eucrim
2012 / 4
THE EUROPEAN CRIMINAL LAW ASSOCIATIONS' FORUM

Focus: Organised Crime
Dossier particulier: Criminalité organisée
Schwerpunktthema: Organisierte Kriminalität

Guest Editorial
Michèle Coninsx

Addressing Organised Crime in Fraud Cases
Deniz Genç

The Evolving Structure of Online Criminality
Dr. *Tatiana Tropina*

Anti-Money Laundering: New Obligations Imposed by the 2012 Guardia di Finanza Circular in Italy
Dr. *Maria Cristina Bruno*

Legal Nature of European Union Agricultural Penalties
Dr. *Justyna Łacny* / Dr. hab. *Monika Szwarc*

2012/4 ISSUE / ÉDITION / AUSGABE

Contents

News*

European Union

Foundations
142 Enlargement of the EU
143 Schengen

Institutions
143 Commission
143 European Court of Justice (ECJ)
144 OLAF
144 Europol
145 Eurojust
146 Frontex

Specific Areas of Crime / Substantive Criminal Law
147 Protection of Financial Interests
148 Organised Crime
149 Illegal Online Gambling
149 Cybercrime

Procedural Criminal Law
150 Data Protection
151 Freezing of Assets

Cooperation
151 Police Cooperation
151 Judicial Cooperation

Council of Europe

Foundations
152 Reform of the European Court of Human Rights
152 Other Human Rights Issues

Specific Areas of Crime
152 Corruption
153 Money Laundering

Procedural Criminal Law

Legislation

Articles

Organised Crime

154 Addressing Organised Crime in Fraud Cases – Developing a More Efficient Legal Framework
Deniz Genç

158 The Evolving Structure of Online Criminality. How Cybercrime Is Getting Organised
Dr. *Tatiana Tropina*

165 Anti-Money Laundering: New Obligations Imposed by the 2012 Guardia di Finanza Circular in Italy
Dr. *Maria Cristina Bruno*

170 Legal Nature of European Union Agricultural Penalties. Comments on the ECJ Ruling in Case C-489/10 Ł. Bonda
Dr. *Justyna Łacny* /
Dr. hab. *Monika Szwarc*

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.

Guest Editorial

Dear Readers,

I am very pleased to introduce this issue of eucrim, devoted to the fight against organised crime – a very complex criminal phenomenon covering a wide range of serious offences threatening the security and fundamental rights of EU citizens, the proper functioning of business and public institutions, and the solvency of the economy and financial markets.

To tackle organised crime and bring criminals to justice, competent authorities of Member States and EU agencies need to work together, align their actions, and ensure complementarity. Eurojust's core tasks, ensuring proper cooperation and coordination, contribute to these goals, resulting in swiftly executed MLA requests, simultaneous execution of EAWs, and the setting up of Joint Investigation Teams. Eurojust's coordination meetings and operational coordination centres bring together both law enforcement and judicial authorities, allowing streamlined, immediate, and targeted action to dismantle organised criminal networks and convict the criminals involved.

In a case concerning Bulgaria and Greece, coordination meetings organised by Eurojust led to identification of a criminal network's members residing in both Member States and ensured their simultaneous detention in Greece through execution of EAWs issued by the competent Bulgarian authorities. As a result, the victims, pregnant Bulgarian women forced to travel to Greece to give up their newborn babies for adoption to Greek couples, were freed, and their testimonies were used as evidence before the Greek court.

Two goals of Eurojust's action plan against trafficking in human beings 2012–2016 are to increase the number of investigations and prosecutions of THB cases and to enhance judicial cooperation in this area.

Freezing and confiscation of proceeds of crime are essential tools in the fight against organised crime. Efficient recovery of criminal assets is indispensable to prevent and combat money laundering activities, the financing of other criminal activities, and infiltration of the common market. However, experience shows that international judicial cooperation in these areas is often hampered by differences between legal systems and the unsatisfactory implementation of EU instruments. The need for common instruments applicable in all Member States and further harmonisation of substantive criminal law is evident. In addition, a multidisciplinary approach amongst police as well as administrative and judicial authorities is required.

Michèle Coninsx

Protecting the EU's financial interests, especially in times of economic crisis, is a clear priority. In this context, the Lisbon Treaty creates new opportunities. It provides the possibility for Eurojust to strengthen judicial cooperation by resolving conflicts of jurisdiction and having the competence to initiate criminal investigations. Subsequently, it opens the door for a European Public Prosecutor's Office "from Eurojust," fostering the further development of a European area of freedom, security and justice.

Increasing information flow and strengthening ties with the national authorities in the Member States are both key elements for efficient cooperation and an effective fight against organised crime. The 2008 Council Decision on Eurojust has responded to these needs by establishing Eurojust National Coordination Systems in the Member States, enabling the detection of links between organised crime cases. The need for close cooperation equally applies with regard to non-EU Member States, as organised crime does not stop at the EU borders.

