eucrim
2011 / 3
THE EUROPEAN CRIMINAL LAW ASSOCIATIONS' FORUM

Focus: Information and Investigations
Dossier particulier: Information et investigations
Schwerpunktthema: Information und Ermittlungen

2011 / 3 ISSUE / ÉDITION / AUSGABE

Contents

News*

European Union

Council of Europe

Articles

Information and Investigations

Imprint

* News contain internet links referring to more detailed information. These links can be easily accessed either by clicking on the respective ID-number of the desired link in the online-journal or – for print version readers – by accessing our webpage www.mpicc.de/eucrim/search.php and then entering the ID-number of the link in the search form.

Editorial

Dear Readers,

One of the fastest growing needs in information management for global networks is cybersecurity and its related policies. The leading role of information technology and the growth of e-commerce have made cybersecurity essential to the economy and the operation of infrastructure systems.

In the past year, the European Network and Information Security Agency (ENISA) has been actively strengthening bridges with fellow EU agencies that are part of its "Justice, Freedom and Security" cluster. With its mission to protect information, ENISA has been called upon to provide insight, expert advice, and guidance to its fellow agencies in order to deal with the continually expanding need for cybersecurity. We are now aiming to assist in the way cybercrime is perceived and handled on the European and international legal digital frontline. Cyberthreats are a global reality, which is developing in increasingly rapid, sophisticated, and sinister ways, and we believe international coordination of the networks focusing on the security policy landscape is essential. This includes cooperation throughout Europe as well as worldwide, both in the public and private sectors. In many ways, it is this international dimension that distinguishes cybersecurity from what we have referred to in the past as information security. The alignment of European and international legislative frameworks and procedures as well as collaboration models will ensure adequate policy implementation.

As announced by US Homeland Security Secretary, Janet Napolitano, and European Commission Vice President for the Digital Agenda, Neelie Kroes, a joint effort to deal with cybersecurity and cybercrime issues will result in a cyber-exercise between the EU and the US in 2011. Its code name was recently agreed upon: "Cyber Atlantic 2011." ENISA will facilitate the organisation and management of this project.

Worldwide, military communities are debating matters such as cyberwar and cyberdefence; law and enforcement networks are analysing threats and solutions related to cybercrime; and intelligence task forces are concerned with cyberespionage. In today's information society, we are concerned with the way in which new threats affect infrastructures, applications, and information data related to internal markets as well as the EU's Information Society. Information security

Udo Helmbrecht

involves the protection of digital information from accidental or unauthorised access, destruction, modification, or disclosure. Now, the ever expanding dimension of the cyber highways means the magnitude of breaches is alarming, unregulated, and needs to be tackled with new strategies. One of ENISA's tasks is to bridge the gap between policy and operational requirements; it does so by being an impartial European platform for information exchange amongst EU Member States and also with their international counterparts. The agency is working hard in the relevant fields of information security management in order to be in the unique position of brokering the way forward. ENISA is currently supporting the establishment of the EU Institutional CERT (Computer Emergency Response Team). The level of cyberthreats for European institutions is very high, and multiple incidents have already occurred, as recently as March/April 2011 when European Commission IT experts identified an intrusion into their systems.

A joint commitment at the international level will result in a brand new and common understanding of cyber policy implementation, ensuring consistent cross-border defence mechanisms for a safe and sound European digital society.

Professor Udo Helmbrecht
Executive Director of ENISA

European Union*

Reported by Dr. Els De Busser (EDB), Sabrina Staats (ST), Cornelia Riehle (CR) and Nevena Kostova (NK)

Foundations

The Stockholm Programme

Working Method for EU Security Cooperation and Coordination

The 2009 Stockholm Programme provided a general framework for connecting the external and internal aspects of EU security (see eucrim 4/2009, pp. 122-123). On 6 June 2011, the General Secretariat of the Council presented a working method for closer cooperation and coordination in the field of EU security to the COREPER. The initiative for this working method was launched by the Hungarian presidency and endorsed by the COSI.

The document presented includes proposals for establishing a working method by introducing regular inter-institutional meetings to inform representatives of the presidency, Council, and Commission European and External Action Service, on the one hand, and joint meetings between the relevant Council preparatory bodies, on the other. The latter involves pairs of preparatory bodies in the field of external security, with preparatory bodies in the field of internal security, e.g., the Political and Security Committee paired with COSI in a joint meeting.

Additionally, the above-mentioned document identifies the key challenges in EU security as possible areas for cooperation, including terrorism, serious and organised crime, cybercrime and cybersecurity as well as natural and man-made disasters.

During the JHA Council of 9-10 June 2011, the Council took note of this working method. (EDB)

➤eucrim ID=1103001

Enlargement of the EU

Croatia Ready for Accession in 2013

Following the EU Summit on 24 June 2011, the President of the European Council, Herman Van Rompuy, announced that the accession treaty between Croatia and the EU Member States will be signed by the end of 2011. Together with Commission President José Manuel Barroso, he congratulated the Croatian Prime Minister and the Hungarian Presidency for their efforts in the negotiations.

The negotiations on Croatia's accession to the EU started in October 2005 and were officially concluded on 30 June 2011. During the process, difficult hurdles were taken such as the reform of the judiciary and cooperation with the ICTY (see eucrim 2/2011, p. 51 and eucrim 1/2011, pp. 2-3).

On 1 July 2013, Croatia will officially become the 28th Member State of the EU, following the ratification procedures in the Member States and in Croatia. (EDB)

➤eucrim ID=1103002

Serbia One Big Step Closer to Becoming Candidate Member State

On 26 May 2011, the news that Serbian authorities had arrested former Serbian General Ratko Mladić was welcomed by President of the European Council Herman Van Rompuy, High Representative Catherine Ashton, President of the Commission José Manuel Barroso, and Commissioner for Enlargement Štefan Füle.

Cooperation with the ICTY has been an essential element of the Stabilisation and Association Agreement (SAA) signed between Serbia and the EU on 29 April 2008. The aims of the SAA are *inter alia:*

- To support the efforts of Serbia to strengthen democracy and the rule of law;
- To contribute to political, economic, and institutional stability in Serbia;
- To support the country's efforts to develop its economic and international

* If not stated otherwise, the news reported in the following sections cover the period May – July 2011.

cooperation, including via the approximation of its legislation to that of the Community.

All EU Member States must ratify the SAA, a process that was started on 14 June 2010, following a report by the Prosecutor of the ICTY stating that Serbia has maintained cooperation with the Tribunal with a view to delivering positive results in the future.

In his statement after the arrest of Ratko Mladić, Commissioner for Enlargement Štefan Füle described the arrest as the removal of a great obstacle on the Serbian road to the EU. (EDB)

➤eucrim ID=1103003

Schengen

Commission's Plans Regarding Schengen and Migration Policy

As a follow-up to the Communication on migration presented on 4 May 2011 (see eucrim 2/2011, pp. 51-52), the Commission proposed a set of measures on 24 May 2011. The main objective of the measures is to improve management of migration flows from the Southern Mediterranean region after the recent events in Tunisia, Libya, and other countries.

The Commission proposed a package of measures consisting of three components:

- A Communication on "Dialogue for migration, mobility and security with the Southern Mediterranean countries";
- The Annual Report on Immigration and Asylum of 2010;
- A proposal to amend Regulation 539/2001 listing third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from this requirement.

The package of measures was discussed during the JHA Council of 9 June 2011 and the European Council of 24 June 2011. The heads of state and government stressed that the free movement of persons is a core principle of the EU but also recognised the pressure on the external border and thus on one or more specific Member State(s), following exceptional circumstances. The Council therefore requested the Commission to propose a mechanism to respond to these exceptional circumstances. This may, however, put the functioning of the Schengen cooperation at risk. In truly critical situations, internal borders could be reintroduced, but only under strict conditions. This means that measures should be taken on the basis of specified objective criteria and based on a common assessment, with a limited scope, and for a limited period of time, taking into account the need to be able to react in urgent cases.

Following the European Council, the Commission responded by stating that it is ready to present proposals for these measures in early autumn 2011.

The Commission also stated that it was ready to present legislative proposals on a European Border Surveillance System (EUROSUR) towards the end of 2011. EUROSUR should be operational by 2013 and aims to ensure that operational information about any incident at the external border can be exchanged in real-time between neighbouring Member States.

Additionally, the European Council expressed its wish to see the Common European Asylum System completed by 2012 and to develop partnerships with the countries of the Southern and Eastern Neighbourhood, such as Tunisia, Morocco, and Egypt. (EDB)

➤eucrim ID=1103004

European Parliament's Position Regarding Schengen Revision

The EP reacted strongly to the plans to revise the Schengen rules. In its Resolution of 7 July 2011, the EP expressed the opinion that the aforementioned problems with the Schengen borders stem from "a reluctance to implement common European policies in other fields, most crucially a common European asylum and migration system." According to the EP, reintroducing border controls on an exceptional basis would definitely not reinforce the Schengen system. With this resolution, the EP also addressed Denmark's reintroduction of border controls (see this issue of eucrim p. 97). Thus, the EP affirmed its opposition to any new Schengen mechanism with objectives other than those of enhancing freedom of movement and reinforcing EU governance of the Schengen area. (EDB)

➤eucrim ID=1103005

Commission Confirms that France and Italy Formally Respected Schengen

On 25 July 2011, the Commissioner for Home Affairs, Cecilia Malmström, stated that France and Italy formally complied with the rules applicable to the Schengen zone after the arrival of large groups of immigrants following recent events in North Africa.

The measures that had been taken include the issuing of residence permits and travel documents by Italian authorities and police checks by French authorities. After analysis, the Commission could not conclude that these measures were in breach of the Schengen rules. However, Commissioner Malmström regretted that the spirit of the Schengen rules had not been respected.

Therefore, governance of the Schengen zone should be addressed in a comprehensive and coordinated way. Commissioner Malmström reiterated that proposals from the Commission would be presented in September 2011. (EDB)

➤eucrim ID=1103006

Denmark Reinstalls Border Controls

On 11 May 2011, the Danish government informed the European Commission of their plans to strengthen border control by establishing a permanent and visible customs control at the Danish borders. The reintroduction of border controls is the result of a compromise between the Danish government and the Danish People's Party.

After the Commission made a pre-

liminary assessment, Commissioner for Home Affairs Malmström expressed concern that the measures could be in breach of Denmark's obligations under EU and international law.

Following this statement, a dialogue commenced between the Commission and the Danish authorities regarding the compliance of Danish rules with EU legislation on the free movement of goods, services, and persons. In order to verify whether these rules are also being put in practice accordingly, Commissioner Malmström announced that European Commission experts would visit Denmark on 14 and 15 July 2011. Afterwards, the visiting experts reported that they were unable to get sufficient justifications from the Danish side for the intensification of the controls at the internal borders. In particular, the risk assessment required to justify the controls was not sufficient and there were no clear instructions to the border control officers on how to carry out controls. Commissioner Malmström reacted concerned and did not exclude additional visits if necessary. (EDB)

➤eucrim ID=1103007

Bulgaria and Romania Not Yet Part of the Schengen Area

After discussions on whether or not to allow Bulgaria and Romania to enter the Schengen area (see eucrim 2/2011, pp. 57-58 and eucrim 1/2011 pp. 3-4), the EP voted in favour of their accession on 8 June 2011. The MEPs concluded that, although some remaining issues will require regular reporting and further attention in the future, they do not constitute an obstacle to full Schengen membership for either Bulgaria or Romania.

Even though the result of this vote was sent to the Council, the JHA Council of 9 June 2011 decided not to allow Bulgaria and Romania to enter the Schengen zone. The Council stated that the Schengen evaluation process for both countries has been completed and concluded that it will return to the issue no later than September 2011. (EDB)

➤eucrim ID=1103008

Common abbreviations

AML	Anti-Money Laundering
CBRN	Chemical, Biological, Radiological, and Nuclear
CCJE	Consultative Council of European Judges
CDPC	European Committee on Crime Problems
CEPEJ	European Commission on the Efficiency of Justice
CEPOL	European Police College
CFT	Combating the Financing of Terrorism
CJEU	Court of Justice of the European Union
COSI	Standing Committee on Operational Cooperation on Internal Security
COREPER	Committee of Permanent Representatives
DG	Directorate General
EAW	European Arrest Warrant
ECHR	European Convention of Human Rights
ECJ	European Court of Justice (one of the 3 courts of the CJEU)
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EIO	European Investigation Order
EJN	European Judicial Network
ENISA	European Network and Information Security Agency
(M)EP	(Members of the) European Parliament
EPO	European Protection Order
EPPO	European Public Prosecutor Office
GRECO	Group of States against Corruption
GRETA	Group of Experts on Action against Trafficking in Human Beings
ICTY	International Criminal Tribunal for the former Yugoslavia
JHA	Justice and Home Affairs
JIT	Joint Investigation Team
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
OLAF	European Anti-Fraud Office
SIS	Schengen Information System
SitCen	Joint Situation Centre

Institutions

Council

UN Grants EU Representation Rights

On 3 May 2011, the UN adopted a Resolution granting the EU – as a regional bloc – several representation rights before the Assembly. The EU now has the right to make interventions, the right of reply, and the possibility to present oral proposals and amendments before the UN.

EU delegations may speak with representatives of major groups or be invited to participate in the Assembly's general debates. They now have the opportunity to exercise the right of reply, restricted to one intervention per item, and their communications will be circulated directly.

Following the example led by the EU, a number of delegates from other regional groups (e.g., the Caribbean Community, the African Union, and the Arab Group) expressed their expectations that the adopted text will serve as a precedent and that the EU will support requests for similar rights by other regional groups. According to the Resolution, the Assembly might adopt modalities for the par-

ticipation of representatives from other regional organisations.

Many concerns arose as to whether the adoption of the Resolution might change the nature and organisation of the UN as an intergovernmental body. Small Member States, like Nauru, are concerned that granting rights to regional organisations may be detrimental to the influence of small States that do not enjoy the political and economic influence of large developed countries. Hungary's representative, who submitted the draft resolution on behalf of the EU, replied that the rights granted to the bloc would in no way increase the EU's capacity for action, since the EU will remain an observer in the General Assembly without the rights to vote, to co-sponsor resolutions or decisions, or to put forward candidates.

In a statement following the adoption, Catherine Ashton, the High Representative of the EU for Foreign Affairs and Security Policy and Vice-President of the Commission, welcomed the adoption of the resolution and said that it "enables EU representatives to present and promote the EU's positions in the UN, as agreed by its Member States." (ST)

➤eucrim ID=1103009

Court of Justice of the EU

Parliament Must Disclose Galvin Report after ECJ Judgment

On 7 June 2011, the ECJ delivered a decision on a case (T-471/08) regarding the release of the so-called "Galvin Report."

The "Galvin Report" (06/02) contains details on how some MEPs abused an allowance system intended for parliamentary assistants, e.g., by employing family members, by using service contracts to channel funds from their allowances to companies that they had set up, or by claiming to pay the full allowance (approx. €200,000) to only one person. In many cases, no value added tax was paid. The report also found that, since there was a failure to submit supporting documents such as receipts in order to prove spending, there was no documentary proof for many of the fees paid out.

In June 2008, the applicant, Irish barrister Ciarán Toland, requested access to the 2006 Annual Report of the EP's Internal Audit Service. In July 2008, the EP granted access to 13 of the 16 internal audit reports and partial access to two further internal audit reports. The EP fully refused access to the fourteenth report (The "Galvin report", Report 06/02) on the grounds that it contains sensitive information with respect to a future reform of the system of parliamentary assistance. Granting access to the requested documents would undermine the ongoing decision-making process.

The applicant, supported by Denmark, Finland, and Sweden, then turned to the ECJ to seek annulment of this decision.

The ECJ now ruled that "the fact that the use by the Members of Parliament of the financial resources made available to them is a sensitive matter followed with great interest by the media (...) cannot constitute in itself an objective reason sufficient to justify the concern that the decision-making process would be seriously undermined, without calling into question the very principle of transparency intended by the EC Treaty." Also, "the alleged complexity of the decision-making process did not constitute in itself a specific reason to fear that disclosure (…) would seriously undermine that process". The court therefore annulled the contested decision.

The report led to a review of the EP's allowance system and to the creation of a new, stricter system of controls which came into force after the 2009 elections. Although parts of report 06/02 (the "Galvin Report") were already leaked in early 2009, the EP refused to publish the whole report. Following the ECJ's judgment, the Parliament's bureau published the report on its website on 22 June 2011. (ST)

➤eucrim ID=1103010

OLAF

OLAF and Eurojust Strengthen Cooperation

On 19 July 2011, OLAF's Director-General, Giovanni Kessler, met with Aled Williams, President of Eurojust, to discuss ways to improve cooperation in combating crime detrimental to the EU's financial interests. Mr. Kessler emphasised that both institutions complement each other in their aim to safeguard the financial interests of the EU. He reiterated that interaction and cooperation between the agencies should be enhanced to achieve their common goal. During the meeting, both agencies agreed on the enhancement of cooperation and on the regular exchange of information on complex and multinational cases. (ST)

➤eucrim ID=1103011

OLAF Considers Joint Investigations with World Bank and UN

On 27 May 2011, OLAF's Director-General, Giovanni Kessler, met with Executive Directors of the World Bank and UN representatives at the 12th Conference of International Investigators in Washington DC. OLAF intends to strengthen cooperation with the investigative services of the World Bank and the UN and is considering "joint investigations on cases of common interest." (ST)

➤eucrim ID=1103012

Court of Auditors Follows Up on Management of OLAF

On 2 May 2011, the European Court of Auditors (ECA) released its follow-up audit (special report No. 2/2011) on the management of OLAF (No. 1/2005), issued in 2005. The audit follows up on measures taken after the 2005 report and proposes new actions to improve OLAF's work. The audit finds that most recommendations have been implemented to varying degrees and suggests that OLAF continue to ensure their full implementation.

The ECA also made a series of new

recommendations to enhance the performance of OLAF, e.g.:

- To increase the amount of time spent on its investigative function;
- To improve efficiency by including estimates of resources required as well as deadlines in investigation plans;
- To publish performance statistics on activity, potential, and actual results;
- To define a procedure for consulting the Supervisory Committee before transmitting information to national judicial authorities. (ST)

➤eucrim ID=1103013

OLAF and Italian Authorities Jointly Fight Development Aid Fraud

Following an OLAF investigation in close cooperation with the Italian judicial authorities, the Italian *Carabinieri* Antifraud-Unit (NAC) arrested two people in connection with the fraudulent use of funds from the EU and the European Development Fund (EDF). Both suspects are connected to an Italian company, which received at least €10 million from the EU and the EDF for the delivery and supply of goods to several developing countries. The investigation showed that the company repeatedly acted in breach of the contracts related to EU and EDF funds. (ST)

➤eucrim ID=1103014

Joint Investigation between OLAF and Belgian Authorities Leads to Imprisonment of EU Staff Member

On 12 May 2011, OLAF released information on investigations initiated by OLAF and then carried out as a joint investigation between OLAF and Belgian judicial authorities, The investigation led to the conviction of a former staff member from the EU delegation to Ukraine on the charge of corruption. He was sentenced to 18 months of imprisonment and a fine of €5000.

The staff member had asked bidders in a tender process for a 4% commission. One of the bidding companies agreed to pay a commission of 2.5% of the contract value of about €19 million. The staff member did not receive any commission, however, since the tender was stopped before a contract was concluded. OLAF initially received information from a company that had turned down the staff member's offer and then opened an investigation into the matter. (ST)

➤eucrim ID=1103015

OLAF and Italian Authorities Fight Fraud in EU-Funded Research Projects

On 5 May 2011, Italian authorities announced that the Italian judiciary had concluded a criminal investigation into a suspected fraud network in EU-funded research projects. The investigation was conducted in cooperation with OLAF and concerns 22 projects with a total amount of over €50 million in funding. The networks of various companies operating in many Member States are suspected of claiming reimbursements of non-existent expenses and of using sham companies as partners or sub-contractors. (ST)

➤eucrim ID=1103016

Europol

Terrorism Situation and Trend Report 2011

Europol has published its 2011 EU Terrorism Situation and Trend Report (TE-SAT 2011). Europol Director Rob Wainwright presented the report in the EP on 29 April 2011. Besides giving a general overview of the situation in the EU in 2010, the report contains detailed chapters on the phenomena of Islamist terrorism, separatist terrorism, left-wing and anarchist terrorism, right-wing terrorism, and single-issue terrorism. Overall, the report finds that the threat of terrorism remains high in the EU and is diversifying in scope and impact.

In 2010, the EU experienced 249 terrorist attacks in nine Member States; the majority of them took place in France (84) and Spain (90). 611 individuals were arrested for terrorism-related offences. 46 threats were made by terrorist organisations against EU Member States (threat statements by and against individuals were not counted), the vast majority of these having an Islamist terrorist background. 307 individuals were tried on terrorism charges compared to 398 individuals tried in 2009. The highest number of individuals tried for terrorist offences in 2010 was in Spain. As regards communication, the Internet has been a crucial facilitating factor for terrorists and extremists.

Regarding Islamist terrorism, the main findings of the report conclude that three Islamist terrorist attacks were carried out in Member States in 2010. 179 individuals were arrested for Islamist terrorist offences, and 89 individuals were arrested for the preparation of attacks in the EU. Only 20% of the arrested persons were linked to an Islamist terrorist group while a substantial number of the arrested persons were either members of quasi autonomous jihadist cells or self-radicalised "lone actors." The fact that the proportion of arrested suspects with EU citizenship or born in the EU is further increasing makes home-grown terrorism and the extreme radicalisation of EU citizens an ongoing source of concern. The Internet, online forums, and social networks provide useful communication channels for propaganda, radicalisation, incitement, and recruitment. Finally, it is reported that the security situation outside the EU impacts on Islamist terrorist activities inside the EU.

Looking at separatist terrorism, 160 separatist attacks were counted in 2010, most of them taking place in France and Spain. 349 individuals were arrested for separatist terrorism-related offences, with the majority stemming from France (123), Spain (104), and the Republic of Ireland (57). Notably, 22% of the arrested suspects were female, which is a high percentage in comparison to other types of terrorism. As regards financing, the main source of income for most separatist terrorist groups in Europe is extortion. Furthermore, the report observes an

increased level of international cooperation between separatist terrorist groups inside and outside the EU. Finally, it is found that ethno-nationalist and separatist terrorist groups, such as ETA and the PKK/KONGRA-GEL, continue to seek international recognition and political self-determination. They are motivated by nationalism, ethnicity, and/or religion.

