching upon national security, marginal standards will be set with respect to the use of information obtained by the AIVD by means of investigative powers which are comparable to the powers of the investigative authorities. It is also important that the European proposals assuming the free movement of information between the intelligence services and the investigative authorities are critically examined. The comparison with US law demonstrates the significance of filters in the movement of information and of judicial control. Neither Europe, nor the Netherlands seems to have sufficiently learned the lesson implied. In any case, the fight against terrorism cannot serve as an argument to undermine *sub rosa* the foundations of the rule of law and the public administration of criminal justice. *Sub lege libertas.*

[108] *Kamerstukken II* 2003-2004, 29 743, p. 12.