Organised criminals stick together, are driven by profit, and are proficient in creatively bypassing law enforcement and judicial efforts. Hence, if we want to be effective in our fight, we need to work together in going after their money and should be creative in doing so as well.

Michèle Coninsx,
President of Eurojust

European Union*

Reported by Dr. Els De Busser (EDB), and Cornelia Riehle (CR)

Foundations

Enlargement of the EU

Commission Adopts Enlargement Package

On 10 October 2012, the European Commission adopted the so-called enlargement package. Each year, the Commission adopts this set of documents, which clarify its enlargement strategy and the progress made by candidate countries and potential candidate countries.

The Commission recommended starting accession negotiations with the Former Yugoslavian Republic of Macedonia, as the country has been implementing significant reforms. The start of a High Level Accession Dialogue with the Commission in March 2012 further accelerated reforms, e.g., improvement of the legislative framework for elections and the decriminalisation of defamation.

With regard to Albania, the Commission recommended granting the country the status of candidate country due, inter alia, to its substantial progress on four key priority areas: the functioning of parliament, the adoption of laws requiring reinforced majority, the appointment of the Ombudsman and the hearing and voting processes for key institutions, and the modification of the legislative framework for elections. However, the status of candidate country is still subject to completion of key measures in the areas of judicial and public administration reform as well as revision of the parliamentary rules of procedure. Albania's continuing efforts in the fight against corruption and organised crime will also be monitored.

Kosovo is confirmed as being almost ready for opening negotiations for a Stabilisation and Association Agreement (SAA). Therefore, a feasibility study is part of the Commission's enlargement package. This study assesses Kosovo's progress in fulfilling the political, economic, and legal criteria for the Stabilisation and Association Agreement. Kosovo needs to demonstrate its preparedness to implement specific reforms in four areas before the Commission can propose negotiating directives for an SAA: rule of law, public administration, protection of minorities, and trade.

Serbia obtained the status of candidate country on 1 March 2012 and is doing well in sufficiently fulfilling the political criteria and conditions of the stabilisation and association process. Nonetheless, the key issue in this process is its relations with Kosovo. The Commission stated that progress on this priority is required in order to further the negotiations.

For the first time since the opening of the accession negotiations, a progress report on Montenegro was included in the enlargement package. The candidate country still needs to make further efforts in the area of rule of law, in particular finalising the ongoing constitutional reform and bringing about stronger judicial independence. Additionally, Montenegro needs to continue implementation of legislation, especially with regard to corruption and organised crime.

While Iceland is making excellent progress, the Commission is less positive for Bosnia and Herzegovina as functional, coordinated, and sustainable institutional structures have not yet been built. Through the High Level Dialogue on the Accession Process, the EU continues to support the country's efforts. With regard to candidate country Turkey, concern remains regarding respect for fundamental rights, in particular freedom of the media.

The Republic of Moldova is not a potential candidate country yet and was not included in the enlargement package. Commissioner Štefan Füle declared on 24 September 2012, however, that Moldova is taking meaningful steps to

* If not stated otherwise, the news reported in the following sections cover the period October–December 2012.

come closer to the EU politically and economically. (EDB)
➤eucrim ID=1204001

Schengen

Negotiations on Establishing European Border Surveillance System

On 24 October 2012, the Council of the EU mandated the Cyprus presidency to start negotiations with the Commission and the EP on the proposal to establish EUROSUR, the European Border Surveillance System. The mechanism aims at enabling operational information-sharing between the competent Member States' authorities. Additionally, the objective is for these authorities to cooperate both with each other and with Frontex for the purpose of detecting, preventing, and combating illegal migration and cross-border crime and to contribute to the better protection of migrants.

In spite of a number of Member States having reservations, the Cyprus presidency hopes to overcome them and make progress with the proposal. Since the EP's LIBE Committee voted in favour of the EUROSUR proposal on 27 November 2012, negotiations will be starting soon. (EDB)
➤eucrim ID=1204002

Schengen Accession for Bulgaria and Romania – State of Play

For quite some time the accession of Bulgaria and Romania to the Schengen zone has been pending (see eucrim 1/2012, p. 3). The decision has not been taken because the required unanimity was not reached.

A two-step approach is currently proposed: in a first step, checks on persons would be abolished at internal sea and air borders with and between Bulgaria and Romania, which goes hand in hand with the two countries fully joining the SIS. In a second step, the checks on persons at internal land borders would be lifted. A decision on both countries joining Schengen, however, has again been postponed.

In the meantime, the Council welcomed the progress made by both countries under the Cooperation and Monitoring Mechanism, which will stay in place. (EDB)
➤eucrim ID=1204003

Institutions

Commission

Commission Work Programme for 2013

On 23 October 2012, the Commission presented its work programme for 2013, starting with the highest priority – the economic crisis. Besides establishing a genuine economic and monetary union, building a safe and secure Europe is one of the other objectives.