In 2010, left-wing and anarchist groups remained highly active, being responsible for 45 attacks and six fatalities. 34 individuals were arrested for left-wing and anarchist terrorist activities. While these groups were traditionally active in Greece, Italy, and Spain, other countries have seen increased activity in 2010, which may be explained by increasing social unrest due to the global economic downturn. From the modus operandi observed in a number of attacks, conclusions may be drawn as to increased transnational coordination between terrorist and extremist left-wing and anarchist groups and an emerging international coordination.

Although no right-wing terrorist attacks occurred in the EU in 2010, the report sees right-wing extremist groups becoming more professional in their manifestations.

In the field of single-issue terrorism, the report notes an increase in environmental extremist activities in 2010. Single-issue terrorism is defined as violence committed with the desire to change a policy or practice within a target society. In Europe, the term is used to describe animal rights groups and environmental eco-terrorist groups. More than 200 single-issue extremism related incidents were recorded in the EU in 2010, including 24 arson attacks using improvised incendiary or explosive devices.

The content of the 2011 TE-SAT report is based on information supplied by EU Member States; several third States (notably Colombia, Croatia, Iceland, Norway, Switzerland, Turkey, and the US); Eurojust and Interpol, as well as open sources. (CR)

➤eucrim ID=1103017

Europol Back-Up Data Centre

On 26 July 2011, Europol and the Federal Republic of Austria signed an agreement whereby Austria will host Europol's back-up data centre in a government facility. Through the back-up data centre, Europol will be able to continue its critical IT-enabled services in the event that its primary data centre in The Hague were to become completely unavailable for a prolonged period of time. The agreement will last 10 years and can be extended further. The back-up data centre will become operational in 2012. (CR)

➤eucrim ID=1103018

EU First Response Network

To deal with the aftermath of the recent attacks in Norway through an integrated operational platform, Europol's Director Rob Wainwright invited the police chiefs of seven European countries – Norway, Denmark, Finland, Germany, Poland, Sweden, and the UK – to establish an EU First Response Network. This was announced by Europol on 27 July 2011. For this network, senior experts from these countries will be included in Europol's operations centre, a platform that provides:

- An international database of terrorist suspects and extremists;
- The ability to track terrorist financing;
- An operational platform to coordinate major international lines of enquiry.

The First Response Network will focus on pursuing a number of international leads and assessing the wider implications of the incidents in terms of the threat from right-wing extremism across Europe.

The idea to transform Europol's Counter Terrorism Task Force into an EU First Response Network was adopted in 2007 by the JHA Council. It has been on standby since then, tasked to organise the first response of Member States and Europol to major terrorist incidents. (CR)

➤eucrim ID=1103019

European Police Chiefs Convention

From 29 June until 1 July 2011, Europol hosted the European Police Chiefs Convention for the first time. The convention focused on the combating and prevention of serious organised crime and terrorism affecting Europe.

Concerning counter-terrorism, the convention identified the need for de-radicalisation and prevention of radicalisation in society. According to the convention, a more integrated approach involving all actors, such as police, justice officials, schools, and social services, should be aimed at. Furthermore, in order to create a genuine European law enforcement culture, criminal and intelligence databases should be further harmonised and interconnected and concrete best practices and training developed. A comprehensive strategy for security matters that encompasses all types of threats should be developed. The convention encourages setting up flexible private partnerships as well as a dialogue with vulnerable communities such as schools, etc. Administrative boundaries that currently exist between key agencies, e.g., Europol, SITCEN, Frontex, should be reduced. Furthermore, the convention recommends obligatory reporting of all terrorist events in the Member States to Europol, which should play a more intense role; some participants even saw the need to give executive powers to Europol.

Concerning the fight against organised crime, the convention recognised the need to break away from the traditional methods to embrace a more creative approach, e.g., serious crime prevention orders. Furthermore, asset recovery and financial investigation capabilities must be strengthened. Given the increasing globalisation of organised crime, the convention saw a mutual benefit in expanding EU law enforcement support and the promotion of intelligence-led investigation to countries and areas where criminal groups impact on Member States. Finally, the use of Internet services was seen as an opportunity

to help law enforcement work in partnership with EU citizens.

The convention was attended by almost 300 Chiefs of Police, senior law enforcement officers, academic experts, the European Commissioner for Home Affairs, Cecilia Malmström, and the Secretary General of Interpol, Ronald Noble. (CR)

➤eucrim ID=1103020

Conference on Violent Animal Rights Extremists

At the beginning of July 2011, Europol and Eurojust held a joint international conference in Europol's new headquarters in The Hague, the Netherlands, to discuss the issues behind the increased violence committed by extremists in the name of animal rights.

The growing violence of animal rights extremists is demonstrated, for instance, by the increased use of Improvised Explosive Devices (IEDs) and Improvised Incendiary Devices (IIDs). Further measures include threatening emails, warning phone calls, intimidating the targets' families, and committing physical assaults – even arson attacks on their property in so-called "home visits."

The fur and pharmaceutical industries have been actively targeted, for instance, animals being released and feeding/water installations destroyed. Another new trend is the closer collaboration between single-issued extremist groups and between these groups and other extremist groups.

Recommendations drawn from the conference include:

- Development of a renewed dialogue on animal protection and animal welfare at the EU level;
- Closer cooperation with the corporate security community and their branch organisations;
- Enhancement of information exchange with Europol and Eurojust on attacks in order to develop a common strategy and to identify best practices. (CR)

➤eucrim ID=1103021

Hit Against Currency Counterfeiters

Three suspects were arrested and more than 100,000 euros banknotes as well as around 120,000 counterfeited US dollars were seized in a joint police operation in Bulgaria on 2 June 2011. The operation was conducted by a Joint Investigation Team involving Bulgaria, Spain, the US Secret Service, Eurojust, and Europol. (CR)

➤eucrim ID=1103022

Eurojust

2010 Annual Report

Eurojust published its ninth annual report, reviewing its activities in the year 2010. Besides some general information on its activities and management, the report focuses mainly on Eurojust's operational activities, relations with EU partners, and further development.

As in previous years, the caseload at Eurojust increased with 1,424 newly registered cases, an increase of 4% compared to 2009. Approximately one fifth of these cases involved three or more countries. In 2010, Eurojust held 141 coordination meetings, which constitutes a 7% increase compared to 2009. Approximately two thirds of coordination meetings involved three or more countries.

Practical obstacles encountered in Eurojust's judicial cooperation casework include lack of resources and sometimes lack of adequate equipment at the national level for the timely execution of judicial cooperation requests. Legal obstacles derive from procedural differences, differences in the definition of criminal offences, problems arising from different rules on the admissibility of evidence, the practical use of relevant terms of the legal instruments, the reluctance of national authorities to use EU legal instruments, the lack of or insufficient implementation of European legislation, and a lack of training and trust. An early involvement of Eurojust and full implementation of the Eurojust Decision is seen as crucial to ensuring that the investigation resources yield results.

In 2010, almost 20% of all cases (280) registered at Eurojust concerned the execution of EAWs. Particular problems identified by Eurojust are missing or unclear information and requests for additional information, translation issues, trials in absentia, differences between legal systems, the principle of proportionality, the speciality rule, the return of nationals to serve sentence after surrender for trial, and the practical organisation of surrender of the suspect. The report also outlines the problems encountered with freezing orders, asset recoveries, and controlled deliveries.

Eurojust's operational priorities for 2010 included terrorism, drug trafficking, trafficking in human beings, fraud, corruption, cybercrime, money laundering, and other activities related to the effect of organised criminal groups on the economy.

Looking at terrorism, the report shows that the number of cases where Eurojust's assistance has been sought increased in 2010. The largest number of cases (254) registered at Eurojust in 2010 concerned drug trafficking. 6% of Eurojust's total casework (87 cases) concern trafficking in human beings, with 13 coordination meetings conducted in this regard. While the number of fraud-related crimes – including tax fraud, computer fraud, advanced fee fraud, misappropriation of corporate assets, and VAT fraud (198 cases, 14% of the total casework, 17 coordination meetings) – slightly decreased compared to the previous year, the number of corruption cases (31 cases, 11 coordination meetings) increased by 55% compared to the previous year. For the phenomenon of cybercrime, Eurojust registered 32 cases in 2010. However, the report sees an element of underreporting in these figures claiming that, since national authorities' concentrate on the results of cybercrime (fraud, pornography, etc.), the methods by which the crimes were committed had not always been central to recording

practice. Concerning money laundering, the number of cases increased again to a total of 146 cases (125 cases in 2009). Money laundering figured in 26 coordination meetings, nine of them including Europol's involvement.

With regard to JITs, Eurojust's National Members participated in 20 JITs and Eurojust received 11 notifications from Member States regarding the setting-up of JITs. In December 2010, Eurojust and Europol jointly organised the sixth annual meeting of the network of national experts on JITs at Europol (see eucrim 1/2011, p. 15). Furthermore, Eurojust continued to support JITs in 2010 by providing financial and logistical assistance (see eucrim 4/2010, p. 133).

As regards Eurojust's casework involving third States, a study that was started on 1 September 2008 and completed on 31 August 2010 showed that the most frequently requested third States were Switzerland, the US, Norway, Croatia, the Russian Federation, Turkey, Albania, and Ukraine. Cases mainly concerned drug trafficking, swindling and fraud, money laundering, participation in a criminal organisation, and smuggling of human beings. Cases registered with Eurojust by its liaison officers from third States include 50 registered cases from the Liaison Prosecutor from Norway, 11 cases from the Liaison Prosecutor from Croatia, and three cases from the Liaison Prosecutor from the US.

With respect to Eurojust's cooperation with states and bodies inside and outside the EU, 2010 saw the signature of a Memorandum of Understanding between Eurojust and the United Nations Office on Drugs and Crime. Brazil, Cape Verde, India, and Kazakhstan were added to Eurojust's network of contact points in third States, an agreement on cooperation between Eurojust and the Former Yugoslav Republic of Macedonia entered into force, and negotiations for cooperation agreements with the Russian Federation, Ukraine, and Liechtenstein were reconfirmed as priorities. Turkey was added to the priority list for the negotiation of co-operation agreements.

As in previous years, relations with the EJN were strengthened by, for example, establishing a Joint Task Force consisting of representatives from Eurojust, the EJN, and its Secretariat in order to find practical ways to strengthen cooperation between them. Cooperation with Europol was further fostered through, for instance, the entry-into-force of the revised Co-operation Agreement, Eurojust's association with three more Europol Analytical Work files (AWFs), Europol's participation in Eurojust's coordination meetings, and Eurojust's contribution to the TE-SAT and the European Union Organized Crime Threat Assessment (OCTA). Regular contacts were also maintained with OLAF through the mutual referral of cases, regular liaison meetings, and a study visit within the framework of the Eurojust-OLAF Exchange Programme. Contacts with Frontex were intensified through a meeting of the President of Eurojust, Aled Williams, and the Director of Frontex Ilkka Laitinen. Further cooperation included training programmes with the European Judicial Training Network (EJTN) and the European Police College (CEPOL) that were established through a Memorandum of Understanding.

Eurojust's budget in 2010 was €30,2 million. Eurojust executed 98% of its commitment appropriations budget.

Achievements with regard to administrative issues included the first Multi-Annual Strategic Plan (MASP) covering the years 2012-2014 and establishing four strategic goals (improving operational work, becoming a centre for effective judicial action against cross-border crime, improving relationships with key partners, and achieving further efficiency in working methods). The Host State,

Report

European Arrest Warrant and Surrender Procedures between Germany and Poland

On 9-10 June 2011, a conference on the European Arrest Warrant and the surrender procedures between Germany and Poland took place in Collegium Polonicum – a cross-border, academic institution run by the European University Viadrina in Frankfurt (Oder) and the Adam Mickiewicz University (Poznan).

This international (German-Polish) conference was organised by Professor Maciej Małolepszy (Chair for Polish Criminal Law at the European University Viadrina) with support from Prof. Dr h.c. Andrzej J. Szwarc (Adam Mickiewicz University) and Prof. Dr Gudrun Hochmayr, Prof. Dr Jan C. Joerden, and Prof. Dr Uwe Scheffler (European University Viadrina).

The conference was attended by 30 Polish and German judges, prosecutors, and criminal defence lawyers involved in the surrender procedures between Germany and Poland. The idea was to bring together representatives of different judicial institutions with different perspectives and views in order to discuss problems regarding present cooperation in criminal matters. In their presentations, some of the difficulties highlighted were a "starting point" for discussions and offered the opportunity to clear reoccurring obstacles and improve the cooperation between Germany and Poland.

The problems identified concerned the question of proportionality in the issuing of Arrest Warrants, the need to provide better standards for the defence, or the excessive use of arrest. Some controversy arose as to the criteria under which the defendant has the best possibilities for reintegration into society. The latter topic was discussed in the context of the obligation to return Polish nationals in order to serve in Poland their custodial sentence or the detention order passed against them in Germany. When reasons indicate better chances for resocialisation, the sentence could be executed in Germany (despite the obligation to return).

Dr. Paweł Nalewajko, European University Viadrina, Frankfurt (Oder)

the Netherlands, offered to finance and construct a new building for Eurojust by the end of 2015.

Further developments included the establishment of an On-Call Coordination system (see the news in the following column) and the Secretariats of the Networks for JITs and for Genocide and related crimes.

Finally, Eurojust held a strategic seminar on the future of Eurojust under the Lisbon Treaty (see eucrim 2/2011, pp. 55-56) in September 2010.

The final chapter of the report deals with the follow-up of Council conclusions to Eurojust's Annual Report of 2009. (CR)

➤eucrim ID=1103023

Eurojust 2010 Annual Report: Council Conclusions

Eurojust's 2010 Annual Report was welcomed by the JHA Council at its meeting from 9-10 June 2011. While the Council appreciated that most of the objectives for 2010 had been achieved, it reiterated its observation that Eurojust should focus further on providing assistance to complex cases that require coordination, while simple bilateral cases should generally be referred to the contact points of the EJN.

Hence, the Council requests that Eurojust further elaborate and implement mechanisms aiming at enhancing cooperation with the EJN. Member States are urged to implement the new Council Decision 2009/426/JHA on the strengthening of Eurojust. They are also invited to promote, among their judicial authorities, information about the possibilities offered by the Decision and, in particular, the Eurojust National Coordination System (ENCS). Furthermore, noting the obstacles pointed out in the report with regard to judicial cooperation, the Council urges the Member States to further enhance assistance to its competent authorities, also in respect of training and resources.

The Council noted that the report missed information on the implementation of the new Eurojust Decision in certain respects such as cooperation with the EJN, its new rules of procedure, and its readiness to receive information and give feedback to national authorities. Hence, the Council invited Eurojust to report on these issues in its next annual report. (CR)

➤eucrim ID=1103024

Eurojust On-Call Coordination Service Available

On 4 June 2011, Eurojust's new On-Call Coordination (OCC) service became available. The OCC service allows national authorities to request Eurojust's assistance in urgent cases by contacting their representatives on a 24/7 basis. When calling the OCC, the caller is greeted in the language of his/her Member State and then forwarded to the national OCC representative on duty. In case the country of origin of the call cannot be established automatically or that the call is made from outside the EU, recorded messages in English allow the caller to connect to an OCC representative. Despite the possibility to leave messages, conversations between the caller and the representative are not recorded.

Notification of the available telephone numbers has been restricted to judges, prosecutors, and law enforcement officials in the Member States. (CR)

➤eucrim ID=1103025

Eurojust Newsletter: 4th Issue

Eurojust has published the fourth issue of its newsletter, this time dedicated to the fight against financial and economic fraud. Besides a general overview and case examples of Eurojust's work in the area of financial and economic fraud and its relation with OLAF in this regard, the newsletter contains an interview with the Head of the Central Fraud Group within the Crown Prosecution Service, Matthew Wagstaff, and with the Senior Financial Crime Investigator of Europol's Criminal Finances & Technology Unit, Rafaël Rondelez.

In 2010, 14% of Eurojust's total casework dealt with fraud-related cases (229 cases). Eurojust also runs a Financial and Economic Crimes (FEC) Team, which is chaired by the Finnish National Member for Finland, Ritva Sahavirta. (CR)

➤eucrim ID=1103026

European Judicial Network

Revised EJN Website Launched

On 27 May 2011, the EJN launched its new website. Besides its new look, the website includes new functionalities and tools, especially on the practical application of EU mutual recognition and mutual legal assistance instruments. It also contains a comprehensive library including all relevant legal instruments, forms, handbooks, case law, reports, etc. in the field of judicial cooperation in criminal matters in the EU. Ultimately, one of the achievements of the revised website is its greater user-friendliness and easier navigation. (CR)

➤eucrim ID=1103027

Frontex

New Frontex Regulation: Political Agreement

On 23 June 2011, the Council and the EP reached political agreement on the draft regulation amending the Frontex Regulation (see eucrim 1/2010, pp. 9-10; eucrim 1/2011, p. 6; and eucrim 2/2011, p. 56). Under the political agreement, the main changes to Frontex operational capabilities will encompass the following:

- The possibility for Frontex to buy or lease its own equipment or to buy such equipment in co-ownership with a Member State;
- A mechanism for Member States to second national border guards and make available equipment to Frontex;
- Registration of equipment put at the

disposal of Frontex in a centralised record of a Technical Equipment Pool (TEP);
- More provisions in the operational plan regarding, e.g., tasks and responsibilities, the composition of the teams, and the applicable jurisdiction;
- Strengthening of provisions for the protection of fundamental rights, including the establishment of a Consultative Forum on Fundamental Rights and the designation of a Fundamental Rights Officer;
- Specific provisions for the protection of personal data, including the possibility to transfer personal data to Europol or other EU law enforcement agencies on persons suspected of involvement in cross-border crime, the facilitation of illegal immigration, or human trafficking.
- Strengthening of coordinating role for Frontex as regards joint return operations, with full respect for fundamental rights;
- The possibility for Frontex to launch technical assistance projects and deploy liaison officers in third countries.

The text still requires formal approval in European Parliament and then in the Council. (CR)
➤eucrim ID=1103028

Study on Ethics in Border Security

Frontex published its study on the Ethics of Border Security on 29 April 2011. The study shall provide border guards with an overview of the ethical issues that can arise from their work and a guide to the ethical principles to help manage and resolve these issues.

The study is divided into three parts: The first part is a survey and analysis of codes of conduct currently used by border agencies in EU countries to identify the main areas of overlap as well as gaps between the national codes of conduct and the Schengen Code and Handbook. The second part addresses these gaps by providing a comprehensive overview of the main ethical principles that relate to border guard practice, giving examples of good practice. The third part provides an overview of the ethical issues arising from the use of detection and identification technologies by border guards.

The study was carried out by the Centre for Global Ethics of the University of Birmingham (UK). (CR)
➤eucrim ID=1103029

Specific Areas of Crime / Substantive Criminal Law

Fraud

Commission Proposes New Anti-Fraud Strategy

On 24 June 2011, the Commission adopted a Communication (COM(2011) 376 final) to improve and modernise its Anti-Fraud Strategy. The last Commission Anti-Fraud Strategy was adopted in 2000 (COM(2000)358 final), and its goals were implemented by the 2001-2003 and the 2004-2005 Action Plans (COM(2001)254 final and COM(2004)544 final).

The new policy paper covers fraud prevention and detection, cooperation between OLAF and Commission Services, recovery of misused funds, and penalties. The Commission plans to increasingly involve OLAF in the process of developing and implementing sectoral anti-fraud strategies. Currently, there is only an exchange of best practices between OLAF and certain Commission services managing EU funds. The Commission plans to extend this information exchange to all Commission services. OLAF shall organise a Fraud Prevention and Detection Group, which will emerge from the Inter-service group of Fraud Proofing Correspondents. This network is intended to serve as a centre of expertise and to disseminate best practices and fraud risk assessments. As regards investigations, the Commission expects the reform of OLAF (COM(2011) 135) to help increase efficiency in both the conduct of the investigations and the information exchange between OLAF and other authorities.

Furthermore, the Communication contains, *inter alia*, measures to give more guidance and protection to whistleblowers and informants and ways to better monitor the recovery of funds wrongly paid.

The measures proposed in the Anti-Fraud Strategy are expected to enter into force by 2014.

Alongside the new Anti-Fraud Strategy, the Commission presented the new Action Plan to fight the smuggling of cigarettes and alcohol along the EU Eastern border (SEC(2011) 791 final). The plan identifies short-term and medium-term actions to be carried out with the help of the Member States as well as Russia and the Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine). The proposed actions include setting up trained mobile units and new equipment along the border (e.g., automated recognition tools, scanners, night vision devices), reviewing the application of penalties in the respective Member States, and enhancing international cooperation and information exchange. (ST)
➤eucrim ID=1103030

Protecting the EU's Financial Interests

On 26 May 2011, the Commission adopted a Communication on new measures to enable prosecutors and judges to fight crime detrimental to the EU's financial interests more effectively. *Inter alia*, the Commission plans to clarify definitions of crime (e.g., "embezzlement" or "abuse of power") and to raise both OLAF and Eurojust's capacities to carry out their investigations more effectively. The paper discusses the possibility of setting up a specialised European Public Prosecutor's Office to focus on the application of common rules on fraud and other offenses involving EU funds. A key element of the policy paper is the enhancement of ways to exchange information between customs, tax authorities, judiciary authorities, and other

competent authorities. Therefore, the Commission plans to prepare a proposal on mutual administrative assistance for the protection of the EU's financial interests. (ST)
➤eucrim ID=1103031

Corruption

Commission Presents Plans for EU Anti-Corruption Report

On 6 June 2011, the Commission presented a Communication on fighting corruption in the EU.

The Commission will set up a new mechanism to monitor and assess anti-corruption efforts taken in the Member States: the EU Anti-Corruption Report. The Report will include a research-based section on specific aspects of the fight against corruption in the EU, country analyses, including recommendations for each Member State, and a section on current trends at the EU level. In drawing up the report, the Commission intends to make greater use of existing monitoring instruments, e.g., the OECD or GRECO, and will therefore request the authorisation of the Council to negotiate EU participation in GRECO with the Council of Europe. The EU Anti-Corruption Report will be issued by the Commission every two years, starting in 2013.

Seeing that many existing anti-corruption legal instruments at the EU and international levels (e.g., the CoE Criminal Law Convention on Corruption or the OECD Anti-Bribery Convention) have not yet been ratified and transposed by all Member States, the Commission plans to put more emphasis on monitoring the ratification and transposition procedures in the Member States. According to the Communication, there is also a need to focus on corruption in the areas of judicial and police cooperation and to improve private-public dialogue on how to prevent corruption within the business sector. (ST)
➤eucrim ID=1103032

Counterfeiting & Piracy

Annual Report on EU Customs Enforcement of Intellectual Property Rights

On 14 July 2011, the Commission published the annual report on EU Customs Enforcement of Intellectual Property Rights (IPR). In 2010, the number of shipments suspected of violating IPR went up by almost 50% compared to 2009, increasing from 43,500 cases in 2009 to almost 80,000 cases in 2010. More than 103 million products were detained at the EU external border. Cigarettes accounted for 34%, followed by office stationary, tobacco products, labels, clothing, and toys. The report estimates the value of the equivalent genuine products at over €1 billion. (ST)
➤eucrim ID=1103033

Success for Major Joint Customs Operation

On 27 June 2011, the Commission released information on a large joint customs operation ("Fireblade"), which led to the confiscation of more than 28,000 items of counterfeit products. The joint action was organised by the Hungarian National Tax and Customs Administration in cooperation with both OLAF and Europol. It targeted counterfeit clothing and accessories entering the EU by road via the Eastern EU border. All Member States were invited to participate in the operation. The counterfeit products seized during the operation represent approximately €1 million in terms of the market value of counterfeit goods and an additional €1.5 million in terms of evaded duties and taxes on smuggled cigarettes. (ST)
➤eucrim ID=1103034

New Directive on Counterfeit Medicine

On 27 May 2011, the Council adopted a Directive amending Directive 2001/83/EC relating to medicinal products for human use, as regards the prevention of entry into the legal supply chain of falsified medicinal products. The EP had adopted the agreed text in its plenary vote on 16 February 2011.

The new Directive includes provisions to fight falsified medicinal products:

- Medicinal products subject to prescription must be identifiable throughout the supply chain and must have safety features that provide sufficient protection against tampering. So far, this provision does not include non-prescription medicines.
- Importers, manufacturers, and distributors of active substances will have to be registered with the respective authorities.
- Manufacturers will be obligated to inform competent authorities about medicinal products they suspect of being falsified.
- Member States will have to ensure that all falsified or otherwise dangerous medicine can be recalled.
- Member States will have to set up a website listing all persons or bodies in that Member State that are authorised to offer medicinal products for sale via the Internet. Websites offering medicines must be linked to this website.

The new Directive must be transposed into national law within 18 months starting from the date of publication in the Official Journal. (ST)
➤eucrim ID=1103035

Organised Crime

Council Announces Priorities in Fight Against Organised Crime

At the JHA meeting from 9-10 June 2011, the Council adopted conclusions on the fight against organised crime from 2011-2013. In its conclusions, the Council lists its main priorities, which include, e.g.:

- Focusing on the role of the Western Balkans as a logistical centre for organised criminal groups;
- Reducing the production and distribution of synthetic drugs in the EU (see this issue of eucrim, p. 105);

■ Combating all forms of trafficking in human beings by targeting the organised criminal groups conducting such criminal activities;
■ Disrupting the trafficking of illegal goods to the EU. (ST)
➤eucrim ID=1103036

Council Discusses Counter-Terrorism Policies

At the JHA meeting from 9-10 June 2011, the Council discussed a paper on the implementation of the EU Counter-Terrorism Strategy, presented by the EU Counter-Terrorism Coordinator. The paper analyses the consequences of recent developments that influence the fight against terrorism, such as Osama Bin Laden's death or the reforms in several Arab countries.

The paper then gives recommendations for improving the EU Counter-Terrorism Strategy, e.g., how to improve prevention tools, increase transport security, and move towards the implementation of the strategy on chemical, biological, radiological, and nuclear security (CBRN). (ST)
➤eucrim ID=1103037

The Council also adopted conclusions on enhancing the links between internal and external aspects of counter-terrorism. In the conclusions, the Council calls for closer cooperation between the respective authorities in the field of EU security and for tangible results on counter-terrorism capacity building efforts focused on countries and regions that are of priority to the EU.

Member States, the Commission, and the High Representative assisted by the EEAS are asked to ensure consistency in the EU's internal and external priorities in the fight against terrorism. The High Representative is invited to assist in the conduct and further development of EU counter-terrorism activities as part of the political dialogue with third countries and international organisations. The Counter-Terrorism Coordinator shall contribute to ensuring the implementation and evaluation of the EU Counter-Terrorism Strategy and regularly present policy recommendations to the Council. (ST)
➤eucrim ID=1103038

Consensus on Stricter Rules to Combat Illegal Trafficking in Firearms

On 29 June 2011, the Council, the EP, and the Commission reached political consensus on a new Regulation implementing Art. 10 of the UNs' Firearms Protocol and establishing export authorisation and import/transit measures for firearms, their parts, components, and ammunition (COM (2010) 273). The Regulation will improve the tracing and control of imports and exports of civilian firearms from and to the EU territory. The ratification of Art. 10 of the UN Firearms Protocol has been pending since 2002. The EP and the Council are expected to soon vote on the proposed regulation. (ST)
➤eucrim ID=1103039

Fighting New Synthetic Drugs

On 11 July 2011, the Commission published a report on the danger of new synthetic drugs entering the EU market. In 2010, 41 new psychoactive substances, which imitate the effects of illegal drugs such as ecstasy and cocaine, were identified. So far, these substances are sold legally, although they may be toxic, addictive, and have long-term adverse effects. They include plant-based substances, synthetic derivatives of established drugs, and so-called "designer drugs."

The report concludes that there are no mechanisms in place to effectively keep up with the large numbers of new substances entering the market. Therefore, there is an urgent need to re-evaluate the current system of monitoring substances that pose serious health risks. The Commission intends to present plans to fight these substances later in 2011. (ST)
➤eucrim ID=1103040

Fighting Drug-Related Crime

At the G8 ministerial meeting on 10 May 2011, the Commission provided an overview of current initiatives to combat drug-related crime:

■ The new European border surveillance system (EUROSUR) will improve border intelligence through the use of new technologies such as satellite imagery;
■ Within the Maritime Analysis and Operation Centre-Narcotics (MAOC-N) or the information exchange platforms in Dakar and Accra, the EU is working together with third countries to fight the smuggling of drugs into the EU along major trafficking routes;
■ The Commission plans to propose new legislation on asset recovery by the end of 2011. (ST)
➤eucrim ID=1103041

Trafficking in Endangered Species

On 20 May 2011, Europol presented a study, which concludes that many organised criminal groups are illegally trading in endangered species of wild fauna and flora. Criminal organisations use the same routes as those used for illegal immigration and drug trafficking. Europe is a key market for exotic animals, which are often trafficked as eggs and hatchlings. Unfortunately, over 90% of specimens being trafficked do not survive the capture and transportation phase. Still, trafficking in endangered species is a lucrative business, with revenues estimated to be over €4 billion per year. Europol has forwarded its findings to Interpol's Environmental Crime Programme, which assists Interpol's Member Countries in the effective enforcement of national and international environmental laws and treaties. (ST)
➤eucrim ID=1103042

2011 OCTA Report

On 4 May 2011, Europol published its 2011 EU Organised Crime Threat Assessment (OCTA) report. The report assesses current trends in organised crime and describes emerging threats in this area. One of the report's key findings is that organised crime is becoming more diverse in its methods, group structures, and impact on society. There is greater collaboration between criminal groups

and a higher level of mobility and use of the Internet. The report finds that criminal groups are becoming more and more "poly-criminal," meaning that they engage in many different criminal fields, including new areas with lower levels of perceived risk involved (e.g., carbon credit fraud, payment card fraud, and commodity counterfeiting). According to the report, the global economic crisis brings EU citizens closer to organised crime. For example, there is higher tolerance for counterfeit goods, and more citizens are recruited by criminal groups, e.g., for cannabis cultivation or as drug couriers.

Geographically, the report identifies five key hubs for organised criminal activities:

- The North West hub being the most important coordination centre for drug distribution;
- The North East hub as a major transit route for the transit of illegal commodities;
- The South West hub as a transit zone for cocaine, cannabis, and victims of trafficking in human beings;
- The Southern hub as a major centre for all kinds of criminal activities, ranging from the transit of counterfeit currency and commodities to the transit of victims of trafficking in human beings and illegal immigrants.
- The report puts a special focus on the South East hub, which has seen the greatest expansion of all hubs in recent years. There has been a significant increase in trafficking via the Black Sea and many Balkan routes as well as more illegal immigrants entering the EU through Greece. The report also highlights the fact that criminal groups are exploiting opportunities in the possible accession of Bulgaria and Romania to the Schengen zone. (see this issue of eucrim, p. 96) If Bulgaria and Romania join the Schengen area, the role of the Western Balkans as a logistical hub may increase and more illicit traffic via these countries can be expected. (ST)

➤eucrim ID=1103043

Cybercrime

General Approach on Attacks Against Information Systems

During the JHA Meeting on 9-10 June 2011, the Council reached a general approach on the compromise text of the draft Directive on attacks against information systems, proposed by the Commission in September 2010 (see eucrim 4/2010 p. 136). This text will form the basis for upcoming discussions with the EP. The general approach outlines the level of penalties and the scope of punishable acts as discussed during previous Council sessions (see eucrim 4/2010 p. 135 and eucrim 2/2011 p. 59). The UK and Ireland used their opt-in right in accordance with Art. 3 (1) of Protocol No. 21 to the Treaties and expressed their wish to participate in the adoption and application of the Directive. The future instrument will not apply to Denmark. Greece and Spain have reservations concerning the proposed level of penalties. (NK)

➤eucrim ID=1103044

EU Establishes Computer Emergency Response Pre-configuration Team

After cyber attacks on the French Finance Ministry, the EU Emissions Trading System, and on EU institutions (see eucrim 2/2011 p. 60), the EU established its own Computer Emergency Response pre-configuration Team (CERT) in June, based on the recommendations of cyber security experts known as the *"Rat der IT Weisen"* (a council of experienced IT specialists).

The CERT consists of ten Internet security experts from several EU institutions, including the European Commission, the EP, the Council, the Committee of the Regions, and the Economic and Social Committee as well as ENISA. The team will work closely with other CERT units in the Member States that are to be set up by 2012. It will assist in the exchange of information on threats and ways to tackle them in real time.

An inter-institutional Steering Board will oversee the operation of the EU CERT, and an assessment will follow after one year of preparatory work by the team. This will provide the basis for determining the conditions under which a full-scale EU CERT can be established.

The establishment of the CERT is an important step forward in the fight against cyber attacks. It also reinforces the EU Information Security Policy to which the Commission dedicated itself with the adoption of the Digital Agenda for Europe in May 2010. In light of this goal, the Council also reiterated the importance of developing national CERTs and the organisation of national and pan-European cyber exercises (see eucrim 1/2011, p. 10) in its conclusions on Critical Information Infrastructure Protection in May. (NK)

➤eucrim ID=1103045

Environmental Crime

Council Sets Up EnviCrimNet

At the JHA meeting from 9-10 June 2011, the Council adopted a Resolution on the creation of an informal network to counter environmental crime (EnviCrimeNet). The new Resolution aims to facilitate the identification of criminal networks in this field by improving the exchange of information and the gathering of criminal intelligence between the respective authorities. The new network will be supported by Europol, and the Netherlands will act as its first rotating secretariat. (ST)

➤eucrim ID=1103046

Member States Face Court Proceedings over Breach of EU Environmental Legislation

The Commission is taking several Member States to the ECJ for not complying with EU environmental legislation despite having received warnings from the Commission.

- The Commission is referring the Czech Republic to the ECJ over its fail-

ure to meet the European requirements on biocidal products as set out by Directive 2010/5/EU. Despite having received several warnings on the matter, the Czech Republic has not added acrolein, a substance used in certain biocidal products, to its national list of active substances that are covered by biocides legislation.

➤eucrim ID=1103047

■ Although the ECJ already ruled on the matter one and a half years ago, Ireland has still not adopted the necessary measures to ensure that septic tanks are subjected to adequate checks and inspections. According to the EU Waste Framework Directive (2008/98/EC), domestic waste water involving septic tanks or other individual waste water must be recovered or disposed of without endangering human health or the environment. The Commission has now referred the matter to the ECJ and asks the Court to impose a lump-sum fine of €2,7 million and a daily penalty payment of €26.173.

➤eucrim ID=1103048

■ The Commission is also taking Ireland to Court for allowing industrial installations to operate with outdated permits. The Integrated Pollution Prevention and Control (IPPC) Directive required Member States to issue new permits or revise existing permits by 30 October 2007 for all industrial installations that were in operation before 30 October 1999. However, the permits of at least 17 Irish livestock installations have not yet been reconsidered or updated. The Commission is therefore referring the case to the ECJ. The Commission has previously taken 10 Member States to Court for infringements of the IPPC Directive (see eucrim 2/2011, p. 61).

➤eucrim ID=1103049

■ Since France has so far failed to effectively tackle excess emissions of airborne particles known as PM10 in several zones across the country, the Commission has decided to refer the matter to the ECJ. Directive 2008/50/EC on ambient air quality and cleaner air for Europe requires Member States to limit the exposure of citizens to these particles.

➤eucrim ID=1103050

■ Spain faces proceedings before the ECJ for failing to ensure that waste water is being treated according to the Urban Wastewater Treatment Directive (91/271/EEC) and for failing to submit its plans for managing river basins as required by the EU Water Framework Directive (2000/60/EC). The Commission decided to refer both cases to the ECJ. (ST)

➤eucrim ID=1103051

EU-Liberia Agreement on Illegal Timber Imports

On 9 May 2011, the EU and Liberia signed a Voluntary Partnership Agreement (VPA), which aims to ensure the legal origin of imported wood products to the EU. From 2014 on, all shipments of wood products from Liberia to the EU will be required to carry a license certifying their legal origin. Liberia intends to set up stronger control systems to closely monitor all wood products destined for the EU market, whereas the EU has agreed to guarantee unrestricted access to its market for all wood products coming from Liberia. The EU has already signed similar agreements with many timber producing countries, such as Cameroon and the Republic of Congo (see eucrim 2/2010, p. 47 and 4/2010, p. 36). (ST)

➤eucrim ID=1103052

Sexual Violence

Fighting the Sexual Exploitation of Children: Agreement Reached

On 30 June 2011, the Council and the Parliament reached a political agreement on a new Directive aimed at combating the sexual abuse and exploitation of children as well as child pornography (see eucrim 1/2011, p. 13 and eucrim 1/2010, p. 12). Once adopted, the Directive will harmonise many criminal offences and introduce a high level of penalties for the respective offences. Regarding the sexual abuse of children, the Directive foresees maximum penalties ranging from at least one year of imprisonment (for causing a child to witness sexual activities) to at least 10 years of prison (for coercing a child into sexual actions). The minimum sentence for forcing a child into child prostitu-

ENISA

6th Computer Emergency Response Team (CERT) Workshop

Prague, Czech Republic, 3-4 October 2011

This annual workshop will again focus on current topics that are relevant for national/governmental CERTs and law enforcement authorities. It will address network and information security (NIS) aspects of cybercrime.

Within Europe, ENISA is in a unique position to break barriers that impede cooperation between various communities. For this reason, the agency is organising its traditional workshop jointly with Europol this year. The event is also being supported by the national Computer Emergency Response Team in the Czech Republic (CSIRT.CZ).

Given the importance of cybercrime and relevant NIS issues in the Communication of the European Commission (COM(2010)245), the participants will focus on and address specific tasks in order to enhance this cooperation in practice.

Workshop attendance is on an invitation-only basis.

For further information, please contact Jo De Muynck, Phone +30 2810 391283 or cert-relations@enisa.europa.eu.
http://www.enisa.europa.eu/act/cert/events/6th-workshop-cybercrime

EU Defence Rights

London, United Kingdom,
21 October 2011

This conference is being organised by the Institute of Advanced Legal Studies, University of Birmingham, European Criminal Law Association (UK), Fair Trials International and Justice.
The topics will focus on defence rights in the EU and include the following:

- Challenges facing the defence and the legitimacy of criminal justice within the EU;
- The roadmap on procedural safeguards: progress so far;
- Case studies – the European Arrest Warrant and defence rights.

The proceeds will be published in 2012 by the European Criminal Law Review (EuCLR) in Sweden.

Admission is free. Those wishing to attend must register in advance via e-mail at IALS.Events@sas.ac.uk
www.sas.ac.uk/events/view/9932

tion will be 10 years of imprisonment, and the possessing of child pornography must be punished with at least one year of imprisonment. If the production of child pornography or child abuse were preceded by an online invitation to the child ("grooming"), the maximum sentence is aggravated (at least one year higher than otherwise).

The new Directive will oblige Member States to ensure that websites containing child pornography can be removed promptly. Member States may also block access to such websites, but must follow transparent procedures when making use of this possibility (see also eucrim 2/2011, pp. 61-62).

Furthermore, the Directive aims at tackling sex tourism more effectively and introduces compulsory jurisdiction over nationals who commit crimes outside of EU territory.

The Parliament is expected to vote on the Directive in September, and the Council is to formally adopt it shortly after. (ST)

➤eucrim ID=1103053

Procedural Criminal Law

Procedural Safeguards

Proposal on Right of Access to a Lawyer and Right to Communicate upon Arrest

On 8 June 2011, Vice-President and Commissioner for Justice Viviane Reding presented a new proposal for a Directive on the right of access to a lawyer in criminal proceedings and on the rights to communicate upon arrest (COM(2011) 326 final).

This draft Directive is the third step in the so-called Roadmap on procedural rights of 30 November 2009 (see eucrim 4/2009, p. 134), guaranteeing minimum rights to a fair trial in every Member State. The two previously presented instruments are the proposed Directive on the right to information in criminal proceedings (see eucrim 2/2011, p. 62 and eucrim 1/2011, p. 13) and the adopted Directive on the right to interpretation and translation in criminal proceedings (see eucrim 4/2010, pp. 138-139 and eucrim 1/2010, pp. 14-15).

Common minimum standards are needed, since a person suspected of a criminal act has a right to defence in every Member State, but the conditions under which a lawyer can be consulted are different. Similarly, differences exist between the Member States with regard to notifying the suspect's family.

Thus, minimum standards in the proposed Directive include the right to access to a lawyer as soon as possible and throughout the proceedings as well as the right to have confidential meetings with the lawyer. The lawyer should be allowed to play an active role during interrogations and to check detention conditions. A suspected person who is deprived of his liberty should be able to inform at least one relative or employer of his arrest or custody. Foreign suspects should be allowed to contact their embassy or consulate. Additionally, persons subjected to an EAW should be able to obtain legal counsel in both the Member State where the EAW was issued and the Member State where it was executed.

These rights and the provisions governing them in the proposed Directive correspond to the case law of the ECtHR and the interpretations it has given to the right to fair trial. In the next stage, the proposed Directive will be discussed by the EP. (EDB)

➤eucrim ID=1103054

Commission Presents Green Paper on Detention

After being invited by the Council, on 14 June 2011, the Commission presented a green paper on the application of EU criminal justice legislation in the field of detention (COM(2011) 327 final).

Green papers are questionnaires that trigger a public consultation on a certain topic and are followed by a white paper that sets out the policy lines to follow in the legislative proposal to be drafted.

With this green paper, the Commission wishes to learn more about the interplay between detention conditions, on the one hand, and mutual recognition instruments, e.g., the EAW and pre-trial detention, on the other. In order for mutual recognition instruments for detention conditions to function properly, a basic mutual trust between Member States' judicial authorities should be in place. Since detention conditions vary between the Member States, the Framework Decisions on the EAW, the transfer of prisoners, mutual recognition of alternative sanctions and probation, and the European Supervision Order are all potentially affected by a lack of mutual trust. Thus, the Commission has drawn up a list of ten questions for judges, practitioners, NGOs, government bodies, and academics to answer.

This green paper on detention conditions and mutual recognition stems from the Roadmap on procedural rights (see eucrim 4/2009, p. 134). The public consultation runs from 14 June 2011 to 30 November 2011. (EDB)

➤eucrim ID=1103055

Data Protection

Options for a European Terrorist Finance Tracking System

On 13 July 2011, the Commission presented a communication listing available options for a European Terrorist Finance Tracking System (COM(2011) 429 final).

The EU-US Agreement on the processing and transfer of financial messaging data for the purposes of the terrorist finance tracking program entered into force on 1 August 2010 (see eucrim 2/2011, pp. 63-64 and eucrim 2/2010, pp. 49-50). The Council invited the Commission to create the legal and technical framework for the extraction of data on EU territory and develop an EU version of the American terrorist finance tracking program within one year after this date. This objective was also explicitly mentioned in Art. 11 of that Agreement.

The aim of the new system is to ensure that the processing of data on money transfers takes place in accordance with EU data protection legislation and principles. It should also be in accordance with the EU Charter of Fundamental Rights.

The data will be extracted from the databases held by the so-called designated provider. This term currently refers to the Belgian based company SWIFT (Society for Worldwide Interbank Financial Telecommunication) that handles data on the majority of money transfers worldwide. However, it is not inconceivable that other designated providers may be appointed in the future.

The communication of 13 July 2011 describes the different steps the Commission has taken towards establishing such a legal and technical framework, and it presents several options for achieving this goal without indicating a preferred option. A European Terrorist Finance Tracking System (TFTS) must provide an effective contribution to the fight against terrorism and its financing within the EU. Additionally, the amount of personal data transferred to third states must be limited. In other words, the necessity and the proportionality principles must both be complied with, and this applies to requests for raw data as well as any searches performed on the requested data.