In the light of this objective, the Commission is prepared to fill in the missing links, e.g., establishing a European Public Prosecutor's Office to fight against crimes affecting the EU budget and protect its financial interests, fight trafficking in firearms, strengthen judicial cooperation in criminal matters, revise legislation on nuclear safety, and propose new legislation on nuclear insurance and liability. With the Citizenship Report, the Commission ultimately plans to review progress made in ensuring that EU citizens can readily exercise their rights and identify future action. Other plans include new arrangements for Schengen governance, an anti-corruption report and the first judicial scoreboard monitoring progress, and identification of best practices. (EDB)
➤eucrim ID=1204004

European Court of Justice (ECJ)

General Court Judgment in Al-Aqsa Case Annulled by Court of Justice

Since 2003, the Dutch Al-Aqsa foundation has been involved in a legal battle against their inclusion in the Council list of persons and entities whose assets have been frozen as a measure in the fight against terrorism (see eucrim 4/2010, p. 141). Several judgments have annulled successive Council decisions to include or retain the foundation in the list. The last judgment in this case was pronounced by the General Court in 2010, and it annulled a number of Council decisions to include Al-Aqsa in the terrorist list. These decisions were based on Dutch terrorism regulation that was later repealed and therefore triggered the annulment of the Council decisions. Both Al-Aqsa and the Netherlands have appealed this judgment (joined cases C-539/10 P and C-550/10 P).

The appeal by Al-Aqsa sought amendment of the reasoning of the judgment and was therefore dismissed by the Court of Justice. The appeal by the Netherlands was based on the General Court erring in law, as the Dutch terrorism regulation had not been repealed due to its content or consequences for Al-Aqsa. The regulation was repealed because of its overlap with EU Regulation 2580/2001 and, in accordance with the TFEU, Member States should refrain from adopting national provisions that are parallel to EU legal instruments. Thus, the Court of Justice annulled the General Court's judgment and, in a final judgment, dismissed the initial action brought by Al-Aqsa on the following grounds. First, according to the Court, there was enough evidence for the Council to include Al-Aqsa in the list, and the Council had not failed to comply with its obligation to review the grounds justifying the decision to freeze the assets. It finds that the repeal of the Dutch terrorism legislation as such was not sufficient to render the maintenance of Al-Aqsa in the list incompatible with EU law. Second, the Council's decisions do not infringe Al-Aqsa's right to property and, finally, the argument that the Council's decision does not satisfy the duty to state reasons for including them in the list was also rejected. (EDB)
➤eucrim ID=1204005

President of the Court of Justice Re-Elected

Mr. Vassilios Skouris has been re-elected President of the Court of Justice of the EU for the period from 9 October 2012 to 6 October 2015.

Mr. Skouris has been President of the Court since 2003, after being a judge at the Court since 1999. His re-election follows the replacement of some Members of the Court of Justice. (EDB)

➤eucrim ID=1204006

OLAF

OLAF's Press Statement Regarding Commissioner Dalli

On 19 October 2012, OLAF issued a press statement regarding the investigation into alleged bribe requests to obtain the lifting of the EU ban on snus (a tobacco product that has been illegal in the EU for a long time). The press statement follows media reports on the possible involvement of Commissioner Dalli in this case.

OLAF states that its investigation revealed that requests for payment from the snus industry were made by a Maltese entrepreneur using Commissioner Dalli's name in exchange for a legislative proposal lifting the ban on this product. The snus industry declined and no payments were made. The OLAF investigation did not find evidence of the direct involvement of Commissioner Dalli. In accordance with OLAF Regulation 1073/99, the case has been transferred to the national Maltese authorities.

OLAF also states that Commissioner Dalli had taken no action to prevent or dissociate himself from the facts, even though circumstantial pieces of evidence indicate that he was aware of the use of his name and position for the purpose of financial gain. Therefore, OLAF has referred the case to the Commission's President.

As the matter is under consideration by the competent authorities, OLAF decided not to deliver further comments on details of the investigation. (EDB)

➤eucrim ID=1204007

Europol

New Europol Review 2011 Published

On 28 September 2012, Europol released its Europol Review for the year 2011. The Europol Review is essentially Europol's annual report reviewing the work Europol carried out and the results achieved in 2011.

The report consists of five chapters dealing with Europol's organisational structure, its work, its operational activities, its reach, and, ultimately, Europol's way ahead. From an organisational perspective, the most important event in 2011 is seen as Europol's move into its new headquarters.

Regarding its work in 2011, Europol has continued to develop new and modern collaboration tools such as the Europol Platform for Experts (EPE), Europol's Network of Advisory Teams (EuNAT), and its 24/7 operational centre that, in 2011, increased its operational support services, up 17% from the year 2010.