The Commission introduced three alternative approaches. They are all hybrid options because the two ends of the spectrum of possibilities – a purely national solution or a centralised EU approach – were not supported by the stakeholders consulted before this Communication was drafted. The three options presented by the Commission are the following:

- A central EU TFTS coordination and analytical service would be responsible for issuing requests for raw data (in cooperation with national authorities) to the designated provider and verifying them. Running the searches, analysing the search results, and forwarding reports to those who requested them would also be centralised in this service. In order to comply with the necessity principle and demonstrate the nexus of the request, the competent national authorities would have to share information with the central TFTS service, or they would have to pre-authorise the requests so that no further verification is needed. In case the US or other third states wish to issue a request, they would have to follow a similar procedure;
- An EU TFTS extraction service would be responsible for issuing and verifying requests for data and the requests for searches as well as running the searches. However, it would not be responsible for analysing the search results. This task would be reserved for the national authorities. Only searches conducted on behalf of third states or EU institutions could be analysed by the TFTS extraction service;
- A Financial Intelligence Unit (FIU) coordination service would be responsible for collecting the needs of all FIUs of the Member States and composing a request for data. This request would also be verified and authorised at this central level. Nonetheless, each FIU would be responsible for running searches and managing the search results on behalf of its Member State as well as for carrying out analyses and forwarding reports to those it considers relevant. Only when EU institutions or third states request searches would the FIU coordination service be responsible for conducting searches and analysing the results. Verification of the searches would be done at the national level or EU level.

The options describe above are not necessarily limitative and are currently being examined by the Commission as part of the ongoing impact assessment. As the possible establishment of an EU TFTS could have significant consequences for the content of the EU-US Agreement on the processing and transfer of financial messaging data for the purposes of the terrorist finance tracking program, the potential amendment of this Agreement should also be an element of future discussions. The Commission considers it necessary to reserve sufficient time to debate the three options and the decisions that need to be made in view of data protection and the aforementioned EU-US Agreement, both in the Council and in the EP. (EDB)

➤eucrim ID=1103056

Insufficient Adherence to the Safer Social Networking Principles for the EU

In June 2011, the European Commission published the results of a second independent assessment of the implementation of the Safer Social Networking Principles for the EU. These principles were established within a self-regulatory agreement signed by 21 companies, including Facebook, Google, and MySpace, which had been negotiated with the help of the EU Commission in 2009.

The agreement aims at strengthening protection against misuse of the personal data of minors, as it may present risks such as cyber-bullying, grooming, privacy violation, or exposure to harmful content.

Some of the measures outlined in the Safer Social Networking Principles are:

- Ensuring that services are age-appropriate;
- Providing easy-to-use mechanisms by which to report harmful conduct or content in violation of their Terms of Service;
- Responding quickly to such notifications;
- Empowering users to control their information with easily accessible tools and technology.

The published findings conclude that there have been considerable improvements since the first assessment; safety information for children and parents is easily understandable and accessible, there is a reported increase in responses to user help-requests, and several sites also provide child-friendly versions of their Terms of Use.

The report, however, also criticizes that the majority of social network platforms still make minors' personal information visible to users beyond the minor's approved list of contacts. Furthermore, the findings reveal that only in four services can minors, by default, be contacted by friends only. In 13 of the 14 tested services, some of the information provided by the minor during registration was automatically mapped into the user's profile without prior notification thereof.

The Commission therefore stresses the need for clear commitment by social networking services to remedy these shortcomings by applying appropriate safety tools and thus preventing the risks related to data misuse. (NK)

➤eucrim ID=1103057

EDPS Opinion on Commission's Evaluation of Data Retention Directive

On 31 May 2011, the EDPS published his opinion on the evaluation report from the Commission to the Council and the EP on the Data Retention Directive (Directive 2006/24/EC). The Commission presented its evaluation of the Directive on 18 April 2011 (see eucrim 2/2011, pp. 62-63). The Data Retention Directive obliges telecommunication providers to store personal data for up to two years for potential use in criminal investigations.

In the past, the EDPS, as well as other stakeholders in the area of data protection, have expressed their opinions against the Data Retention Directive (see also eucrim 3/2010, p. 94 and eucrim 2/2010, p. 50). After analysing the Commission's evaluation report, the EDPS stuck to his view that the Directive does not meet the requirements imposed by the fundamental rights to privacy and data protection.

The reasons for this conclusion are:

- Insufficient demonstration of the need to retain data under the Directive;
- The privacy-intrusive manner in which the storage of personal data is regulated;
- Member States are left with too much discretion to regulate the conditions under which data are stored and accessed and the purposes for which they might be used.

The EDPS stated that a future data retention instrument should at least be comprehensive, exhaustive, and proportionate. The possibility of repealing the current Directive is not excluded. (EDB)

➤eucrim ID=1103058

Council Asks Member States to Implement Prüm Decisions

During the JHA Council of 9-10 June 2011, the Council requested the Member States to speed up the process of implementing the so-called Prüm Decisions.

Decisions 2008/615/JHA and 2008/616/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, provide the Member States' law enforcement authorities with additional tools to deal with these areas of crime. The most eye-catching of these tools is the automated exchange of DNA, fingerprints, and vehicle registration data. The provisions covering this automated data exchange should be implemented by 26 August 2011. Therefore the Council called upon stakeholders to speed up the implementation process. (EDB)

➤eucrim ID=1103059

Large-Scale IT Agency Operational in 2012

During the JHA Council of 9-10 June 2011, after intense debates, the Commission, and the EP, a compromise text finally resulted in political agreement on the setting up of a European agency for the operational management of large-scale IT systems (see eucrim 1/2011, p. 15 and eucrim 4/2010, p. 140).

The aim is to have one agency responsible for the operational management of the second-generation Schengen Information System (SIS II), the Visa Information System (VIS), and EURODAC as well as information systems that will be developed in the area of freedom, security and justice in the future. The inclusion of any additional systems requires a mutual decision by the Council and the EP.

The agency's seat will be in Tallinn, Estonia with tasks related to development and operational management to be carried out in France and a backup site in Austria.

The next step in the legislative process is now the first reading of the compromise text in the EP. The plan is to have the agency operational by the summer of 2012. (EDB)

➤eucrim ID=1103060

EU Citizens Concerned about the Use of Their Personal Data

EU citizens accept the release of personal data but are concerned about what companies, search engines, and social networks do with their data. This is one of the results of the new Eurobarometer survey on attitudes towards data protection and electronic identity, released by the Commission on 16 June 2011.

Since 1973, the Commission's Public Opinion Analysis sector regularly monitors public opinion on key issues such as data protection and electronic identity.

The previous Eurobarometer on this issue dates from 2008.

60% of all European Internet users shop online and use social networking sites. 70% indicate concern over how companies use their data, and 74% would prefer to give their specific consent before data are collected and used on the Internet. Citizens trust public authorities to gather personal data, but their trust is low when private companies, including Internet providers and online services, are involved. (EDB)
➤eucrim ID=1103061

Victim Protection

Council Confirms Victims' Rights as a Matter of Priority

The roadmap for strengthening the rights and protection of victims, in particular in criminal proceedings that was presented by the Commission on 18 May 2011 (see eucrim 2/2011, p. 64), was adopted during the JHA meeting of 9-10 June 2011.

This roadmap includes a proposed Directive on establishing minimum standards on the rights, support, and protection of victims of crime, revising Framework Decision (2001/220/JHA) on the standing of victims in criminal proceedings. Additionally, the roadmap includes a proposed Regulation on mutual recognition of protection measures for victims in the context of civil matters. As a matter of priority, the Council will now discuss the proposals presented by the Commission regarding these two measures. In the meantime, the UK and Ireland have notified the Commission of their wish to participate in the adoption and application of the proposed Directive and Regulation.

The regulation on mutual recognition of protection measures in civil matters will complement the EPO in criminal matters (see eucrim 1/2011, p. 15), which is currently in the discussion stage in the Council. (EDB)
➤eucrim ID=1103062

Freezing of Assets

Measures Taken Against Officials and Associates of Syrian and Libyan Regimes

On 9 May 2011, the Council adopted a Regulation and a Decision providing for an embargo on exports to Syria of arms and equipment that could be used for internal repression, as well as a visa ban and an assets freeze. The funds or economic resources of 13 officials and associates of the Syrian regime (identified by the Council as responsible for violent repression against civilians in Syria) have been frozen. Due to the increasing seriousness of the situation, 17 additional persons, including President Bashar al-Assad, and 4 entities (companies, organisations or bodies) were added to this list on 23 May and 23 June 2011 by adopting further legal instruments.

The situation in Libya has resulted in similar freezing measures being imposed on 79 persons and 47 entities. This was achieved by adopting a series of Decisions and Regulations since February 2011. On 7 June 2011, six Libyan port authorities were added to this list.

On 14 July 2011, the EP's Foreign Affairs Committee heard Syria's and Libya's opposition leaders. Both asked the EU to help them by supporting Syrian protesters and releasing the Libyan regime's frozen assets to use them for humanitarian aid. The members of the Foreign Affairs Committee confirmed that the EU should step up support for the Syrian protesters. (EDB)
➤eucrim ID=1103063

Cooperation

Police Cooperation

CEPOL 2010 Annual Report

At its meeting of 12 May 2011, the JHA Council endorsed the 2010 CEPOL Annual Report.

In 2011, CEPOL organised 80 courses and seminars and 11 conferences (99 in total, 2 less than in the previous year). Of these 99 activities, eight had to be cancelled. A total of 2,198 participants attended these 91 events, 77% of the available 2,869 potential places were used. Most participants were from Bulgaria, France, and Spain. On average, 14 Member States participated per course (13 in the previous year); however, 69 of the 91 activities saw less than two thirds of the Member States represented. According to the report, explanations for this low representation could be the lack of financial resources and available persons within the target group and topics not being a priority in these Member States. Overall feedback from the participants on the courses was very positive and better than the previous year, with 95% being satisfied in general. A total of 791 experts contributed to the CEPOL activities, 622 from EU Member States, 34 from non-EU countries, and 134 from EU bodies and organisations.

Concerning online training, CEPOL started the production of online learning modules in 2010. Furthermore, two Common Curricula on money laundering and drug trafficking, including trainers and study guides were able to be finalised in 2010 and translation orders processed.

From September to mid-November 2010, 82 police offers were given the opportunity to participate in the third CEPOL Exchange Programme, a 13-day "one-to-one" exchange. Furthermore, several courses, technical seminars, conferences, and meetings of the CEPOL Euromed Police II Project, a project strengthening international police cooperation with the MEDA countries (Algeria, Egypt, Israel, Lebanon, Jordan, Morocco, the Palestinian Authority, Syria, and Tunisia) were implemented.

Regarding its external cooperation, CEPOL has reinforced its cooperation with relevant EU agencies, notably Frontex, Eurojust, and Europol. Cooperation agreements have been signed with

the Turkish National Police Institute and the Croatian Police College.

In the field of research, in 2010, CEPOL conducted the 2010 CEPOL European Police Research and Science Conference and the CEPOL Research Symposia and published three further issues of the Police Science and Research Bulletin. Furthermore, CEPOL has published a map of European police-research institutions as well as a topical research list for the benefit of course managers, with links to publically available material on the Internet.

The European Police Science Handbook/Encyclopedia and the update survey on Police Research and Science were not concluded in 2010.

Administratively, 2010 saw the departure of one CEPOL Director and the arrival of a new Director and accounting team. Besides the successful implementation of the 2010 budget, the anomalies in the financial statements of the 2008 budget could be resolved in 2010 (see eucrim 1/2011, p. 15 and eucrim 4/2010, p. 143). (CR)

➤eucrim ID=1103064

CEPOL Five-Year External Evaluation Report

At its meeting of 9-10 June 2011, the JHA Council endorsed the CEPOL five-year external evaluation report covering the period of 2006-2010. The report consists of two parts. The first part includes the quantitative and qualitative five-year external evaluation of CEPOL by Blomeyer & Sanz assessing its governance and performance. The second part provides for recommendations on CEPOL's structure and working practices by its Governing Board. Overall, the findings are positive and foresee seven specific recommendations:

- To clarify the CEPOL intervention logic;
- To streamline governance and rationalise structures,
- To strengthen the CEPOL Secretariat;
- To merge capacity building for law enforcement;
- To assess Member State engagement with CEPOL;
- To concentrate capacity-building efforts;
- To measure results and impacts. (CR)

➤eucrim ID=1103065

Battle Against Falsified and Counterfeit Medicines

The delivery of small consignments of falsified and/or counterfeit medicines by express freight or postal freight through the Internet allows perpetrators to remain anonymous. This is only one example of the increasing global problem of falsified and counterfeit medicines.

Hence, at its meeting of 9-10 June 2011, the JHA Council adopted conclusions on the role of law enforcement cooperation in countering the distribution of falsified and/or counterfeit medicines. The conclusions are a further step in EU efforts to combat falsified medicines in combination with *inter alia* the current amendment procedure for Directive 2001/83/EC and the EU's Internal Security Strategy "Towards a European Security Model" (see eucrim 1/2011, p. 2).

Member States are invited to use Internet monitoring units within their respective authorities active in the field of falsified and/or counterfeit medicines to identify websites with potentially illegal offers of medicines. This includes websites that do not meet the safety requirements laid down in the aforementioned Directive on the sale of medicinal products at a distance to the public. Furthermore, Member States shall designate and draw up a list of national contact points within law enforcement authorities. They shall ensure that adequate training is provided to the respective personnel of competent law enforcement authorities as well as encourage cooperation between all authorities involved. Relevant information shall be sent to Europol for inclusion in its respective Analysis Work Files (AWFs), and Member States shall benefit from the Europol Platform for Experts (EPE) on the Internet. Europol is invited to consider broadening its relevant AWFs. Where necessary, Member States may set up JITs. They may make full use of Eurojust. Member States should also consider the possibility of submitting project proposals with a view to obtaining EU support funding. For its citizens, Member States shall encourage specific awareness-raising programmes and campaigns pointing out the health threat posed by falsified and/or counterfeit medicines. Finally, Member States are asked to continue supporting the ongoing work on this subject in international forums, such as the Council of Europe, Interpol, World Health Organization, and other bodies.

The Commission is invited to ensure that due attention is given to medicines in the context of the work of the Customs Expert group on counterfeiting and the Internet. It should also consider the possibility of carrying out a study on the scope and nature of falsified and/or counterfeit medicines, their impact within the EU, the enforcement of intellectual property rights, and best practices in this field.

Ultimately, the Council invites CEPOL to consider the possibility of developing training modules and exchange programmes in the field of combating falsified and/or counterfeit medicines. (CR+ST)

➤eucrim ID=1103066

Police Equal Performance Project

In the JHA Council meeting of 9-10 June 2011, Austria presented the "Police Equal Performance" project (PEP), an initiative for a focused operational approach to cooperation between the EU and the Western Balkans in fighting serious and organised crime.

PEP is a regional strategy developed by Austria for Central and South Eastern Europe. It aims improving the performance of police forces by applying best practices in policing and enhancing the operational cooperation between EU Member States and Western Balkan police forces. (CR)

➤eucrim ID=1103067

European Investigation Order

Council Agreement on Main Principles

At its meeting of 9-10 June 2011, the JHA Council agreed on the main principles governing the proposed European Investigation Order (EIO) in criminal matters (for details on the EIO, see eucrim 2/2011, pp. 68-69; eucrim 1/2011, p. 16; eucrim 4/2010, p. 145; eucrim 2/2010, p. 54). The agreement covers the following issues:

- Criminal proceedings, but also proceedings inititated by administrative authorities having a criminal dimension.
- Grounds for non-recognition and non-execution to ensure that an EIO is not executed if it could harm national security interests or immunities established in the executing State.
- Entitlement of interested parties to legal remedies equivalent to those available in a similar domestic case. Proper information on this possibility must be available. Legal remedies may be provided by both the issuing and the executing State.
- Acknowledgement of receipt of an EIO within 30 days. The investigation measure must be carried out within 90 days.
- Assumption of the costs of an EIO by the executing State for measures carried out in its territory. (CR)

➤eucrim ID=1103068

Law Enforcement Cooperation

Road Safety

On 6 July 2011, the EP voted in favour of a compromise text for a Directive on cross-border enforcement in the field of road safety. The Directive will cover the most dangerous road offences, e.g., speeding, driving under the influence of alcohol or drugs, and illegal use of mobile phones or other communication equipment while driving (for details, see eucrim 1/2011, pp. 17-18 and eucrim 3/2010, p. 97).

Based on negotiations with the EP, items inserted in the proposal concern better protection for personal data, mandatory requirements for the offence notification to be sent to the presumed offender, an obligation for Member States to report back to the Commission on the Directive's effectiveness (including figures), and a requirement for the Commission to produce a detailed report within five years after the Directive's entry into force. The latter should include, if necessary, a proposal to revise it as well as an annex requiring Member States to act to ensure greater convergence of road traffic rules and their enforcement, including comparable methods, practices, and minimum standards at the EU level.

As a next step, the draft Directive must be formally adopted by the Council. After its adoption, Member States will have two years to transpose the Directive into national law. (CR)

➤eucrim ID=1103069

European Network of Specialised CBRN Law Enforcement Units

At its meeting of 9-10 June 2011, JHA Ministers adopted conclusions on the creation of a European network of law enforcement units specialised in the prevention of terrorist attacks involving chemical, biological, radiological, or nuclear (CBRN) materials. The creation of such a network is part of the implementation of the 2009 EU CBRN Action Plan. Together with the Commission and Europol, Member States were asked to set up a network of specialised CBRN law enforcement units with the aim of facilitating the exchange of information and good practices, organising joint training exercises, and updating them on the latest developments. (CR)

➤eucrim ID=1103070

European Best Practice Guidelines for Police and Customs Cooperation Centres

At its meeting of 12 May 2011, the Council adopted the European Best Practice Guidelines for Police and Customs Cooperation Centres (PCCC). The guidelines provide practical recommendations for Member States on how to set up and operate their own PCCC.

The guidelines include advice on the establishment of a PCCC. It is defined as a support structure for exchanging information on and providing support to the activities of the operational agencies responsible for police, border, and customs tasks in the border area, bringing together staff from the authorities responsible for security in a single location.

The guidelines recommend setting up an agreement between the partner States as the legal basis for a PCCC. A model agreement is provided in the annex to the guidelines.

Further recommendations are made with regard to the location of a PCCC. It is suggested that it be set up in the immediate vicinity of the borders between participating States. The territorial competence of a PCCC should be primarily related to and carried out in the border area; however, the agreement may allow requests to be referred to the PCCC by agencies outside this area.

Rules for the operation of a PCCC should be laid down in an operating regulation. A model operating regulation is given in the annex to the guidelines. Recommended tasks for a PCCC include collecting and exchanging information, assisting operations taking place in the border area, and conducting specific analysis of cross-border crime.

To coordinate a PCCC, the appointment of one national coordinator per participating State is recommended. With regard to the functional organisation of a PCCC, the guidelines suggest that the centre's staff be specifically and exclusively assigned to it and possess sound language skills and legal knowledge. A PCCC should be open 24/7 or at least maintain a permanent contact point. It should have a secure internal and external communication system. Each unit should have permanent direct access to its own national databases. Computer

management of a PCCC should allow for the circulation of information in real time, fast processing of questions, standardised recording of statistics, and be available in all languages of the PCCC.

Regarding the budget of a PCCC, it is recommended that the costs of installing and operating PCCCs be shared between the participating States. It is up to the partners, however, to decide on the rules for sharing expenditure.

The guidelines also recommend setting up a sound evaluation procedure for the PCCC and makes proposals for the status, composition, and role of the evaluation committee and the evaluation procedure. (CR)

➤eucrim ID=1103071

European Medical and Psychological Experts' Network for Law Enforcement

At its meeting of 14 May 2011, the JHA Council adopted a resolution on the creation of a European Medical and Psychological Experts' Network for Law Enforcement (EMPEN). Through the EMPEN, those involved in medical, medico-legal, and psychological activities in the law enforcement field will be given a platform to exchange experiences and best practices. The network shall focus on two main topics:

- First, the network shall support the scientific activities of medical and psychological experts in the field of law enforcement. Experts shall be given the possibility to disseminate their knowledge through conferences, seminars, professional journals, and possibly the EMPEN website or online forum.
- Second, the network shall focus on the exchange of information in certain fields of law enforcement psychology, e.g., psychological assessment, psychological support and care for police officers, and psychological support provided by police services.

Member States are invited to designate and draw up a list of national EMPEN contact points.

Hungary is providing administrative support during the network's development phase as well as the first rotating secretariat

The Commission is invited to consider providing appropriate funding to support the activities of EMPEN. CEPOL is asked to consider whether specific training courses could be provided. (CR)

➤eucrim ID=1103072

Sports Events Security

Due to the increasing international character of sport events and their organisation with non-EU countries, the Polish Presidency aims at establishing common standards for cooperation in this field. As a first step, Poland has prepared a questionnaire on police cooperation with non-EU countries in the area of sports events security that was sent to twenty-seven Member States, seven non-EU countries (Switzerland, Croatia, Turkey, Serbia, Russia, Ukraine, Israel), and Europol. Replies were received from a total of thirty countries and from Europol.

The results of the questionnaire indicate that almost all National Football Information Points (NFIPs) cooperate and exchange information both with Member States' NFIPs and contact points in non-EU countries; some countries also have other contact points. While most NFIPs are also responsible for exchanging information in relation to the Olympic Games as well as other sports events (such as basketball, skiing, tennis, athletics, etc.), eight countries do not exchange information in connection with the Olympic Games, and four NFIPs are concerned with football matters only. Almost all NFIPs have been involved in international police cooperation with non-EU countries, using the "Football Handbook" as a basis for the exchange of information. However, many of them have not exchanged personal data. 22 countries and Europol have conducted joint supportive actions in cooperation with non-EU countries.

The largest obstacle identified by all countries as regards cooperation with non-EU countries is the lack of NFIPs or other contact points. Most countries have identified the establishment of NFIPs or the designation of other contact points in those countries as the best solution to this problem. According to almost all countries, a document providing guidelines on cooperation with non-EU countries in the area of security at sports events should deal with the scope of cooperation, the type of exchanged information, the means of data exchange, the terms of cooperation, the division of tasks between various entities, and the elements of common standards of data protection.

On the basis of these results, as a next step, the Polish Presidency is planning to propose certain amendments to the "Football Handbook." (CR)

➤eucrim ID=1103073

Conclusions of the 6th Annual JIT Experts Meeting

The General Secretariat of the Council published the report and conclusions of the 6th Annual Meeting of the National Experts on JITs held in The Hague from 2-3 December 2010 (see also eucrim 1/2011, p. 15). The meeting focused on:

- Europol's newly available support to JITs;
- JITs in the Western Balkan region;
- Experiences with JITs from Belgian, French, Dutch, and Spanish examples;
- JITs with third countries;
- JIT funding;
- Profile requirements for the successful JIT expert at the national level (workshop);
- A solution-oriented discussion on issues commonly encountered during the setting-up, running, and conclusion of JITs.

With regard to the JIT expert profile, the following requirements were identified: JIT experts should possess expertise and extensive practical experience with JITs; they should be the central contact points in their Member States and available on a 24/7 basis. Besides being proactive and good networkers, JIT experts should have a sound knowledge of

national, EU, and other Member State law and be familiar with EU funding schemes. JIT experts should be responsible for raising awareness with regard to the funding schemes. They should receive information to identify JIT cases at an early stage and have enough national budgetary and manpower support to fulfil their role.

Looking at the main issues encountered by practitioners during the setting-up, running, and conclusion of a JIT, the workshops recommend early involvement of Eurojust or Europol to assist in the drafting of the JIT Agreement and the application for funding. The EU Commission funding application procedure was found cumbersome and inappropriate for international police/judicial cooperation. Training for seconded members was seen as helpful if the length, duration. and intensity of training measures was tailored to individual cases.

The importance of awareness-raising and increasing practitioners' confidence was emphasised.

The meeting was attended by experts and practitioners from 22 Member States and by representatives of the Commission, the General Secretariat of the Council, Europol, and Eurojust. (CR)

➤eucrim ID=1103074

Prüm: Updated Implementation Guide for DNA Data Exchange

The German delegation has published an updated version of the implementation guide concerning DNA data exchange under the Prüm provisions. It is based on the knowledge and experience of and prepared by experts of the German Federal Criminal Police Office (*Bundeskriminalamt* [BKA]). The guide aims to help Member States with the IT implementation of the Prüm requirements, especially with regard to software components. It contains recommendations from a technical and forensic point of view (for further details on the Prüm Decisions, see eucrim 1-2/2008, pp. 35-36). The scope of the guide concerns Chapter 1 of the Annex to Decision 2008/616/JHA and mainly covers the following aspects of DNA data exchange:

- Interface control documents;
- Application architecture;
- Network infrastructure;
- Testing methodology;
- Further steps.

For the future, the BKA sees the need to define a general procedure for further development of the standards, specifications, and deployment of DNA data exchange components at the EU level. (CR)

➤eucrim ID=1103075

Prüm: France Ready to Exchange Dactyloscopic Data

Having fully implemented the data protection provisions required to pass the evaluation procedure under Council Decision 2008/616/JHA, France can now engage in the automated exchange of fingerprint data for the purpose of the prevention and investigation of criminal offences.

The Council adopted a respective Decision at its meeting of 9-10 June 2011 (for further details on the Prüm Decision, see eucrim 1-2/2008, pp. 35-36). (CR)

➤eucrim ID=1103076

Council of Europe*

Reported by Dr. András Csúri

Foundations

Reform of the European Court of Human Rights

Sir Nicolas Bratza Elected President of ECtHR

On 4 July 2011, the ECtHR elected Sir Nicolas Bratza as its new President. He will take office on 4 November 2011.

Sir Nicolas was born on 3 March 1945, studied law at the University of Oxford, served as a member of the European Commission of Human Rights between 1993 and 1998, and has been a judge at the Court since 1 November 1998 (Vice-President of the Court since 19 January 2007).

➤eucrim ID=1103077

New Statistics and Instructions on Requests to Suspend Expulsion of Applicants before the ECtHR

The Court amended and published a practice direction of instructions covering requests for interim measures, in part as a response to the drastic increase in Rule 39 requests (see eucrim 2/2010, p. 56). Interim measures are exceptional and bind the State concerned. They can be requested

* If not stated otherwise, the news reported in the following sections cover the period May – July 2011.

by virtue of Rule 39 of the Rules of Court only in cases when the applicant faces real risk of serious, irreversible harm if the measure is not applied.

The instructions require the applicants and their lawyers to comply with a series of legal requirements when requesting the application of interim measures, e.g.:

- Detailed reasoning, specifying the grounds and nature of the alleged risks and the provisions of the ECHR alleged to have been violated;
- Attached copies of the relevant decisions;
- The expected time, date, and time of removal in case of extradition or deportation, with the applicant's address or place of detention and official case-reference number;
- Requests shall be sent by facsimile or post and, where possible, in the official language of one of the countries that has ratified the Convention. Requests sent by e-mail will not be processed;
- Requests should be received by the Court as soon as possible after the final domestic decision or, if there is a risk of immediate enforcement, beforehand (especially in extradition or deportation cases). The Court is unable to process requests received less than one working day before the planned removal in extradition or deportation cases.

Every six months, the Court will publish on its website statistics on the number of requested and rejected interim measures classified by the state concerned and the country of destination.

➤eucrim ID=1103078

Filtering Section Speeds Up Processing of Cases

One of the main challenges of the Court is the efficient filtering out of the large number of inadmissible cases brought before it each year (an estimated 90% of all cases in the Court's Registry). The impetus for this process was provided by the entry into force of Protocol No. 14 (see eucrim 1/2009, pp. 25-26 and 4/2009, pp. 147-148) and the establishment of the "single judge" formation (see eucrim 4/2009, p. 147). In the wake of the Inter-Governmental Conference at Interlaken in February 2010 (see eucrim 4/2009, p. 147), the Court has set up a new filtering section (in operation since 2011) to handle the incoming cases from five of the highest case-count countries: Russia, Turkey, Romania, Ukraine, and Poland. It intends to minimise the time taken to respond to applicants' complaints and to reduce the backlog of unexamined cases (see eucrim 4/2009, p. 147).

By the end of June 2011, the filtering section proved itself in speeding up the administrative and legal processing of incoming complaints. Further modifications in organisation and procedure are envisaged in the second half of 2011 to further improve efficiency.

➤eucrim ID=1103079

Other Human Rights Issues

Human Rights Commissioner Publishes 1st Quarterly Activity Report for 2011

On 25 May 2011, Thomas Hammarberg, CoE Commissioner for Human Rights (hereinafter: the Commissioner), published his first quarterly activity report for 2011. It consists of an overview of the central themes of the Commissioner's most recent work (including media freedom, the human rights of Roma, human rights in relation to migration, the rights of persons with mental health problems or intellectual disabilities), the visits he made, a summary of meetings he attended (including the Conference on "Social Networks" marking Data Protection Day 2011), and his work related to the ECtHR. The latter follows up on the Interlaken Declaration (see eucrim 4/2009, p. 147) to encourage the prompt implementation of judgements issued by the ECtHR. In this connection, the Commissioner addressed the following countries with concrete concerns: Malta (the issue of mandatory detention of irregular migrants), Turkey (freedom of religion), Armenia and Hungary (freedom of expression).

➤eucrim ID=1103080

Commissioner on Prosecutors' Wide Range of Responsibility

The Human Rights Commissioner held a speech at the Plenary Meeting of the Network of Public Prosecutors or Equivalent Institutions at the Supreme Judicial Courts of the Member States of the European Union in Rome (26-28 May 2011).

The Commissioner underlined the need for the impartiality of this institution and its general role in defending and promoting human rights. Even though their mandates may differ from Member State to Member State, there are certain principles that are always to be respected. These standards are compiled in Recommendation (2000)19 of the Committee of Ministers to Member States on the role of public prosecution in the criminal justice system and in Recommendation 1604 (2003) on the role of the Public Prosecutor's office in a democratic society governed by the rule of law. These recommendations urge avoiding conflicts of interest, ensuring check and balances, the impartiality and independence of the justice system in general, as well as the importance of the assignment and reassignment of cases with regard to internal operations.

The Commissioner then stressed situations that often give rise to concerns, e.g., when the police have responsibility for prosecutions, when the Public Prosecutor is responsible for challenging decisions to detain, or when a judicial decision to release a detained person is suspended by an appeal by the prosecutor. Finally, the Commissioner stressed more child-friendly approaches throughout the investigation process (e.g., interviews carried out by trained professionals) and paying particular attention to the needs of migrants who entered a country as victims of human trafficking.

➤eucrim ID=1103081

Specific Areas of Crime

Corruption

GRECO: 11th General Activity Report and Call for More Resources

On 29 June 2011 GRECO presented its annual report on its activities throughout 2010. The report described the various evaluation procedures. In 2010, eleven Third Round Evaluation Reports were published on Armenia, Azerbaijan, Bulgaria, Greece, Hungary, Montenegro, Portugal, Romania, Serbia, the Former Yugoslavian Republic of Macedonia, and Turkey. For summaries of these reports, refer to eucrim 4/2009, p. 149; 1/2010, pp. 20-22; 3/2010, pp. 101-103; 4/2010, pp. 149-150, and 1/2011, pp. 19-21).

In 2010, GRECO agreed on a fourth evaluation round, to be launched in 2012, in order to assess corruption prevention in parliamentary assemblies, the judiciary, and among other actors in the prejudicial and judicial process.

The report addresses cooperation with EU and describes the pace of exchange as having increased during 2010. The main reason for this is the 2009 Stockholm Programme, in which the European Council invited the European Commission to develop a comprehensive anti-corruption policy in close cooperation with GRECO and, further, to submit a report on a future accession of the EU to GRECO. These consultations resulted in a provisional common understanding of the key issues that need to be clarified in connection with EU participation.

While presenting the annual report, Drago Kos, Chair of GRECO, called for more resources to fight corruption in Europe and at the global level. He described the performance of a number of countries – most of them EU Member States – in the third evaluation round (examining the criminalisation of corruption and the transparency of political funding) as "globally unsatisfactory." He concluded that more time, effort, and funding is needed to fight corruption in Europe. He expressed his concerns regarding "slumps in political determination or even backtracking of previous achievements." Finally, he expressed his great expectations from strengthened cooperation with the EU in this field.

➤eucrim ID=1103082

CDPC Discusses Corruption in Sports

At its plenary session on 14-17 June 2011, the CDPC took note of the information provided by the Secretariat of the CoE, the Enlarged Partial Agreement on Sport (EPAS), and by the Chair of GRECO concerning the integrity of sports and the issue of match-fixing.

The Committee of Ministers is due to adopt the draft recommendation on the Promotion of the Integrity of Sport against the Manipulation of Results by the end of September 2011.

Nevertheless, Mr. Drago Kos, Chair of GRECO, concluded in his information document that "…in order to effectively fight match-fixing internationally there is no need for changes in the area of criminal offences at the level of international legal instruments. Nor is there any need for radical changes at the level of national legislation. In a very limited number of countries some definitions – concerning the position of sport in the public or private sector – could be slightly adjusted and, also, in a very limited number of countries, the sentences provided for basic cases of fraud could be slightly increased. In comparison to the enormous proceeds gained by perpetrators from match-fixing world-wide over recent years, such an effort should not place too heavy a burden on countries."

➤eucrim ID=1103083

GRECO: Third Round Evaluation Report on Andorra

On 15 June 2011, GRECO published its Third Round Evaluation Report on Andorra. As usual, the report focused on two distinct matters: the criminalisation of corruption and the transparency of party funding, with both areas in need of improvements. GRECO made a total of 20 recommendations to the country.

Regarding the criminalisation of corruption, the report found that further amendments to the Criminal Code are necessary in order to comply with the standards of the CoE's Criminal Law Convention on Corruption (hereinafter: the Convention), which Andorra has ratified. The findings identify the somewhat restrictive manner of the criminalisation of bribery and trading-in-influence offences as a partial but possible explanation for the absence of prosecutions and convictions of such offences. As regards bribery, shortcomings were identified in the criminalisation of non-material benefits and of bribery in the private sector, in general. The report further calls for stiffer penalties in this field and urges Andorra to ratify the Additional Protocol to the Convention.

Regarding the transparency of political financing, GRECO calls for considerable changes to the relevant legislation. According to the report, the current election financing law intends to ensure that public funds are properly used under the supervision of the court of audit. However, the law concerns only those private funds that are eligible for reimbursement by the state and does not ensure the overall transparency of political financing or the avoidance of undue financial influence on public decision making. For these reasons, the report urges Andorra to make considerable changes to its legislation to make it obligatory for political groups to publish their accounts on a regular basis by specifying their major sponsors and in-kind supporters.

➤eucrim ID=1103084

GRECO: Third Round Evaluation Report on Georgia

On 1 July 2011, GRECO published its Third Round Evaluation Report on Georgia, with a total of 15 recommendations to the country. The main conclusion is the need for effective supervision of the application of legislation on political financing.

Regarding the criminalisation of corruption, the report acknowledged that the provisions on corruption in the Georgian Criminal Code are almost fully in line with the requirements of the Convention and its Additional Protocol. Shortcomings still exist in the bribery of foreign arbitrators and jurors, the provisions on jurisdiction, the inadequate covering of undue third-party beneficiaries in case of private-sector bribery and active trading in influence, as well as the risk of abuse of "effective regret" as a special defence. GRECO calls for the revision of these provisions.

Concerning the transparency of party funding, GRECO noted the positive features of the current legislation, which aim to strengthen the transparency of political financing. However, it emphasised the need for more detailed and publicly accessible information on parties' income, expenditure, assets, and debts. The report identifies the lack of effective monitoring as the fundamental weakness in the current system. This undermines the effectiveness of improving legislation. Therefore, the establishment of an adequate, impartial supervisory authority must be a future priority in this field.

➤eucrim ID=1103085

Money Laundering

MONEYVAL: Report on Fourth Assessment Visit to Czech Republic

On 16 June 2011, MONEYVAL published the Report on its Fourth Assessment Visit to the Czech Republic. The fourth cycle of assessments is, in general, a follow-up round, in which important Financial Action Task Force (FATF) Recommendations are reassessed as well as those findings for which the state received non-compliant or partially compliant ratings in its third round report. The report summarises, describes, and analyses the major anti-money laundering and counter-terrorist financ-

Ratifications and Signatures (Selection)

Council of Europe Treaty	State	Date of ratification (r) or signature (s)
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)	Armenia	08 April 2011 (s)
Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181)	Armenia	08 April 2011 (s)
Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182)	Ireland Ukraine	26 July 2011 (r) 14 September 2011 (r)
Convention on Cybercrime (ETS No. 185)	United Kingdom	25 May 2011 (r)
Convention on Cybercrime, concerning the criminalisation of acts of a racist and xénophobic nature committed through computer systems (ETS No. 189)	Finland Germany	20 May 2011 (a) 10 June 2011 (r)
Protocol amending the European Convention on the Suppression of Terrorism (ETS No. 190)	Germany	13 July 2011 (r)
Additional Protocol to the Criminal Law Convention on Corruption (ETS No. 191)	Finland Finland Bosnia Herzegovina	04 May 2011 (s) 24 June 2011 (a) 07 September 2011 (s & r) 07 September 2011 (s & r)
Convention on the Prevention of Terrorism (CETS No. 196)	Germany	10 June 2011 (r)
Convention on Action against Trafficking in Human Beings (CETS No. 197)	Andorra	23 March 2011 (r)
Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198)	Ukraine France	02 February 2011 (r) 23 March 2011 (s)
Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201)	Austria Romania Finland Luxembourg	25 February 2011 (r) 17 May 2011 (r) 09 June 2011 (a) 09 September 2011 (r)
Convention on preventing and combating violence against women and domestic violence (CETS No. 210)	Austria Finland France Germany Greece Iceland Luxembourg Montenegro Portugal Slovakia Spain Sweden Turkey Norway FYROM Slovenia	11 May 2011 (s) 11 May 2011 (s) 11 May 2011 (s) 11 May 2011 (s) 11 May 2011 (s) 11 May 2011 (s) 11 May 2011 (s) 11 May 2011 (s) 11 May 2011 (s) 11 May 2011 (s) 11 May 2011 (s) 11 May 2011 (s) 11 May 2011 (s) 07 July 2011 (s) 08 July 2011 (s) 08 September 2011 (s)

➤eucrim ID=1103089

ing measures (AML/CFT) in place at the time of the fourth on-site visit (May 2010). It offers recommendations on how to strengthen certain aspects of the AML/CFT system.

The report welcomed the adoption of the new AML/CFT Law, which implements the 3rd EU Directive and many of the important preventative recommendations of MONEYVAL's 3rd round evaluation report. Furthermore, the Financial Intelligence Unit (FIU) of the Czech Republic was assessed as well trained, and is now more effective with proactive approaches and a good level of international cooperation. Nevertheless, the report urges the verification of beneficial owners of accounts to be more embedded in practice and states that the vulnerable sectors of the Czech financial system regarding ML and FT need to be identified more precisely. Legislation requires further amendments in order to comply with international ML standards, and Czech law still does not provide for corporate criminal liability. Nonetheless, the report recognised legislative progress towards a more complete legal framework against FT. MONEYVAL suggests that Czech authorities analyse the discrepancy between the low number of ML cases being prosecuted in contrast with the high incidence of ML and the total damage from economic crime in the country. Ultimately, the report warns that the lack of statistics on confiscation orders negatively affects the overall effectiveness of the system.

➤eucrim ID=1103086

MONEYVAL: Report on Fourth Assessment Visit to Albania

On 7 July 2011, MONEYVAL published its fourth round Evaluation report on Albania.

Albania has a history of clan-based and hierarchically organised networks, mainly involved in drug trafficking. The sectors with illegal practices further make Albania at high risk of ML activity. The reliance on cash and its use in the informal economy has an overall impact on the effectiveness of preventive measures, as such transactions circumvent these preventive measures. The report states that the country also remains at risk regarding possible FT activities.

Nevertheless, Albania has made considerable progress in improving its AML/CFT regime since the 2006 third round report. It has fully criminalised ML, largely in compliance with international standards. It enacted a new Organized Crime Law that provides for civil preventive confiscation in case of many serious offences. Albania has also updated its legal framework of preventive measures for financial institutions. Despite these measures, there are very few convictions for ML, and the countries evidence-based procedure has a further negative impact on the effective use of these provisions. Furthermore, the enhanced FT legislation and the preventive measures for financial institutions still fall short of FATF and international standards. In the latter case, the implementation of the law proves to be difficult because of a disparate understanding of the provisions among financial institutions. The report regards domestic and international cooperation as being generally good but described co-operation between the supervisory agencies as "underutilised."

➤eucrim ID=1103087

Procedural Criminal Law

CCJE: Opinion No. 14 on "Justice and new information technologies"

The CCJE working group (CCJE-GT), entrusted with the preparation of Opinion No. 14 on "Justice and new information technologies," held its meeting in Strasbourg on 15 and 16 June 2011. It was based on a draft prepared by an expert consultant.

A questionnaire on this subject was also sent to Member States, of which 36 have replied. In view of its adoption, the draft opinion will be examined at the next plenary meeting in November 2011.

➤eucrim ID=1103088

Associations for European Criminal Law and for the Protection of the EU Financial Interests

20 Years Later: A New Impetus

The first Association was formally constituted in Rome in October 1990. Today, there are 32 Associations altogether, representing all the Member States (except Cyprus), plus Croatia, San Marino, Switzerland, and Turkey. AGON, the bulletin of the Associations, was first published in April 1993. It was replaced by eucrim in 2006. The Associations meanwhile function as a network and serve as a forum in the field of European criminal law and the protection of the financial interests of the European Union. They are made up of representatives from the legal and judicial professions (academics and practitioners) as well as other law enforcement agencies (police, inspection departments, etc.). Their mission is based on a series of guiding principles established in the early nineties and highlighting their structure, functions, role, objectives, and activities. Twenty years later, in the light of experience gained and the new environment provided by the Lisbon Treaty, it is appropriate to reflect upon the future role of the Associations in the EU legal space. To this effect, new guidelines were agreed upon among the Associations' delegates in May 2011 concerning the structure, role, and priorities of the Associations. The guidelines aim, in particular, to improve the cooperation with OLAF, to analyse the possibilities for the creation of a European Public Prosecutor and for coherent legislation regarding the protection of the financial interests of the European Union – in the spirit of the Council decision of 30 November 2009 and the Stockholm Programme.

Guiding Principles for the Associations' Network Members

I. Common Aims

In a European area of freedom, security and justice, the traditional aims of criminal law can no longer be achieved on a purely national basis. Thus, the scope of criminal law should not be limited by national borders but instead become transnationally effective. It must also protect supranational values beyond national interests, such as the EU's financial interests in particular. At the same time, criminal law must guarantee civil liberties and be based on the principles of democracy and the rule of law. In addition, criminal law should only be used as a last resort, and it must be enhanced or replaced by non-criminal measures as far as possible. This is illustrated in the protection of the financial interests of the European Union, an area which has become the motor for the development of European criminal law and which will continue to be a catalyst under the Lisbon treaty. The Associations for European Criminal Law and for the Protection of the EU Financial Interests federated in the network are committed to the achievement of the above-mentioned aims and objectives.

II. Basic Principles

1. Network Identity

The name of the network is "Associations for European Criminal Law and for the Protection of the EU Financial Interests."

2. Membership in the Associations

The common requirement for membership in the Associations shall be a professional interest in the legal issues raised by the protection of the financial interests of the European Union.

- Members of the Associations may include judges, magistrates, academics, prosecutors, government lawyers and barristers, and lawyers in private practice or employed in internal and external financial bodies. Members of other related professions, such as accountants or professionals from relevant regional or provincial institutions of a Member State, are also welcome.

- An adequate representation of the regions or provinces of the Member State shall be encouraged.
- Members of the Associations shall be assured independence under the statutes of each Association and join in a purely personal capacity.

3. Objectives

Objectives of the Associations shall include:
- The dissemination of information, advancement of knowledge, and promotion of research in relation to European Criminal Law and the protection of the EU financial interests at the national level;
- The improvement of cooperation and mutual assistance between different jurisdictions and the increase in knowledge of other legal systems through contacts between Associations;
- The stimulation and promotion of debate on issues relating to European Criminal Law and the protection of the financial interests of the EU;
- Contributions to the development of relevant aspects of national and European criminal law.

4. Activities

In pursuit of the objectives of the Associations, it is anticipated that activities will include the organization of meetings, seminars, and conferences at the national and EU levels as well as the carrying out of studies, issuing of publications, and organisation of training seminars, etc.