The priorities of Europol's operational activities in 2011 included the fight against drug trafficking, trafficking in human beings, intellectual property crime, cigarette smuggling, Euro counterfeiting, VAT fraud, money laundering and asset tracing, mobile organised criminal groups, outlaw motorcycle gangs, and terrorism. Furthermore, the European Cybercrime Centre (EC3) was established in 2011 (see eucrim 2/2012, p. 57).

Common abbreviations

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
CONT	Committee on Budgetary Control
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
(M)EP	(Members of the) European Parliament
EPO	European Protection Order
EPPO	European Public Prosecutor Office
FATF	Financial Action Task Force
FT	Financing of Terror
GRECO	Group of States against Corruption
GRETA	Group of Experts on Action against Trafficking in Human Beings
JHA	Justice and Home Affairs
JIT	Joint Investigation Team
JSB	Joint Supervisory Body
LIBE Committee	Committee on Civil Liberties, Justice and Home Affairs
(A)ML	Anti-Money Laundering
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
OSCE	Organisation for Security and Cooperation in Europe
SIS	Schengen Information System
SitCen	Joint Situation Centre
TFEU	Treaty on the Functioning of the European Union

Looking at Europol's reach in 2011, it has not only maintained a live 24/7 connection with the Europol national units in all 27 EU Member States and organised regular awareness and training events but, additionally, Europol has cooperated with 18 non-EU countries, nine EU bodies and agencies, and three other international organisations.

With a view to the envisaged impact assessment by the European Commission and the future proposal for a Europol Regulation to replace the 2009 Europol Council Decision, in 2011, Europol's Management Board initiated an evaluation of Europol's implementation of its 2009 Council Decision and activities. (CR)

➤eucrim ID=1204008

Europol Access to EURODAC: Presidency Note

On 21 September 2012, the Cypriot Presidency sent a note to the JHA Council explaining the need for Europol to be able to request comparison with Eurodac data for the purposes of preventing, detecting, and investigating terrorist offences and other serious criminal offences.

According to the Cypriot Presidency, this need is based on two main concerns: firstly, Europol's role as the EU criminal information hub; and, secondly, its role in protecting victims of labour and sexual exploitation.

The Presidency argues that Europol's role as the EU criminal information hub – that allows Europol to cross-match information, including fingerprint data, received from different Member States, third countries, international bodies, private parties and to combine it with its own analysis – puts Europol in the position to get indications proving reasonable grounds to consider that a comparison with Eurodac data would lead to the identification of a victim or suspect of serious crime. An individual Member State, however, might not become aware of these indications as not all information collected, analysed, and cross-matched at Europol is directly shared with all Member States. Furthermore, access to Eurodac by Europol would help prevent the abuse of the asylum system by organised criminal networks from third countries trying to bring criminal members of the network into an EU Member State. If Europol could compare the fingerprint data of these criminal members with EURODAC data, it could detect false identities used by these members. Since organised criminal groups and human traffickers also abuse the asylum system to bring victims of labour or sexual exploitation into the EU, the Presidency further argues that Europol could identify these victims or traffickers by comparing the data received from the Member States with Eurodac data. (CR)

➤eucrim ID=1204009

Europol Access to EURODAC: Opinion of the JSB

On 10 October 2012, Europol's Joint Supervisory Body (JSB) published its Opinion on Europol's access to EURODAC data. The main concern of the JSB is the necessity of such access. According to the JSB, no verification has been given so far that Europol's access to EURODAC data would be needed.

Hence, the JSB recommended the following:

- to show that it is necessary for Europol to access Eurodac;
- not to give Europol greater access to Eurodac data than the Member States have, in order to prevent Member States without access to Eurodac data from circumventing the law;
- to introduce the obligation to guarantee independent verification;
- to introduce the condition that there should be a substantiated suspicion that the perpetrator has applied for asylum;
- to include conditions to make sure that access to Eurodac is proportionate;
- not to allow the comparison of fingerprints with Eurodac data for analysis of a general nature and of a strategic type;
- to exclude the possibility for Europol to access Eurodac data for criminal acts that are "so reprehensible that it justifies querying databases registering persons with a clean criminal record;"
- to introduce an obligation for Europol to inform the originator of the data when data appear to be inaccurate;
- to ensure that relevant records will be available for the JSB and the national data protection supervisory authorities;
- to state that the processing of data by Europol shall be supervised by the independent joint supervisory body;
- to further assess the question of when Europol and the Member States may not inform a third State or international organisation – with whom they are jointly investigating a specific crime – on the results of a Eurodac comparison. (CR)

➤eucrim ID=1204010

Computer-Based Scam Using Europol's Logo

On 12 October 2012, Europol had to publish a warning concerning the misuse of its logo through a new variant of a computer-based scam using a police ransomware malware. If a PC is infected, it seizes up and a warning window using Europol's logo is displayed stating that the victim's IP address was identified as having been used for illegal activities such as downloading copyrighted material. To unlock the computer, the victim is instructed to pay a "fine" using various online money services.