5. Self-Reliance

Each Association must have the capability and infrastructure necessary to develop a strategy and implement objectives in conformity with the guiding principles. Each Association shall be capable of taking responsibility for all relevant elements of planning, organisation, and financial management of any activities which they undertake.

III. Communication

Communication applies at three levels: (1) Associations/ Commission; (2) within each Association; (3) between different Associations.

1. Associations / Commission

Considering the decentralised structure of the organisation of the network, OLAF should regularly receive a certain amount of information from each Association to increase awareness of activities undertaken in each Association. It is necessary to keep up-to-date all information on the Associations in order to enable OLAF to exercise a communication and supporting function. Information will include annual reports (minutes of Board meetings could be attached to annual reports) and mutual exchanges on an ad hoc basis with regard to important policy initiatives, legislation, judicial decisions, etc. at the national and EU levels. A contact person from each Association will be appointed to this effect.

2. Within Individual Associations

It is important that effective means are developed to ensure the distribution of information to all members, particularly those who are not living and working in the capital. To this end, minutes of Board or Committee meetings should be circulated. It is vital that, when representatives of an Association attend a seminar or conference, they prepare a summary report for the benefit of other representatives.

3. Between Associations

An information bulletin for all Associations is necessary to enable the exchange of information and ideas as well as to provide a link between the Associations and the Commission. eucrim (formerly AGON) has been developed to this end. The bulletin has three main functions:
- It is the medium for exchanging information on significant developments in law and practice at the national and EU levels that affect the protection of the EU financial interests and developments in EU criminal law in general;
- Actions organised by the Associations need to be communicated to a wider audience than just participants, via summaries of the contributions to be circulated;
- The Associations share a common identity and wish to develop better information flows and the sharing of expertise amongst those active in combating EU fraud, either as policy makers or as legal professionals in Member States. An Association may choose to communicate its activities by creating a website (with an interlink to the OLAF website).

IV. Functioning

Programming

The annual meeting of the Presidents of Associations contributes to defining the priorities of the network. Each Association shall present an annual activity programme in due time before the meeting of the Presidents of Associations.

Die Verwendung fiktiver Identitäten für strafprozessuale Ermittlungen in sozialen Netzwerken

Überlegungen zur Grundrechtsrelevanz und Zulässigkeit nach deutschem Recht

Stefan Drackert

The ongoing spread of social networking pages such as Facebook and Google+ recently sparked the interest of German security agencies. In a statement of 14 July 2011, the federal government acknowledged the relevance and conduct of criminal investigations on social networking pages. The government takes the view that the pseudonymous participation does in general not require a specific legal basis since there is no legitimate expectation of privacy on websites which do not require a verification of identity by registration. This view is partly shared in legal writing and refers to a relatively vague section in a recent judgment of the federal constitutional court. The article analyses that argument and reveals that it is too undifferentiated for a transfer to social networks and thus not in accordance with the constitutional requirements in Germany.

Einleitung

Soziale Netzwerke[1] bieten Strafverfolgungsbehörden zahlreiche Ermittlungsansätze. Eine Äußerung der Bundesregierung vom 14.7.2011[2] bestätigt nun das in der Literatur bereits beschriebene[3] Interesse der Behörden an eben diesen Informationen. Das Interesse dürfte vor allem auf die weite Verbreitung und Fülle der Inhalte zurückzuführen sein. So haben nach einer aktuellen Studie 76 % der deutschen Internetnutzer ein Profil in einem sozialen Netzwerk. Bei der Gruppe der – auch hinsichtlich der Kriminalitätsbelastung überrepräsentierten[4] – unter 30-Jährigen sind es sogar 96 %.[5] Bei aktiven Nutzern läuft ein Großteil der alltäglichen Kommunikation über die Internetseiten sozialer Netzwerke. Neben Textmitteilungen zwischen den Nutzern und kurzen Statusangaben mit unterschiedlichen Adressatenkreisen bestehen die Inhalte vor allem aus hochgeladenen Bildern und Videos, welche häufig mit Orts- und Zeitangaben sowie Links zu anderen Seiten verknüpft werden. Daneben finden Diskussionen in Online-Gruppen, Meinungsäußerungen über „Fanpages“ sowie Verabredungen zu Veranstaltungen statt. Der besondere Mehrwert und Reiz für die Nutzer besteht in der Möglichkeit, die Inhalte jeweils zu kommentieren und mit anderen Inhalten zu verknüpfen. Hinzu kommt das Profil des Nutzers – eine Art „Online-Visitenkarte“, die neben der Kontaktliste auch Informationen zu Wohn- und Arbeitsstätte, Hobbys, religiösen und politischen Anschauungen enthalten kann.[6] Eine Liste verfügbarer Informationen ließe sich beliebig verlängern und zeigt, dass die sozialen Netzwerke das Potential haben, das gesamte Leben eines Nutzers virtuell zu begleiten. Eben dies kann im Rahmen von Ermittlungen zur Identifikation Verdächtiger, zur Kontaktaufnahme mit potentiellen Zeugen und zur allgemeinen Aufklärung des Umfelds einer Zielperson genutzt werden.[7] In der Antwort der Bundesregierung heißt es, dass das Bundeskriminalamt (BKA) mit Informationen aus sozialen Netzwerken vorhandene Erkenntnisse „verdichtet“.[8]

Der Zugriff auf die relevanten Daten kann entweder vom Betreiber eingeräumt werden oder über ein fremdes oder ein eigens erstelltes Nutzerprofil der Behörde erfolgen. Da soziale Netzwerke bislang keinen Identitätsnachweis[9] bei Anmeldung verlangen, lassen sich Profile mit fiktiven Identitäten erstellen und zur Informationserhebung verwenden. Die Registrierung eines eigenen Profils dürfte aufgrund der einfachen und schnellen Realisierung in der Praxis besonders nahe liegen. Ein weiterer Vorteil dieser Variante besteht in der Möglichkeit der aktiven Teilnahme an der Kommunikation. Im Folgenden soll untersucht werden, ob die Verwendung eines unter fiktiver Identität[10] erstellten Profils zur anschließenden Kontaktaufnahme mit dem Nutzer eine nach deutschem Recht „grundrechtsneutrale“ Internetbeobachtung darstellt.[11]

Hierzu ist zunächst die Verfügbarkeit der Inhalte genauer zu beschreiben. Informationen in sozialen Netzwerken sind in der Regel nur abgestuft öffentlich zugänglich. So wurde etwa bei Facebook standardmäßig[12] folgendermaßen differenziert: 1. Informationen, die für alle, also auch über Suchmaschinen außerhalb der „Community“, zugänglich sind, 2. Informationen, die bloß den zur Kontaktliste hinzugefügten Personen („Freunde“) zugänglich sind und schließlich 3. Informationen, die den Kontakten der Kontakte zugänglich sind („Freunde von Freunden“). Zudem kann der Zugang auf bestimmte

Nutzer/Gruppen beschränkt werden. Weitere Abstufungen betreffen die Suchmöglichkeiten und biometrisch gewonnene Vorschläge für die Markierung abgebildeter Personen auf Bildern.[13] Das soziale Netzwerk von Google (Google+) differenziert die Zugänglichkeit noch stärker. Dort müssen die Kontakte von den Nutzern in selbst erstellte „Circles" eingeteilt werden (bspw. Arbeitskollegen/Familie), um so deren Inhalte zu verfolgen und ihnen eigene Inhalte abgestuft zugänglich zu machen.[14] Für Ermittlungen dürften gerade die Inhalte interessant sein, für die eine Zugänglichmachung durch den Nutzer erforderlich ist. Um an diese Informationen zu gelangen, müssen die Behörden jedoch ein Nutzerprofil anmelden und die Bestätigung über eine „Kontaktanfrage" bzw. eine Zustimmung zum „Teilen" bestimmter Inhalte einholen. Diese Abstufung, die teilweise dem Geschäftsmodell und teilweise den Anforderungen des Datenschutzes geschuldet ist, wird in der Literatur bisher nicht angemessen berücksichtigt. Dies dürfte auch an einer pauschalen Übertragung der für diesen Fall nur eingeschränkt aussagekräftigen Rechtsprechung des Bundesverfassungsgerichts (BVerfG) liegen.

I. Die Internetaufklärung im Urteil des BVerfG zur Online-Durchsuchung

Die Entscheidung des BVerfG zur Online-Durchsuchung[15] wird sowohl in der Antwort der Bundesregierung[16] als auch in den ersten Literaturstimmen[17] für eine relativ weitgehende Zulässigkeit der in Frage stehenden Ermittlungsmethoden herangezogen. Der mit der Verfassungsbeschwerde erfolgreich angegriffene § 5 Abs. 2 Nr. 11 des nordrhein-westfälischen Verfassungsschutzgesetzes enthielt neben der Befugnis zum Einsatz sog. Trojaner (Online-Durchsuchung) auch die Befugnis zum „heimlichen Beobachten und sonstigen Aufklären des Internet, insbesondere zur verdeckten Teilnahme an seinen Kommunikationseinrichtungen"[18] – also Ermittlungsmaßnahmen auf dem „technisch vorgesehenen Weg".[19]

Das BVerfG prüft diese zunächst am Maßstab des Telekommunikationsgeheimnisses, Art. 10 Abs. 1 GG. Dessen Schutzbereich umfasst jedoch nicht das personengebundene Vertrauen in den Kommunikationspartner, sondern nur die Überwachung der laufenden Fernkommunikation „von außen" – also ohne „Autorisierung".[20] Eine Autorisierung liegt vor, wenn der Inhalt für jeden zugänglich ist, oder wenn ein Kommunikationsteilnehmer willentlich den Zugang zu einem nicht öffentlichen Kommunikationsvorgang gewährt. Art. 10 Abs. 1 GG schützt damit die Fernkommunikation vor dem Staat, nicht jedoch vor ungewollter Fernkommunikation mit dem Staat.[21] Diese Vorgaben lassen sich auf Täuschungen durch Verwendung einer fiktiven Identität in sozialen Netzwerken übertragen: Sie greifen nicht in Art. 10 Abs. 1 GG ein, weil sie nicht das Risiko gerade der telekommunikativen Übermittlung betreffen.

Das BVerfG setzt die Prüfung anhand des Allgemeinen Persönlichkeitsrechts, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG fort. Dessen in der Entscheidung entwickelte neue Verbürgung, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht), soll jedoch nicht einschlägig sein. Die Internetaufklärung erfasse lediglich Daten, für die der Betroffene selbst sein System technisch geöffnet habe. Das Vertrauen darauf, dass solche Informationen nicht erhoben werden, sei nicht schutzwürdig.[22]

Unklar ist, ob das Gericht damit Zugriffe auf dem technisch vorgesehenen Weg vom IT-Grundrecht generell ausnehmen will,[23] oder ob der Schutzbereich deshalb nicht eröffnet sein soll, weil der Nutzer die Inhalte im Internet vorhält. Letzteres würde die „technische Öffnung" als Einwilligung bzw. Grundrechtsverzicht werten. Beide Schutzbereichsausnahmen lassen sich jedoch auf zugangsbeschränkte Inhalte sozialer Netzwerke nicht übertragen. Würde das IT-Grundrecht den Zugriff auf dem technisch vorgesehenen Weg generell nicht umfassen, so entstünden zahlreiche Abgrenzungsprobleme. Es stellte sich dann bspw. die Frage, ob schon das Vorhandensein einer Benutzeroberfläche, ggf. mit speziellen Administratorenfunktionalitäten, ein Zugriff auf technisch vorgesehenem Weg ist. Aktuelle Entwicklungen wie das „Cloud Computing" könnten so schutzlos gestellt werden.[24] Allein die Nutzung eines sozialen Netzwerks kann auch nicht als Grundrechtsverzicht verstanden werden, da durch Beschränkung der Zugänglichkeit gerade der gegenteilige Wille deutlich wird. Dass die Privatsphäre-Einstellungen von sozialen Netzwerken häufig zu weitgehende Standardeinstellungen[25] vorsehen und auch im Übrigen aus verschiedenen Gründen nicht mit den Anforderungen des Datenschutzes im Einklang stehen,[26] kann nicht zulasten der unbefangenen Nutzer gehen. Die im Urteil genannten Schutzbereichsausnahmen für allgemein zugängliche Quellen sind somit nicht auf Inhalte in „privaten" Bereichen sozialer Netzwerke übertragbar. Fraglich ist jedoch, ob die Voraussetzungen des IT-Grundrechts im Übrigen gegeben sind und ob eine täuschungsbedingte Autorisation den Schutz entfallen lässt.

1. Eignung des IT-Grundrechts für die Gefährdungslage „soziales Netzwerk"

Das IT-Grundrecht wurde zum Schutz vor technischer Infiltration durch Trojaner entwickelt. In diesen Fällen sieht das Gericht eine Schutzlücke, im Bereich zwischen Art. 10 Abs. 1 GG und dem Grundrecht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Die Schutzlücke

folge daraus, dass sich Art. 10 Abs. 1 GG einerseits nicht auf Inhalte und Umstände außerhalb der laufenden Telekommunikation erstrecke[27] und andererseits der „Gesamtzugriff" auf die zum Teil zwangsläufig bei der Systemnutzung anfallenden Daten einen „äußerst großen und aussagekräftigen Datenbestand" ohne Notwendigkeit weiterer einzelner Erhebungen ermögliche.[28] Die mit Letzterem angesprochene Gefährdungslage der Enthüllung wesentlicher Teile der Persönlichkeit „auf einen Schlag"[29] liegt auch bei sozialen Netzwerken vor. Wie oben beschrieben, erlaubt der dort verfügbare Datenbestand umfangreiche Rückschlüsse auf Lebensgewohnheiten des Anwenders.[30] Das ergibt sich insbesondere daraus, dass viele der eingestellten Inhalte mit Zeit- und Ortsangaben versehen sind und fortlaufend anfallen. Hinzu kommen die Sichtbarkeit des „Online-Status" und die Ausgabe von z.T. biometrisch gewonnenen „Markierungsvorschlägen" für auf Bildern dargestellte Personen. Gerade vor der Möglichkeit, durch „Umfang und Vielfalt" in einem System enthaltener Daten ein „aussagekräftiges Bild der Persönlichkeit" zu erhalten, soll jedoch das IT-Grundrecht schützen.[31] Auch die „Angewiesenheit" auf die Nutzung,[32] dürfte sich mit zunehmender Verbreitung der sozialen Netzwerke und Verwendung auch in beruflichen Kontexten[33] einstellen. Die „Datenproduktion" ist auch nicht durchwegs von den Nutzern steuerbar. Dies zeigen die ohne Einwilligung überraschend eingeführten biometrischen Bildvorschläge bei Facebook. Der Nutzer kann sie erst nachträglich abstellen. Ebenfalls nachträglich eingeführt wurden anhand der Kontaktliste mit statistischen Mitteln generierte Kontaktvorschläge an Dritte.

Die übrigen Voraussetzungen, die das Gericht für das neue Grundrecht aufgestellt hat, sind offen für neue Technologien und lassen sich auf soziale Netzwerke übertragen. So kann sich die notwendige Komplexität des informationstechnischen Systems gerade aus der Vernetzung ergeben und ist nicht an einen „Apparat" gebunden. Das Erfordernis der Eigennutzung lässt sich auf virtuelle Speicher übertragen. Eine Nutzung durch mehrere Grundrechtsträger im Zusammenwirken ist erfasst, wenn sich Komponenten auswählen lassen, die dem Einzelnen zugeordnet werden können.[34] Bei sozialen Netzwerken lässt sich das dem Nutzer zugeordnete Profil, soweit es die Möglichkeit zur Beschränkung des Zugangs bietet, darunter fassen. Wenn dafür die rechtliche Zuordnung von Belang sein soll,[35] so kann man diese in den einschlägigen datenschutzrechtlichen Vorschriften sehen.

2. Verhältnis zu Art. 10 Abs. 1 GG

Das IT-Grundrecht soll jedoch nicht einschlägig sein, wenn ausschließlich Daten aus einer laufenden Kommunikation betroffen sind, insoweit sei allein Art. 10 Abs. 1 GG maßgeblich.[36] Die in sozialen Netzwerken enthaltenen Informationen verbinden jedoch Inhalte klassischer Kommunikation („point-to-point") mit Informationsangeboten an Personenkreise („point-to-multipoint") sowie eine „Informationsaufbereitung" durch den Anbieter. Die Gefährdungslage ergibt sich somit nicht nur aus dem Einschalten eines technisch nicht kontrollierbaren „Übermittlers", sondern gerade auch aus der multipoligen und potentiell umfassenden Vernetzung der Informationen. Auch können soziale Netzwerke ähnlich einer virtuellen Festplatte zur Ablage von Bilddateien oder zur Terminplanung auch ohne unmittelbaren kommunikativen Zweck verwendet werden.[37] Das mit dem IT-Grundrecht verfolgte Ziel des Schutzes eines bestimmten Lebensbereichs als „Zone der Privatheit"[38] bzw. eines Systems als „Vehikel der Persönlichkeitsentfaltung"[39] lässt sich daher auf die Gefährdungslage sozialer Netzwerke zumindest dann übertragen, wenn der Zugriff nicht als Überwachung „von außen" unter Mitwirkung des Betreibers erfolgt.[40]

Es stellt sich dann allerdings die Frage, ob – entsprechend zu Art. 10 Abs. 1 GG – eine Autorisierung die Eröffnung des Schutzbereichs ausschließt. Das Konzept der Autorisierung lässt sich jedoch nur mit dem auf den technischen Übermittlungsvorgang durch Dritte beschränkten Schutzzweck von Art. 10 Abs. 1 GG rechtfertigen. Wie beschrieben, beschränken sich die Gefährdungen in sozialen Netzwerken nicht hierauf. Geschützt ist nicht allein die Integrität, sondern eben auch die Vertraulichkeit des Systems. Die Unerheblichkeit personengebundener Irrtümer wird damit dem IT-Grundrecht nicht gerecht.[41]

3. Grundrecht auf informationelle Selbstbestimmung

Sofern man die Eröffnung des Schutzbereichs des IT-Grundrechts jedoch ablehnt, stellt sich die Frage, inwieweit das Recht auf informationelle Selbstbestimmung einschlägig ist.[42] Dieses gibt dem Einzelnen „die Befugnis, grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[43] Die Konturierung des Schutzbereichs ist hier besonders problematisch.[44] Im Urteil zur Online-Durchsuchung versucht das BVerfG den Schutzbereich zu präzisieren, indem es ihn auf einzelne Datenerhebungen einschränkt, während der „Gesamtzugriff" auf das System vom IT-Grundrecht erfasst sein soll.[45] Unter diesem „dogmatisch entlastenden"[46] Impetus sind die darauf folgenden Ausführungen zu öffentlich zugänglichen Informationen zu sehen: Deren Kenntnisnahme sei dem Staat grundsätzlich nicht verwehrt. Öffentlich zugänglich sollen Informationen dann sein, wenn sie sich an jedermann oder an einen nicht weiter abgegrenzten Personenkreis richten.[47] Erst gezieltes Zusammentragen, Speichern und Auswerten soll, wenn sich daraus eine besondere

Gefahrenlage für die Persönlichkeit des Betroffenen ergibt, einen Eingriff darstellen.[48] Zu Ermittlungen unter Verwendung fiktiver Identitäten führt das Gericht aus, dass ein Eingriff nicht schon vorliege, wenn sich eine staatliche Stelle unter einer Legende in eine Kommunikationsbeziehung begibt, sondern erst wenn sie schutzwürdiges Vertrauen des Betroffenen in die Identität und Motivation seines Kommunikationspartners ausnutzt.[49] Die „reine Internetaufklärung" bewirke in aller Regel keinen Grundrechtseingriff, da keine Mechanismen zur Überprüfung von Identität und Wahrhaftigkeit des Kommunikationspartners zur Verfügung stünden – dies soll auch für den Fall längerfristiger Kommunikationsbeziehungen in Form „elektronischer Gemeinschaften" gelten.[50]

Diese Vorgaben lassen sich allenfalls auf diejenigen Informationen in sozialen Netzwerken übertragen, die vom Nutzer auch tatsächlich allgemein, d.h. ohne Einschränkung auf einen bestimmten Adressatenkreises zugänglich gemacht wurden. Bei Informationen, für die die Ermittlungsperson erst täuschungsbedingt eine Zustimmung erwirkt, liegt – sofern man nicht schon das IT-Grundrecht für einschlägig hält – in der Regel ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor. Auch die Tatsache, dass eine sichere Authentifizierung in den Netzwerken nicht möglich ist, führt nicht allgemein zu einer Schutzbereichsausnahme. Auch wenn man mit der dem Urteil des BVerfG zugrundeliegenden Literaturansicht[51] davon ausgeht, dass allein ein Registrierungsvorgang noch keinen privaten Bereich begründet, so stellt sich die Situation bei durch Täuschung erlangten Zustimmungen in sozialen Netzwerken doch anders dar. Wenn der Nutzer einem Dritten den Zugang zu seinen Inhalten einräumt, beurteilt er anhand der Umstände und Profilinformationen des Anfragenden dessen Glaubwürdigkeit und Identität. Dies stellt ein „Plus" gegenüber rein automatisierten Schlüssigkeitsprüfungen des Betreibers beim Anmeldevorgang dar. Auch spricht die starke Kontextualisierung und Dauerhaftigkeit der Nutzung des Accounts für ein schutzwürdiges Vertrauen. In sozialen Netzwerken kann im Unterschied faktisch der Eindruck einer nicht-pseudonymen-Kontaktsituation sehr glaubhaft hervorgerufen werden.[52] Deshalb kann nicht pauschal von einem Ausschluss auf Schutzbereichsebene ausgegangen werden.[53] Die Grundrechte haben auch unbefangene und leichtgläubige Nutzer zu schützen. Ermittlungen mittels fiktiver Identitäten in sozialen Netzen können somit durchaus in das Grundrecht auf informationelle Selbstbestimmung eingreifen.

Dies bedeutet jedoch noch nicht, dass sie immer unzulässig wären oder dass es keinen eingeschränkt geschützten öffentlichen Bereich geben kann. Allein, dessen Grenzen müssen präziser und anhand des Einzelfalls bestimmt werden. Abschließend stellt sich dann die Frage, auf welche Rechtsgrundlage die Ermittlungen gestützt werden können.

II. Konsequenzen für die Zulässigkeit und Wahl der Rechtsgrundlagen

Die Antwort der Bundesregierung interpretiert das o.g. Urteil so, dass legendierte Teilnahmen an „offener" Kommunikation in sozialen Netzwerken mangels Grundrechtsrelevanz gestützt auf die Aufgabenzuweisung zulässig sind.[54] Dies verkennt jedoch, dass die „legendierte Teilnahme" gerade dort erforderlich sein wird, wo zum Zwecke der Freigabe privater Bereiche mit der Zielperson Kontakt aufgenommen werden soll. Dann handelt es sich jedoch nicht um „offene Kommunikation". Ist die Information öffentlich zugänglich (also auch ohne Registrierung eines Profils), erübrigt sich das verdeckte Vorgehen. Die §§ 161, 163 StPO sollen hingegen als Rechtsgrundlage dienen, soweit ein anhand äußerer Umstände zu beurteilendes Vertrauen vorliegt, Beurteilungsfaktor sei die technische Möglichkeit pseudonymer Anmeldungen.[55] Wie oben dargestellt würde jedoch ein Schluss allein von der pseudonymen Anmeldungsmöglichkeit der Nutzung sozialer Netzwerke nicht gerecht. Zudem darf nicht der Fehler gemacht werden, die noch bestehenden Defizite sozialer Netzwerke in Bezug auf Authentizität, Transparenz und Gefährdungen für das Persönlichkeitsrecht als Argumente für das Entfallen des grundrechtlichen Schutzes heranzuziehen.[56]

Geht man von einem Eingriff – zumindest in das Grundrecht auf informationelle Selbstbestimmung – aus, so ist zu hinterfragen, ob die Ermittlungsgeneralklauseln, §§ 161, 163 StPO, wirklich eine ausreichende Rechtsgrundlage darstellen. Dies wird in der Literatur teilweise bejaht, wobei die Unterscheidung zwischen öffentlich zugänglichen und abgestuft zugänglichen Inhalten nach Maßgabe der Privatsphäre-Einstellungen in sozialen Netzwerken soweit ersichtlich bisher noch nicht vorgenommen wird.[57] Entsprechend unklar bleibt die Abgrenzung.

Die §§ 161, 163 StPO sind in ihrer jetzigen Fassung eine Reaktion auf die Ausweitung des verfassungsrechtlichen Datenschutzes durch das Grundrecht auf informationelle Selbstbestimmung. Da dessen Beschränkung einer gesetzlichen Grundlage unter Wahrung des Bestimmtheitsgebotes erfordert, gleichzeitig jedoch eine „schwer zu übersehende" Fülle von Einzelregelungen vermieden werden sollte, hat sich der Gesetzgeber dafür entschieden die vormals bloßen Aufgabenzuweisungsnormen der §§ 161, 163 StPO zu Befugnisvorschriften umzuwandeln.[58] Von der traditionellen Methode der Aufzählung einzelner Eingriffsermächtigungen sollte dabei jedoch nicht abgegangen werden, so dass die neuen Generalklauseln nur „begrenzt" und zu weniger gewichtigen bzw. weniger intensiven Eingriffen ermächtigen sollen.[59] Problematisch ist dabei nicht nur die Beurteilung von Gewichtigkeit und Intensität von Eingriffen, sondern auch die Bestimmbarkeit

der Normen.[60] Teilweise wird deshalb der Anwendungsbereich der §§ 161, 163 StPO mittels unterschiedlicher Kriterien erheblich weiter eingeschränkt,[61] oder – mit guten Gründen – auf Nichteingriffe beschränkt.[62]

Wie dargestellt, liegt ein Eingriff in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vor, wenn der Beamte pseudonym die Freigabe von Inhalten „erwirkt". Ein Rückgriff auf die §§ 161, 163 StPO scheitert aber auch wenn man die Kriterien Geringfügigkeit und Intensität anlegt. So erlauben die Inhalte sozialer Netzwerke weitgehende und präzise Rückschlüsse auf die Persönlichkeit. Ist der Ermittelnde einmal im Kreis der Kontakte, kann er die Nutzeraktivität kontinuierlich verfolgen und bspw. Eintragungen von Wohnortwechseln, aktuelle Aufenthaltsorte und Online-Status nachverfolgen. Die Eingriffsintensität kann insoweit nicht als gering angesehen werden. Gegen die Heranziehung der Generalklauseln sprechen auch mitbetroffene Grundrechte Dritter, etwa der Kontakte des Nutzers, deren Informationen ebenfalls zugänglich werden können.[63] Die §§ 161, 163 StPO sind somit keine tauglichen Ermächtigungsgrundlagen für Ermittlungen mittels fiktiver Identitäten in sozialen Netzwerken.[64] Derartige Ermittlungen können jedoch als Annex zu „echten" verdeckten Ermittlungen gem. § 110a StPO gerechtfertigt werden.[65] Daneben sind § 100a StPO und § 98 StPO auf einzelne Kommunikationsinhalte der sozialen Netzwerke anwendbar. Sofern man auch den teilnehmenden Gesamtzugriff und das „Mitlesen" der Inhalte ermöglichen will, ist hierzu eine neue Ermächtigungsgrundlage erforderlich.[66]

III. Zusammenfassung

Es hat sich gezeigt, dass die in sozialen Netzwerken enthaltenen Informationen durch Umfang und Vielfalt weitgehende und fortdauernde Rückschlüsse auf die Persönlichkeit und das Verhalten aktiver Nutzer erlauben. Wegen der kontinuierlich zunehmenden Individualisierbarkeit der Adressatenkreise können die Inhalte nicht pauschal als öffentlich zugänglich erachtet werden. Dies führt dazu, dass die Gefährdungslage bei Ermittlungen in sozialen Netzwerken mit derjenigen einer Online-Durchsuchung vergleichbar ist. Derartige Ermittlungen können deshalb in das IT-Grundrecht – hilfsweise in das Grundrecht auf informationelle Selbstbestimmung – eingreifen. Auch die fehlende Identitätsprüfung bei Anmeldung eines Profils lässt das schutzwürdige Vertrauen zumindest dann nicht entfallen, wenn Inhalte täuschungsbedingt freigegeben werden. Die Ermittlungsmaßnahmen können deshalb nicht auf die strafprozessualen Generalklauseln, §§ 161, 163 StPO, gestützt werden und sind allenfalls unter den Voraussetzungen „echter" verdeckter Ermittlungen gem. § 110a StPO zulässig.

Stefan Drackert
Researcher at the Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany

1 Gemeint sind Internetseiten wie Facebook und Google+, in denen Nutzer in einer Community Kontakte pflegen und Informationen austauschen können. Zu den Begriffen „Social Software" und „Social Networks" vgl. *Alby*, Web 2.0, 3. Aufl., 2008, S. 89 ff.
2 Drs. 17/6587 (Antwort auf eine kleine Anfrage der Fraktion „die Linke"; elektronische Vorabfassung).
3 *Henrichs/Wilhelm*, Kriminalistik 2010, 30–37; *Henrichs/Wilhelm*, Deutsche Polizei Nr. 10 / (2010), 6–12; *Henrichs/Wilhelm*, Kriminalistik 2010, 218–224.
4 Vgl. *Streng*, Jugendstrafrecht, 2. Aufl., 2008, Rn. 1; *Eisenberg*, Kriminologie, 6. Aufl. 2005, S. 763 f.
5 Studie der Forsa im Auftrag des BITKOM, Presseinformation v. 13.4.2011, http://www.bitkom.org/files/documents/BITKOM_Presseinfo_PK_Soziale_Netzwerke_13_04_2011.pdf (zuletzt abgerufen am 18.8.2011).
6 Zur Funktionalität vgl. auch *Art. 29-Datenschutzgruppe*, WP 163, 2009, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf (zuletzt abgerufen: 8.9.2011), S. 4–7.
7 Weitere Anwendungsbeispiele nennen *Henrichs/Wilhelm*, Kriminalistik 2010, 218 ff.
8 Drs. 17/6587, S. 5.
9 Einen solchen ermöglicht in gewissen Grenzen der neue Personalausweis, dazu *Borges*, NJW 2010, 3334. Auf nicht-virtueller Identitätsprüfung basiert hingegen das verbreitete Postident-Verfahren, dazu *Möller*, NJW 2005, 1605. Freilich widersprechen beide Verfahren dem auf schnelles und globales Wachstum ausgelegten Geschäftsmodell der sozialen Netzwerke.
10 Zur Vereinfachung genügt es diesen Fall herauszugreifen. Die verfassungsrechtliche Problematik stellt sich bei der Verwendung der Privatidentität ohne Offenlegung der dienstlichen Funktion ebenso.
11 Hier ausgeblendet bleiben die Herausgabe von Mitteilungen durch den Betreiber sowie der Zugang über Profile Dritter und die Nutzung von anderweitig erlangten Zugangskennungen.
12 Änderungen in Richtung stärkerer Nutzerbestimmung hinsichtlich der jeweiligen Adressaten einzelner Angaben werden gerade umgesetzt: http://www.heise.de/newsticker/meldung/Facebook-renoviert-Datenschutz-Einstellungen-1329378.html (zuletzt abgerufen am 8.9.2011).
13 Vgl. die „Datenverwendungsrichtlinien" in der Fassung vom 19.08.2011, https://www.Facebook.com/privacy/explanation/ . Die Version vom 8.9.2011 enthält bereits die o.g. Änderungen und ist derzeit nur mit einem Facebook-Account abrufbar.
14 http://www.Google.com/support/+/bin/static.py?hl=de&page=guide.cs&guide=1257347&rd=1 (zuletzt abgerufen am 19.08.2011).
15 Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370, 595/07; BVerfGE 120, 274.
16 Antwort auf Frage Nr. 3, Drs. 17/6587, S. 3.
17 *Henrichs/Wilhelm*, Kriminalistik 2010, 222 f; *Bär*, ZIS 2011, 58.
18 BVerfGE 120, 282.
19 BVerfGE 120, 276.
20 BVerfGE 120, 340 f.
21 *Bäcker*, in: *Rensen/Brink* (Hrsg.), Die Vertraulichkeit der Internetkommunikation, 2009, S. 107.
22 BVerfGE 120, 344.
23 So *Bäcker*, in: *Rensen/Brink* (Hrsg.), Die Vertraulichkeit der Internetkommunikation, 2009, S. 129.
24 So auch ebd., S. 129.
25 *Art. 29-Datenschutzgruppe*, WP 163, 2009, http://ec.europa.eu/justice/policies/

privacy/docs/wpdocs/2009/wp163_de.pdf (zuletzt abgerufen: 08.09.2011), S. 8.
26 *Erd*, NJW 2011, 21 f.; vgl. auch *Forgó/Krügel*, F&L 2011, 183.
27 Wie dies bei Online-Zugriff auf gespeicherte Daten und Überwachung der Systemnutzung als solcher der Fall sei, BVerfGE 120, 308.
28 BVerfGE 120, 313.
29 Vgl. *Bäcker*, in: *Rensen/Brink* (Hrsg.), Die Vertraulichkeit der Internetkommunikation, 2009, S. 123.
30 Die Profile geben vielfach ein sehr genaues Bild von der Persönlichkeit der Nutzer ab, vgl. *Stopfer/Back/Egloff*, DuD 2010, 459 ff.
31 BVerfGE 120, 314.
32 BVerfGE 120, 312 f.
33 Vgl. auch die Ausführungen von *Viviane Reding* im Rahmen der Tagung zur Zukunft der Internetinitiative des Europäischen Rates von Lissabon am 2. Februar 2009 in Brüssel: „shift from Web 2.0 for fun to Web 2.0 for productivity and services", http://www.future-internet.eu/uploads/media/reding_future_of_the_internet.pdf (zuletzt abgerufen am 08.09.2011).
34 *Bäcker*, in: *Rensen/Brink* (Hrsg.), Die Vertraulichkeit der Internetkommunikation, 2009, S. 127 f.
35 Ebd., S. 128.
36 BVerfGE 120, 309.
37 Die Entwicklung weist auch bei sozialen Netzwerken zu verstärkter Konvergenz in Richtung des „cloud computing" hin. Beispiel sind die vielfältigen Dienste, die unter dem einheitlichen Google-Account nutzbar sind, z.B. Kalender, virtueller Speicher und eben auch soziales Netzwerk.
38 *Bäcker*, in: *Rensen/Brink* (Hrsg.), Die Vertraulichkeit der Internetkommunikation, 2009, S. 123.
39 *Böckenförde*, JZ 2008, Fn. 119.
40 Zugriffe auf kommunikative Inhalte über den Betreiber sind dann je nach Zielrichtung entsprechend den Regelungen zur Emailbeschlagnahme bzw. Telekommunikationsüberwachung zu handhaben.
41 Weitere Kritikpunkte am Autorisierungskonzept: *Schulz/Hoffmann*, CR 2010, 133.
42 Diese Frage stellt sich unabhängig davon, ob man das IT-Grundrecht generell ablehnt, oder aber den o.g. Beschränkungen auf die Fallkonstellation der Online-Durchsuchung folgt. Zur Kritik am IT-Grundrecht statt vieler: *Eifert*, NVwZ 2008, 521.
43 BVerfGE 65, 43.
44 Vgl. *Albers*, in: *Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle* (Hrsg.), Grundlagen II, 2008, Rn. 68.
45 BVerfGE 120, 313.
46 *Bäcker*, in: *Rensen/Brink* (Hrsg.), Die Vertraulichkeit der Internetkommunikation, 2009, S. 124.
47 BVerfGE 120, 344 f.
48 BVerfGE 120, 345.
49 BVerfGE 120, 345.
50 BVerfGE 120, 345 f.
51 Abgrenzung nach dem „Verteilungsmodus der Zugangsberechtigung". Verlangt wird eine „individualisierende Verifizierung", wobei automatisierte Prüfungen (syntaktische Ebene) nicht ausreichen sollen, vgl. *Böckenförde*, Die Ermittlung im Netz, 2003, S. 205 f., 197.
52 Dies stellt m.E. auch den Unterschied zu Chat-Räumen oder Foren dar, anhand derer das restriktive Erfordernis der Identitätsprüfung mittels eines Merkmals der wirklichen Welt entwickelt wurde, vgl. Ebd., S. 246 ff.
53 In diese Richtung auch *Bäcker*, in: *Rensen/Brink* (Hrsg.), Die Vertraulichkeit der Internetkommunikation, 2009, S. 134 und *Hornung*, CR 2008, 305, der auf die mögliche Stabilität von Kommunikationsbeziehung im Web 2.0 abstellt.
54 Drs. 17/6587, S. 3.
55 Drs. 17/6587, S. 3.
56 Vgl. auch *Petri*, DuD 2008, 448.
57 Etwa *Meyer-Goßner/Schmitt*, StPO, 54. Aufl. 2011, § 100a Rn. 7 m.w.N.; KMR-*Bär*, 2010, § 100a, Rn. 33a, *Bär*, ZIS 2011, 58.
58 Drs. 14/1584, S. 16.
59 Drs. 14/1584, S. 17.
60 Vgl. *Böckenförde*, Die Ermittlung im Netz, 2003, S. 155 ff. Zum Bestimmtheitserfordernis beim Grundrecht auf informationelle Selbstbestimmung: BVerfGE 65, 43; für das IT-Grundrecht: BVerfGE 120, 314.
61 Statt vieler SK-StPO-*Wohlers*, § 161, Rn. 10 ff.
62 *Böckenförde*, Die Ermittlung im Netz, 2003, S. 166.
63 Vgl. auch *Schulz/Hoffmann*, CR 2010, 133.
64 So auch der Bundesdatenschutzbeauftragte im 23. Tätigkeitsbericht (2009/2010) S. 86 sowie mit Bezug auf die polizeirechtlichen Generalklauseln *Petri*, in: *Lisken/Denninger* (Hrsg.), Handbuch des Polizeirechts, 4. Aufl. 2007, S. 936.
65 Dazu *Böckenförde*, Die Ermittlung im Netz, 2003, S. 229 ff., 235, 253 ff.
66 Bei einer konsequenten Auslegung des Begriffs „offene Quellen" entstünden dann allerdings Probleme bei Zugriffen auf ausländische Server, die den Bedarf internationaler Regelungen verdeutlichen. Vgl. Weiterführend: *Graf*, BeckOK StPO, 11. Aufl. 2011, § 100a Rn. 130 ff.; *Bär*, ZIS 2011, 53 ff. sowie *Seitz*, Strafverfolgungsmaßnahmen im Internet, 2004, S. 360 ff.

Procedural Rights of Persons under Investigation by OLAF

Voislav Stojanovski, LL.M.

The budget of the EU for 2010 amounted to over €140 billion, a sum greater than the national budget of 20 of the 27 Member States of the Union for the same year.[1] Such a large amount of money calls for sound financial management and presents a significant risk of fraud and corruption. OLAF is the body tasked with safeguarding the financial interests of the EU. Established in 1999 by a Commission Decision,[2] its main task is to fight illegal activities that could have a detrimental effect upon the EU budget. Although formally a part of the Commission, OLAF enjoys full independence when conducting investigations. It must be noted, however, that in practicing its independence, the Office is accountable to a number of EU bodies. OLAF's accountability can be of a disciplinary, political, auditable, administrative, and judicial nature. Depending on the control mechanism prescribed by primary and secondary EU law, OLAF is answerable to the Commission, the Parliament, the Council, the Court of Auditors, the Supervisory Committee,[3] the European Ombudsman, and the Court of Justice.[4]

I. Nature of OLAF Investigations

According to Regulations No. 1073/99 (EC) and No. 1074/1999 (EURATOM), OLAF has a mandate to conduct external investigations (carried out in the Member States of the EU and in third countries) as well as internal investigations (carried out in all institutions, bodies, offices, and agencies of the EU).[5] In practice, this means that OLAF can investigate both individuals and legal entities (economic operators, NGOs, state agencies and bodies, etc.). Investigations are aimed at preventing corruption, fraud, bribery, or other illegal activity or misconduct that could affect the financial interests of the EU.

With regard to external investigations, OLAF activities consist of on-the-spot inspections and checks, examination of financial transactions and business records, access to and copy of relevant documents, interviews, etc. The Member State on which territory the investigation is taking place must be informed and is obliged to provide assistance if sought by OLAF.[6] With regard to internal investigations, activities include immediate and unannounced access to any information, inspection of accounts, access to and copy or seizure of relevant documents, requests for information, interviews, etc.[7] These activities are aimed at drawing up a report containing OLAF's findings. If there is suspicion of illegal activity by the persons under investigation, the report – depending on the type of investigation – is transferred to either a competent disciplinary EU body or to national judicial, investigative, or administrative authorities of a Member State.

The above-mentioned regulations stipulate that OLAF investigations are strictly of an administrative nature and that they do not affect the powers of the Member States to initiate criminal proceedings. A number of authors have argued, however, that OLAF's investigations go beyond the realm of administrative law and touch upon the area of criminal law and justice.[8] The main arguments that can be raised in this regard are:

- OLAF reports may be used as admissible evidence in subsequent criminal proceedings in the Member States;[9]
- Fraud and corruption are usually criminal offences that entail imprisonment;
- OLAF uses its resources to investigate the most serious cases;[10]
- Two-thirds of the investigations are conducted independently (without assistance by national authorities of the Member States).[11]

Furthermore, if OLAF is indeed an office tasked to carry administrative investigations only, one would expect the majority of its investigators to have forensic accountancy and auditing expertise. In reality, however, the majority of OLAF investigators have a background as lawyers, public prosecutors, and magistrates. This holds true for both the previous and the current Director-Generals. OLAF is also a frequent topic in contemporary criminal law literature.

It cannot be argued, however, that OLAF investigators are either police officers or public prosecutors. First of all, they are not authorised to order or use coercive measures such as restraint, arrest, or detention. If a person who is a subject to an external investigation refuses to cooperate with OLAF, the Office is obliged to ask for assistance from the authorities of the Member State in which the investigation is taking place.[12] Once the final report is prepared by OLAF, it is up to the national authorities of the Member State in question to decide whether it will continue the investigation, initiate administrative or judicial proceedings against the person under investigation, or refrain from taking further action. Reports regarding internal investigations are sent to the competent disciplinary EU body, which is supposed to take appropriate disciplinary or legal action and inform OLAF of the outcome. Additionally, if OLAF considers that the findings in the report after an internal investigation may lead to criminal proceedings, it will transfer the report to the Member State of which the person under investigation is a national.[13]

II. OLAF Investigations and Procedural Rights

From the considerations discussed above, it is evident that OLAF inspections may lead to violations of the rights of persons subject to investigation. Since its establishment, the Office has come under fire, not only by those affected by its investigations (EU staff, private individuals, legal entities, and other third parties) but also by EU bodies authorised to supervise its activities. The way in which OLAF conducts its investigations has been criticised by the Court of Auditors, the Supervisory Committee, and the European Ombudsman. Moreover, the Office has lost a number of cases before the General Court (previously Court of First Instance "CFI"), which has resulted in compensatory damages being awarded to persons whose rights have been violated.