Persons that have already been deceived into paying money are advised to make a report to their local police agency.

An information sheet with tips and advice to prevent police ransomware is also available on Europol's website. (CR)

➤eucrim ID=1204011

Eurojust

Trafficking in Human Beings: Final Report and Action Plan Published

In October 2011, Eurojust and Europol signed a Joint Statement to address trafficking in human beings (THB) in a co-

ordinated, coherent, and comprehensive manner. In 2012, Eurojust developed a strategic project titled "Eurojust's action against trafficking in human beings." On 18 October 2012, Eurojust presented its Final Report and Action Plan for this project.

The report presents the main findings of the project, including the main difficulties in the investigation and prosecution of THB cases and the main tools that are proposed to address the identified problems. According to the report, the main problems in THB cases stem from, for instance, high evidentiary requirements, problems with identification of THB cases and victims, the multilateral dimension of THB cases, the lack of knowledge and experience in THB cases, and difficulties with obtaining asset recovery. Looking at the main tools, the report sees advantages in using Eurojust, Europol, and JITs.

The Action Plan against THB for the years 2014-2016 that is presented at the end of the report identifies the following priorities:

- to enhance information exchange to get a better intelligence picture at the EU level in the field of THB;
- to increase the number of detections, joint investigations, and prosecutions in THB cases as well as to enhance judicial cooperation in this area;
- to improve coordination mechanisms, in particular for training, expertise, and operational activities,
- to increase cooperation with third states in THB cases;
- to use alternative approaches, e.g., multidisciplinary approaches to combat human trafficking;
- to disrupt criminal money flows and asset recovery in THB cases. (CR)

➤eucrim ID=1204012

Judicial Cooperation in Criminal Matters with EU Southern Neighbours

On 28 September 2012, Eurojust sent a note to the Working Party on Cooperation in Criminal Matters about the current practical and legal issues, obstacles, and best practices in the field of judicial cooperation in criminal matters between the EU Member States and the southern neighbours of the EU, namely Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestinian Authority, Syria, and Tunisia.

The note consists of four points:

- First, a summary of the current legal and practical issues, obstacles, and best practices regarding mutual legal assistance, extradition, transfer of criminal proceedings, and transfer of sentenced persons between the EU Member States and the southern neighbours of the EU;
- Second, an overview of the legal basis applicable in these four areas of judicial cooperation in criminal matters between each EU Member State and each southern neighbour of the EU;
- Third, statistics on requests concerning the four areas of judicial cooperation in criminal matters issued to and received by each Member State with respect to each southern neighbour of the EU;
- Possible further steps.

Furthermore, the note includes an overview on the applicable legal bases in the field of judicial cooperation in criminal matters between each EU Member State and each Southern neighbour of the EU as well as a questionnaire addressed to the EU Member States, asking for their legal frameworks, legal and practical issues, obstacles, and the best practices identified when cooperating with these southern neighbours.

The note and the results of the questionnaires served as the basis for a Strategic Seminar on Judicial Cooperation in Criminal Matters between the Member States and the southern neighbours of the EU organised by Eurojust and the Cyprus Presidency in Limassol on 3-5 October 2012. The seminar brought together experts from the 27 Member States, high-level judicial experts from the southern neighbour states of Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestinian Authority, and Tunisia, liaison magistrates, and representatives from the European Commission and Frontex. (CR)

➤eucrim ID=1204013

Newsletter on the Fight against Cybercrime Published

The seventh issue of the Eurojust News, published on 7 November 2012, is dedicated to the fight against cybercrime.

The newsletter contains articles on the phenomena of cybercrime and European countermeasures against cybercrime. Furthermore, the issue contains an article on the European Cybercrime Centre (EC3) that will open as of 11 January 2013 as well as an interview with the Director of the EC3 and Assistant Director of Europol, Mr. Troel Oerting.

According to the newsletter, the number of cybercrime cases addressed by Eurojust in the period 2004-2012 increased from 0 cases in 2004 to 34 cases registered between January and September 2012. (CR)

➤eucrim ID=1204014

Frontex

First Fundamental Rights Officer Designated

On 27 September 2012, the Frontex Management Board designated Ms. Inmaculada Arnaez Fernandez as the Agency's first Fundamental Rights Officer. The Fundamental Rights Officer will monitor and report to the Consultative Forum, Management Board, and the Executive Director of Frontex. The Officer is independent in the performance of her duties and has access to all information concerning respect for fundamental rights in relation to all activities of the Agency.

Ms. Arnaez is a Spanish lawyer with fifteen years of experience in fundamental rights, humanitarian law, and international relations. She is currently working on rule-of-law matters at the OSCE Office for Democratic Institutions and Human Rights. (CR)

➤eucrim ID=1204015

Inaugural Meeting of the Consultative Forum on Fundamental Rights

On 16 October 2012, Frontex' newly created Consultative Forum on Fundamental Rights held its inaugural meeting at the Frontex headquarters in Warsaw.