In a Special Report on OLAF prepared in 2005, the Court of Auditors noted that there is no independent control of the legality of investigative actions and recommended that OLAF codify its procedural measures.[14] A Follow-up Report published in 2011 noted that OLAF has accepted the recommendation but is implementing it only partially.[15] In its last Activity Report of 2011, the Supervisory Committee noted that investigations are lengthy, but it could not find an explanation for long periods of inactivity (up to one year in length) by OLAF investigators.[16] Pursuant to an OLAF report in which a journalist was accused of bribery and purchasing confiden-

tial data by an OLAF employee, Belgian authorities decided to search the journalist's office, seizing a large number of his documents. Prior the search, OLAF published a press release accusing an unnamed journalist of bribery. Although the identity of the journalist was not revealed, it was easy to discover who he was, as his newspaper was first to publish the confidential data. Following a complaint addressed to the European Ombudsman by the journalist concerned, the Ombudsman released a Special Report confirming that OLAF went beyond what is proportional and criticising its maladministration.[17]

A number of persons under investigation by OLAF, for which a report was prepared, have initiated proceedings before the CFI and the European Court of Justice (ECJ). In their complaints, they accused OLAF of violating their procedural and defence rights such as the presumption of innocence, data protection, legality and judicial supervision, confidentiality of the investigation, protection of journalistic sources, the right to information, access to the case file, etc. Consequently, many of them have requested annulment of the OLAF report on them as well as compensation for damages resulting from the alleged violations. Requests for annulment of the OLAF report are submitted pursuant to Art. 230 of the Treaty on EU (now Art. 263 of the TFEU), but the ECJ has repeatedly held them inadmissible.[18]

With regard to external investigations, the reasoning of the Court is that the decision by OLAF to transmit a report to national authorities of a Member State is merely a preparatory measure. A final decision is ultimately made by national authorities who are free to decide whether to instigate judicial proceedings or simply disregard the report. The report is to be seen as either a recommendation or an opinion and does not have a legally binding effect. As such, it does not affect the legal position of the person under investigation and is not a formal part of later criminal proceedings before national courts. The situation is similar with regard to internal investigations. The ECJ has held that OLAF investigations are preparatory measures that might not even lead to any proceedings against a civil servant of the EU and are therefore not subject to judicial review.[19] As a result, persons affected by the investigations or the report may only rely on Art. 340 TFEU regarding damages caused by the institutions of the EU or its civil servants.

1. EU Law and Procedural Rights

Art. 2 TFEU states, *inter alia,* that the EU is founded on the values of respect for the rule of law and respect for human rights. Art. 6(3) TFEU stipulates that fundamental rights, as guaranteed by the ECHR and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law. The first paragraph of the same article gives a legally binding character to the Charter of Fundamental Rights of the EU (CFREU), while the second paragraph states that the EU shall accede to the ECHR. The envisaged accession of the EU to the ECHR will be addressed below from the perspective of the possible legal implications it may have for OLAF.

Arts. 47-50 of the CFREU guarantee the procedural rights to effective remedy, fair trial, access to legal aid, and the presumption of innocence. Art. 52 states that in so far as the Charter contains rights that correspond to rights guaranteed by the ECHR, the meaning and scope of these rights shall be the same as those laid down by the said Convention. Furthermore, Art. 41 guarantees the right to good administration, stipulating that every person's affairs with the EU will be handled impartially, fairly, and within a reasonable time by the institutions and bodies of the Union. The latter right includes the right to be heard, the right to access to one's file as well as protection of confidentiality and of professional and business secrecy. It furthermore obliges the administration to give reasons for its decisions, guarantees the right to compensation for damages caused by the EU, and grants to all persons the right to communicate with the Union in one of its official languages.

Only a small number of safeguards exist in secondary EU law. Art. 8 of Regulation 1073/1999 guarantees the protection of confidentiality and personal data. The article states that information forwarded or obtained in the course of internal investigations shall be subject to professional secrecy and its release to persons other than those within the institutions of the EU or to authorities in the Member States whose functions require them to know is forbidden. A Proposal[20] for amendment of Regulation 1073/99 was prepared by the Commission in 2011. 7a and 7b are the most important articles with regard to procedural rights. The first addresses procedural guarantees while the latter envisages a new review procedure, which should offer a semi-judicial overview of the way OLAF conducts its investigations. Arts. 16 and 339 of the TFEU as well as Directive 95/46/EC[21] regarding data protection apply to both external and internal investigations.

Finally, although not legally binding, the OLAF Operation Manual[22] contains a chapter entitled "Individual Rights and Information Duties" that addresses the procedural rights of persons under investigation. It covers the right to be informed as well as defence rights (protection against self-incrimination, legal counsel, the right to use one of EU's official languages, and access to the case file) and envisages an opportunity for the person under investigation to express his views on the facts that concern him. It is interesting to note that, in the latest revision of the Manual, there is an obligation for OLAF investigators to respect the rights enshrined in both the ECHR and the CFREU.

2. Accession of the EU to the ECHR

As the Council of Europe recently noted, EU institutions are "the only public authorities operating in Council of Europe member states that are outside the jurisdiction of the ECtHR."[23] Once the EU accedes to the ECHR, the ECtHR will assume jurisdiction over OLAF investigations regarding their compliance with the procedural guarantees afforded by the Convention. It is to be expected that the question of whether OLAF reports constitute a "criminal charge" as prescribed by Art. 6 ECHR will be brought before the ECtHR. The legal notion of a criminal charge is assessed in an autonomous manner by the ECtHR, and even administrative proceedings[24] can be qualified as criminal.

In the *Engels* case, the ECtHR stated that it is not bound by national qualifications with regard to the type of proceedings; what is of importance is "the very nature of the offence" and "the degree of severity of the penalty that the person concerned risks incurring."[25] Given that fraud and corruption are usually criminal offences that may lead to imprisonment – under the criteria established by the ECtHR – it seems that OLAF investigations might be considered part of a criminal rather than administrative procedure. Such a finding would have tremendous implications for OLAF and the EU. Procedural guarantees contained in Art. 6 ECHR such as the rights to a fair and public hearing, information on the nature and the cause of the accusations, adequate time and facilities for the preparation of the defence, legal counsel, the examination of witnesses, and translation and interpretation will have to be afforded to the persons under investigation. Additionally, the set of directives relating to procedural rights in criminal proceedings already adopted or envisaged for adoption[26] by the EU in the near future will also apply to OLAF. Without venturing into speculation whether this will happen or not, a number of ECtHR cases relating to the rights of persons under OLAF investigation will be discussed below, where appropriate.

3. Presumption of Innocence

The presumption of innocence is one of the most fundamental human rights. It can be found in Arts. 6(2) ECHR and 48(1) CFREU which stipulate that anyone charged with an offence shall have the right to be presumed innocent until proven guilty according to law. In *Franchet and Byk*, a case against OLAF, the CFI stated that the presumption of innocence is breached by statements or decisions which reflect the sentiment that the person is guilty, which encourage the public to believe in his guilt or which influence the assessment of the facts by the competent court.[27] Following an internal investigation, OLAF released a press release implying that the complainants were guilty of a criminal offence before a judgment was passed in their case. Consequently, the CFI found a violation of the right of the complainants to be presumed innocent and ordered the Commission to pay financial restitution and thus compensate the damages for non-material loss caused by OLAF. It would appear that the CFI followed the reasoning stemming from ECtHR case law,[28] in which it is stated that the presumption of innocence can be breached not only by judges, prosecutors, ministers or police officers but also by public officials.

4. Right to be Informed and Heard

Art. 41(2) CFREU stipulates that every person has a right to be heard before any individual measure that would affect him adversely is taken. In the *Hoffman* case, the ECJ noted that observance of the right to be heard requires that, during an administrative procedure, the persons concerned must be afforded the opportunity to make known their views on the truth and relevance of the alleged facts and circumstances and on the documents used by the commission to support its claim that there has been an infringement.[29] Pursuant to Art. 4 of Decision 1999/396,[30] an EU civil servant must be informed that he is under investigation as long as this would not be harmful to the investigation. In the *Franchet and Byk* case discussed above, OLAF transmitted its report to the national authorities, implicating the complainants without first hearing them. As a result, the CFI noted that OLAF committed a sufficiently serious breach of a rule of law conferring rights on individuals[31] and found a breach of Decision 1999/396. In the *Nikolaou* case, the CFI stressed that OLAF must inform a person under investigation of all the facts in his case, either verbally or in writing. Additionally, OLAF is obliged to record any comments that person might make.[32] Given that this was not observed by OLAF, financial damages were awarded to the complainant. The requirement to be informed and heard can be found in Art. 7a of the proposal for amendment of Regulation 1073/99, which follows the reasoning of the CFI discussed above. It requires that information is provided in writing. After an interview has been conducted, a record will be prepared and the person under investigation will be given the opportunity to state whether he approves of it or to add personal observations.

5. Defence Rights

Provisions regarding the rights to defence are to be found in Arts. 41, 42, 47, and 48 CFREU. In the *Michelin* case, the ECJ stressed that the rights of the defence represent a fundamental principle of Community law.[33] In a later case, it was stated that non-observance of the rights of the defence can lead to the imposition of penalties.[34]

a. Principle against self-incrimination

The principle against self-incrimination is a safeguard which protects persons under investigation from self-accusations. Although not specifically contained in the ECHR, the ECtHR has addressed the principle against self-incrimination stating that it is an internationally recognised standard that lies at the heart of the notion of a fair procedure.[35] When determining whether the principle against self-incrimination has been violated, attention should be paid to factors such as the nature and degree of compulsion used to obtain the evidence; weight of the public interest in the investigation and punishment of the offence in issue; existence of any relevant safeguards in the procedure and use to which any material so obtained is put.[36]

The ECJ has also addressed the principle against self-incrimination noting that an economic operator may be compelled to provide all necessary information in its possession but may not be compelled to provide answers which might involve an admission on its part of the existence of an infringement which is a responsibility of the Commission to prove.[37] Art. 7a of the proposal for amendment of Regulation 1073/99 offers protection against self-incrimination.

b. Representation by a legal council

Art. 47 CFREU stipulates that everyone shall have the possibility of being advised, defended, and represented. The ECJ has stated that the rights to legal representation and the privileged nature of correspondence between a lawyer and a client must be respected as from the preliminary-inquiry stage.[38] In its last Activity Report, the Supervisory Committee stated that in practice, OLAF generally offers interested parties the option of being assisted by a person of their choosing.[39] There is currently no case law regarding OLAF and legal representation.

c. Access to the case file

Art. 41(2) states that every person has a right to have access to his file, while the EU must respect the legitimate interests of confidentiality and of professional and business secrecy. In *Imperial Chemical Industries*, the ECJ stated that the right to access to the file is one of the procedural safeguards intended to protect the rights of the defence in all proceedings and circumstances, even if the proceedings in question are administrative.[40] However, in the cases regarding OLAF investigations, EU courts have repeatedly stated that OLAF's independence with regard to its effectiveness and the confidentiality of its mission could be undermined if access to the case file of the person under investigation is granted before the investigation is concluded.[41] The argument once again is that, since the report is not a document adversely affecting the person under investigation, the right of the defence as defined in *Imperial Chemical Industries* does not apply to OLAF investigations.

III. Information Management

As mentioned above, Art. 8 of Regulation 1073/1999 guarantees the protection of confidentiality and personal data with regard to OLAF investigations. In the course of its investigations, OLAF manages data that might be used in the preparation of its reports. Given the particularities of OLAF investigations, the data often contains sensitive information. Besides data management, OLAF frequently transmits information to other bodies of the EU as well as to Member States and third countries.[42] An internal Data Protection Officer is in charge of ensuring adherence to the personal data protection provisions stipulated in Regulation 45/2001.[43]

There are a number of cases in which OLAF has been found to be in breach of personal data protection and other provisions of EU law concerning information management. In the *Nikolaou* case, the CFI found a breach of Regulation 45/2001 after it deduced that OLAF must have leaked information regarding an internal investigation to the press. The CFI concluded that OLAF committed a serious breach of rule of law and that it gravely and manifestly exceeded its limits.[44] The CFI once again found that OLAF had leaked information to the press in the *Franchet and Byk* case. CFI reiterated that the administration must avoid giving the press information concerning disciplinary proceedings that might damage the official concerned and take all necessary measures to prevent any form of dissemination of information that might be defamatory concerning that official.[45] In this case, OLAF was found to be in breach of the principles of confidentiality, presumption of innocence, and good administration. In the *Franchet and Byk* case, the CFI ruled that OLAF should always inform its Supervisory Committee whenever it sends information to Member States so that the Committee can ensure that the procedural rights of the persons under investigation were respected. Informing the Committee must take place before OLAF transmits information to Member States.[46] In its last Activity Report, the Supervisory Committee reported that 28 investigations that required transmission were examined for a period of one year between 2009 and 2010.[47]

IV. Conclusion

It is undeniable that the role of OLAF in the fight against fraud and corruption in the EU is a very important one. Illegal activities against the EU budget from within or outside the EU

can seriously undermine the whole European project. By safeguarding taxpayers' money at EU level, OLAF contributes to the credibility and reputation of the Union. Its independence, however, must be both factual and carefully supervised when it comes to respect for fundamental human rights, which the Office must observe when conducting investigations.

During the first 12 years of its existence, OLAF has been criticised by a number of individuals, legal entities, and EU bodies and institutions to which it is accountable. The length of its investigations and the lack of adherence to procedural rights have been a main cause of concern. It must be admitted, however, that part of that criticism stems from weak legal protection afforded by EU law when it comes to administrative investigations in the field of financial crime. It would appear that striking a balance between fighting serious crime against the EU budget and strong procedural rights is not an area in which the EU legislators have excelled. Although officially "administrative", – from a criminal law perspective – OLAF preliminary inquiries fall in the realm of criminal justice. If a person under investigation is convicted in a criminal trial following a report prepared by OLAF, it becomes apparent that the Office has played a major role in the case and has thus become an integral part of the criminal investigation chain. A fair balance between its particular status and the protection of procedural rights must therefore be achieved – ensuring a balance that would respect the most basic rights as enshrined in the ECHR.

Voislav Stojanovski, LL.M.

PhD Candidate at Masaryk University, Czech Republic; Former trainee at the European Anti-Fraud Office (OLAF).

1 Own comparison, data extracted from The World Factbook 2010 (Field listing: Budget). Washington, DC: Central Intelligence Agency, 2010. URL: https://www.cia.gov/library/publications/the-world-factbook/fields/2056.html.
2 1999/352/EC, ECSC, Euratom, O.J. L 136, 31.5.1999.
3 An internal but entirely independent body empowered with monitoring the way OLAF implements its investigative function.
4 See also Strengthening OLAF, the European Anti-Fraud Office, London: House of Lords, 2004, pp. 18-20.
5 O.J. L 136, 31.5.1999 (See Arts. 3 and 4 in both Regulations).
6 Legal basis of these issues can be found in Regulation No. 2185/96 (Article 2) O.J. L 292, 15.11.1996 and Regulation No. 2988/95, O.J. L 312, 23.12.1995 (Article 9).
7 Art. 4 in both Regulation No. 1073/99 (EC) and Regulation No. 1074/99.
8 See, for example, *Sabine Gleß*/*Helge Elisabeth Zeitler*, Fair Trial Rights and European Community's Fight Against Fraud, European Law Journal, Vol. 7, No. 2, June 2001, pp. 219-237, at 220; *Mariane Wade*, OLAF and the Push and Pull Factors of a European Criminal Justice System, in: eucrim 3-4/2008, p. 129.
9 Art. 8(3) of Regulation No. 2185/96 and Art. 9(2) of Regulation No. 1074/99.
10 Annual Report 2010, Brussels: OLAF, 2010, p. 14.
11 *Ibid*., p. 15.
12 Art. 9 of Regulation 2185/96.
13 Arts. 9 and 10 of both Regulation No. 1073/99 and Regulation No. 1074/99.
14 O.J. C 202, 18.8.2005, para. 83.
15 O.J. C 124, 27.4.2011 (URL link to the Report, p. 37).
16 O.J. C 188, 28.6.2011 (See Annex 6, p. 40).
17 URL: http://www.ombudsman.europa.eu/special/pdf/en/042485.pdf
18 See, for example, Case C-521/04 P(R) *Tillack v Commission*; Case T-215/02 *Gómez Reino v Commission*, and Case T-29/*03 Comunidad Autónoma de Andalucía v Commission*.
19 Case T-215/02 *Gómez Reino v Commission*, para. 62.
20 COM(2011) 135 final, Brussels, 17.3.2011.
21 O.J. L 281, 23.11.1995.
22 URL: http://ec.europa.eu/dgs/olaf/legal/manual/OLAF-Manual-Operational-Procedures.pdf
23 Recommendation 1744 (2006), Strasbourg: Parliamentary Assembly of the Council of Europe, 2006, para. 3.
24 ECtHR *Öztürk v. Germany* 8544/79, 21.02.1984, para. 46-56.
25 ECtHR *Engels and others v. the Netherlands* 5100/71; 5101/71; 5102/71; 5354/72; 5370/72, 8.6.1976, para. 82.
26 Directive 2010/64/EU on the right to interpretation and translation in criminal proceedings (already adopted). Proposals are prepared for a Directive on the right to information in criminal proceedings and a Directive on the right of access to a lawyer in criminal proceedings and on the right to communicate upon arrest). A Directive on communication with relatives, employers, and consular authorities and a Directive on special safeguards for suspected or accused persons who are vulnerable are envisaged.
27 Case T-48/05 *Yves Franchet and Daniel Byk v. Commission*, 8.7.2008, para. 210.
28 See, for example, ECtHR *Butkevičius v Lithuania* 48297/99, 26.3.2002, para. 53.
29 Case 85/76, 13.2.1979, para. 11.
30 Commission Decision of 2 June 1999 concerning the terms and conditions for internal investigations in relation to the prevention of fraud, corruption, and any illegal activity detrimental to the Communities' interests, O.J. L 149, 16.6.1999.
31 *Supra* note 27, para. 156.
32 Case T-259/03 *Nikolaou v. Commission*, 9.12.2003, para. 238, in: *Xavier Groussot/Ziva Popov*, What's wrong with OLAF? Accountability, due process and criminal justice in European anti-fraud policy, Common Market Law Review Vol. 47, pp. 605-643, 2010.
33 Case 322/81 *Michelin v Commission* 9.11.1983, para. 15. See also Case C-328/05 P, 10.5.2007, para. 70.
34 Cases 46/87 and 227/88 *Hoechst AG v Commission*, 21.9.1989, para. 7.
35 ECtHR *John Murray v the United Kingdom* 18731/91, 8.2.1996, para. 45.
36 ECtHR *Jalloh v Germany* 54810/00, 11.7.2006, para. 117.
37 Case 374/87 *Orkem v. Commission*, 18.9.1989 para. 34 and 35.
38 *Supra* note 34, para. 16.
39 *Supra* note 17.
40 Case T-36/91 *Imperial Chemical Industries plc v Commission*, 29.6.1995, para. 69.
41 See, for example, *Franched and Byk* (*supra* note 27), para. 255-262, *Nikolaou* (*supra* note 34), para. 240-246, *Gómez Reino* (*supra* note 19), para. 65.
42 See also *Agnieszka Aleksandra Murawska (Nowakowska)*, Administrative Anti-Fraud Measures within the European Union, Frankfurt/Oder: Nomos, 2007, p. 134.
43 O.J. L 8, 12.1.2001.
44 *Supra* note 32, para. 232.
45 *Supra* note 27, para. 214.
46 *Ibid*., para. 164.
47 *Supra* note 17.

Imprint

Impressum

Published by:

Max Planck Society for the Advancement of Science
c/o Max Planck Institute for Foreign and International Criminal Law
represented by Director Prof. Dr. Dr. h.c. mult. Ulrich Sieber
Guenterstalstrasse 73, 79100 Freiburg i.Br./Germany

Tel: +49 (0)761 7081-0,
Fax: +49 (0)761 7081-294
E-mail: u.sieber@mpicc.de
Internet: http://www.mpicc.de

Official Registration Number:
VR 13378 Nz (Amtsgericht
Berlin Charlottenburg)
VAT Number: DE 129517720
ISSN: 1862-6947

The publication is co-financed by the European Commission, European Anti-Fraud Office (OLAF), Brussels

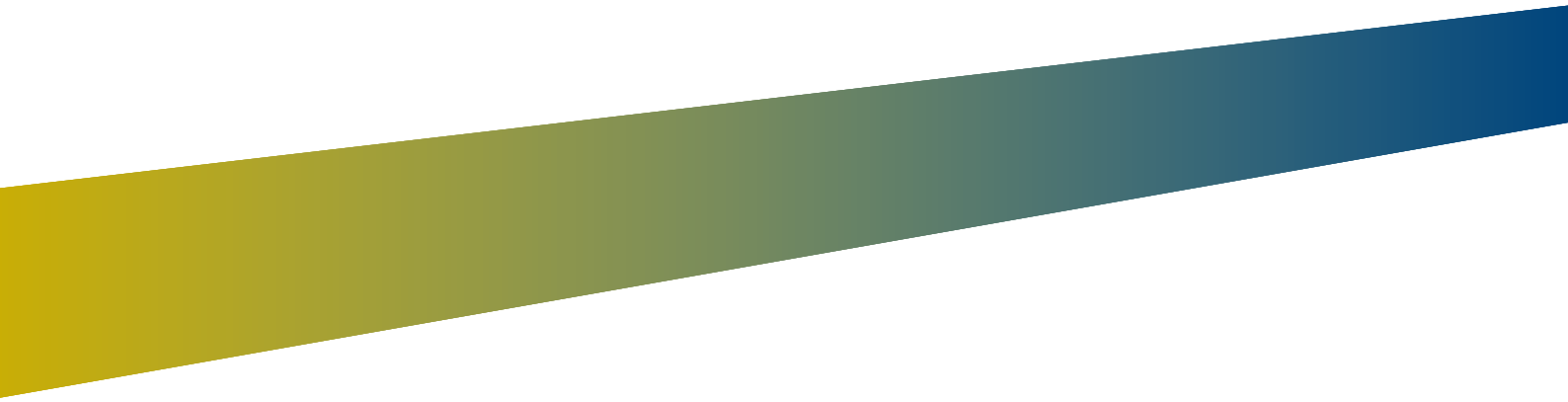
Subscription:
eucrim is published four times per year and distributed electronically for free.
In order to receive issues of the periodical on a regular basis, please write an e-mail to:
eucrim-subscribe@mpicc.de.
For cancellations of the subscription, please write an e-mail to:
eucrim-unsubscribe@mpicc.de.

For further information, please contact:

Dr. Els De Busser
Max Planck Institute for Foreign and International Criminal Law
Guenterstalstrasse 73,
79100 Freiburg i.Br./Germany

Tel: +49(0)761-7081-256 or +49(0)761-7081-0 (central unit)
Fax: +49(0)761-7081-294
E-mail: e.busser@mpicc.de

The European Criminal Law Association is a network of lawyers' associations dealing with European criminal law and the protection of financial interests of the EU. The aim of this cooperation between academics and practitioners is to develop a European criminal law which both respects civil liberties and at the same time protects European citizens and the European institutions effectively. Joint seminars, joint research projects and annual meetings of the associations' presidents are organised to achieve this aim.



Max-Planck-Institut
für ausländisches und
internationales Strafrecht