The Forum is a new body to enable Frontex and its Management Board to gain information and advice on the promotion and respect of fundamental rights in all Frontex activities.

The Forum's role is advisory; it has no decision-making powers. It will deliver an annual report on Frontex' implementation of its fundamental rights obligations. Organisations represented in the Consultative Forum include the folowing:

- Amnesty International European Institutions Office;
- Caritas Europa;
- Churches' Commission for Migrants in Europe;
- Council of Europe;
- European Asylum Support Office;
- European Council for Refugees and Exiles;
- European Union Agency for Fundamental Rights;
- International Catholic Migration Commission;
- International Commission of Jurists;
- International Organization for Migration;
- Jesuit Refugee Service;
- Office for Democratic Institutions and Human Rights;
- Platform for International Cooperation on Undocumented Migrants;
- Red Cross EU Office;
- United Nations High Commissioner for Refugees.

At the inaugural meeting, the Forum elected its first two co-chairs: Ms Aydan Iyigüngör of the European Union Agency for Fundamental Rights and Stefan Kessler of the Jesuit Refugee Service. The co-chairs will serve for one year, representing EU agencies and NGOs respectively. (CR)

➤eucrim ID=1204016

Working Agreement with EASO

On 26 September 2012, Frontex and the European Asylum Support Office (EASO) signed a Working Arrangement to formalise their cooperation and to set up a framework for closer cooperation in future.

To guarantee closer coordination of the activities of Frontex and EASO regarding the reception of migrants at the EU's external borders and the identification of those in need of international protection, the Working Arrangement foresees the following measures:

- Cooperation and coordination of the agencies' assessments and operational responses when assisting Member States, in particular in view of deployment of European Border Guard Teams and/or Asylum Support Teams;
- Cooperation to develop methods to better identify those in need of international protection in the context of mixed migration flows;
- Exchange of information on the profiles and compositions of expert pools as well as on best practices for the functioning of those pools;
- Exploration of the possibilities to establish common or mixed teams of specialists in border management and asylum experts;
- Exchange of best practices and methodologies on data collection and exchange as well as on information-gathering and the production and sharing of statistics and analyses;
- Participation in establishing and implementing specific mechanisms for joint third country monitoring;
- Consultations on the development of training materials, training strategies and plans, and exploration of the possibilities for mutual participation in training activities. (CR)

➤eucrim ID=1204017

Increased Funding

Against the background of Frontex' new tasks, as required under its amended Regulation (see eucrim 1/2010, pp. 9-10, eucrim 1/2011, p. 6, eucrim 2/2011, p. 56, and eucrim 4/2011, p. 141), the Commission published on 23 October 2012 a communication calling for increased funding for Frontex.

According to the communication, a cumulative number of 12 new posts are needed for the Agency with estimated costs amounting to €1.32 million. However, the impact of these costs on the Agency's expenditure in 2013 shall be budget-neutral since the plan is to offset the expenditure against decreasing expenditure related to seconded national experts (SNE) currently performing these tasks and whose relevant posts will be gradually phased out in the course of 2013. The remaining costs shall be met by additional savings. The new posts needed include, for instance:

- a Fundamental Rights Officer;
- six Frontex Coordination Officers for a European Border Guard Team operations and projects;
- one Product and Change Management Officer to develop and operate the information exchange system for ICONET (Information and Coordination Network for Member States' Migration Management Services), classified data, secure information exchange channels and FOSS replacement (Frontex Information exchange web portal – Frontex One Stop Shop), also including the transmission of personnel data to other EU agencies. (CR)

➤eucrim ID=1204018

Specific Areas of Crime / Substantive Criminal Law

Protection of Financial Interests

Council Conclusions on Communication on Tax Fraud and Tax Evasion

On 13 November 2012, the Council adopted conclusions on the Commission's Communication on tax fraud and tax evasion of 27 June 2012 (see eucrim 3/2012, pp. 99-100).

In its conclusions the Council listed the issues that it considers to be priorities. In the field of direct taxation, they include progress on savings agreements with third states (see eucrim 2/2012, p. 56), better information exchange between administrations, and examining the intensification of administrative cooperation. In the field of indirect taxation, priorities include making further progress in effectively combating tax evasion and improving the information exchange between administrations. Administrative and criminal sanctions as well as joint audits are not considered a priority by the Council. (EDB)
➤eucrim ID=1204019

Court of Auditors Tells Member States and Commission to Manage Spending Better

On 6 November 2012, the European Court of Auditors released its annual report on the EU budget and how it was spent in 2011. In that year, the EU spent €129.4 billion, 80% of which was for agriculture and cohesion policies.

According to the Court of Auditors, the control systems that the Member States and the Commission implemented to avoid irregularities in payments have only been partially effective. National authorities should be more committed to managing and controlling EU spending.

The Court's President Vítor Caldeira, stated that the 2011 report was consistent with previous reports in that Member States must implement better rules on how EU money is spent. Both the Member States and the Commission are responsible for implementing their better enforcement. (EDB)
➤eucrim ID=1204020

Organised Crime

Market Abuse Directive – State of Play

The EP Committee on Economic and Monetary Affairs discussed the Market Abuse Directive on 9 October 2012. EU-wide criminal sanctions, including prison terms, should be introduced to avoid future market abuse from insider dealing and market manipulation.

At the present time, definitions of the offences and sanctions applied for these forms of crime are still very different, enabling fraudsters to operate in the state having the most lenient system. For this reason, MEPs want to impose a maximum prison sentence of at least five years for the most serious forms of market abuse, e.g., the intentional use of information to acquire or dispose of financial instruments. Two years of imprisonment should be the maximum sentence for less serious offences, e.g., disclosure of insider information or the intentional use of information for recommendations to acquire or dispose of financial instruments. The report was adopted by the EP Committee with 39 to 0 votes, with one abstention. (EDB)
➤eucrim ID=1204021

Council Adopts Conclusions on EU Strategy against Trafficking in Human Beings

During the JHA Council of 25 October 2012, the Council adopted revised conclusions on the new EU strategy towards eradication of trafficking in human beings (see eucrim 3/2012, pp. 100 ff.). Member States are invited to step up their efforts to effectively combat trafficking in human beings and to protect the victims by strengthening internal and external cooperation. To achieve this, Member States should use the tools that are available to them, e.g., special investigative techniques provided by relevant CoE and UN legal instruments as well as joint investigation teams. The exchange of information can be improved by enhancing the use of relevant EU agencies. Furthermore, the conclusions include, inter alia, a call to intensify efforts to conduct financial investigations and to locate, seize, and confiscate assets related to trafficking in human beings.

The EU agencies involved in the fight against trafficking in human beings are called upon to step up their efforts to combat this form of crime and to facilitate and support the multidisciplinary approaches to do so. The Commission is invited to implement the EU strategy and present a first evaluation in 2014. According to the Council, the Commission should also coordinate action with GRETA and establish cooperation mechanisms in priority third states.

While implementing the actions put forward by the Council, the Member States, the EU agencies, and the Commission should take into account the five priorities identified in the EU Strategy (see eucrim 3/2012, p. 100 ff). (EDB)
➤eucrim ID=1204022

EP Organised Crime Committee Discusses Action against Mafia

On 15 October 2012, the EP special Committee on Organised Crime, Corruption, and Money Laundering discussed a report on possible ways to tackle mafia-related crime. Even though an EU wide definition of organised crime exists, many differences still exist between national definition and approaches to this type of crime.

According to the committee's rapporteur, the future European Public Prosecutor's Office should be accorded a key role in coordinating efforts to defend Member States' financial interests and providing national authorities with input, for instance in combating fraud against the EU budget.

In addition, the report suggests seizing property that is related to a crime as a preventive measure and introducing EU-wide exclusion from public procurement. (EDB)
➤eucrim ID=1204023

Study on Links Between Terrorism and Organised Crime in the EU

The EP's LIBE Committee published a study on the nexus between terrorism and organised criminal groups in the EU in November 2012. The study is based on a combination of qualitative and quantitative analyses of open sources

and field research that was conducted by the author and associates in Europe, Africa, the former Soviet Union, South America, and South Asia. Additionally, unstructured discussions were held with law enforcement and security officials having operational or analytical functions in terrorism and organised crime cases. Relevant private actors were involved as well. A group of experts analysed the findings.

The end result is as set of recommendations and policy-relevant advice for the LIBE Committee.

In addition to these recommendations, the study contains four chapters:

- Theoretical basis of the links between OC and terrorism;
- European case studies;
- Assessment of the threat trajectory;
- The impact of a nexus between terrorism and organised crime on the EU's legal economy, public administration, and financial system. (EDB)

➤eucrim ID=1204024

Illegal Online Gambling

Action against Online Gambling Including Match-Fixing

On 23 October 2012, the Commission presented an action plan against online gambling (see also eucrim 1/2012, p. 11). As one of the fastest growing service activities in the EU, it has also become vulnerable to criminal activities by exposing consumers to unregulated gambling websites, often from outside the EU, which harbour significant risks such as fraud and money laundering.

The Commission's plan is not to harmonise national rules on online gambling but instead to present a set of common principles and initiatives for the next two years in order to encourage Member States to cooperate.

Cooperation is needed, especially with regard to sports and online betting and match-fixing. In a next step, the Commission will adopt three recommendations, namely on the common protection of consumers, responsible gambling advertising, and the prevention of and fight against betting-related match-fixing.

Other measures include the testing of parental control tools to protect children from online gambling and the extension of the scope of the money laundering directive. Member States are also encouraged to collect data on gambling disorders and set up national contact points to combat match-fixing.

The fight against match-fixing has been made a priority before; on 20 September 2012, during the annual EU Sports Forum, deliberations between the Cyprus Presidency, the Commission, and the participants at the Sports Forum resulted in a five-point declaration on the fight against match-fixing. This declaration identified five key areas which initiatives against match-fixing should focus on: education, prevention and good governance, monitoring, sanctions and finally, cooperation and international coordination. (EDB)

➤eucrim ID=1204025

Cybercrime

EU Computer Emergency Response Team Now Permanent

On 12 September 2012, the Commission announced that the EU Computer Emergency Response Team (CERT-EU) has now been established on a permanent basis. As part of the EU Digital

Tackling Cyberlaundering More Effectively

Legal challenges and practical difficulties

Lisbon, 11-12 April 2013

This seminar is part of a project sponsored by the European Commission (Prevention of and Fight against Crime Programme, Directorate-General Home Affairs) and consists of a series of six seminars at different venues: Madrid, Lisbon, Vilnius, London, Sofia, and Stockholm. The overall theme of the series is "Fighting cybercrime: series of intensive seminars for EU legal practitioners." Each seminar will have a specific focus (for a more precise overview of future topics and dates: www.era.int).

The abuse of the Internet by money launderers is a significant threat. Cyberlaundering, i.e., Internet-related money laundering, has become an efficient way to hide the proceeds of crimes. New advanced technological solutions for electronic payment and non-cash transactions, however, have considerably reduced the risk of seizure and forfeiture of money that has been illegally obtained by criminals.

This seminar will look at criminal money flows over the Internet, at the main international and European standards and legal instruments in place, and at the key role accorded to the exchange of information between the private and public sectors.

Key topics are

- The risk of money laundering on the Internet;
- Challenges in investigating and prosecuting financial crimes on the Internet;
- The new OECD international anti-money laundering (AML) standards, a review of the Third EU AML Directive and the proposed new EU Directive on attacks against information systems ("Directive on Cybercrime");
- The involvement of the Internet industry to tackle cyberlaundering;
- Cyberlaundering: recent trends and intelligence tools.

The course will be held in English and is primarily aimed at judges, prosecutors, ministry officials, lawyers in private practice and other independent legal professionals, compliance officers in the banking and financial industry, law enforcement officials, IT security professionals, and representatives of the Internet industry.

For further information, please contact Mr. Laviero Buono, Head of European Criminal Law Section, ERA. e-mail: lbuono@era.int

Agenda (see eucrim 3/2011, p. 106), the CERT-EU was set up as a one-year pilot project, drawing positive reactions from stakeholders.

The CERT-EU cooperates with EU institutions and the national CERTs as well as IT firms. Its resources are provided, inter alia, by the Commission, the Council, the EP, the Committee of the Regions and Economic and Social Committee, and the European Network and Information Security Agency (ENISA). The team operates under the strategic supervision of an inter-institutional steering board. (EDB)

➤eucrim ID=1204026

Basic Training Course on Legal and Technical Aspects of Cybercrime

Focus on jurisdictional issues in cyberspace

ERA, Trier, 25-26 April 2013

This training course is sponsored by the European Commission (Prevention of and Fight against Crime Programme, Directorate-General Home Affairs). It is part of a project consisting of eight seminars that will take place at the ERA headquarters in Trier between 2012 and 2015. The project comprises basic training courses on the legal and technical aspects of cybercrime in order to provide approximately 500 judges and prosecutors with the essential skills necessary to cope with Internet-related offences.

Key topics are

- Introduction to cybercrime: definitions, development of computer crime, overview of the most relevant offences and how they are committed;
- Legal challenges and solutions in fighting cybercrime: challenges in applying traditional criminal law instruments, procedural law, jurisdictional issues, and international cooperation;
- Cybercrime case studies (real-life scenarios to be discussed in small working groups);
- Jurisdictional issues in the cyberspace.

The course will be held in English and is primarily aimed at judges and prosecutors.

For further information, please contact Mr. Laviero Buono, Head of European Criminal Law Section, ERA. e-mail: lbuono@era.int

Procedural Criminal Law

Data Protection

Opinion of the FRA on the Data Protection Reform Proposal

Following the opinions presented by the EDPS (see eucrim 2/2012, p. 59) and the Article 29 Working Party on the proposals for reforming the EU's data protection legal framework, the Fundamental Rights Agency (FRA) issued its opinion on 1 October 2012.

The opinion focuses on the fundamental rights that are protected by the two proposals: the general data protection regulation and the directive on data protection in criminal matters. The list of fundamental rights affected differs between both instruments. This is an issue that the FRA would like to see aligned or a justification should be given for the discrepancy. The FRA also suggests including a reference stating that the proposed legal instruments are applied in a manner consistent with the provisions of the Charter of Fundamental Rights.

In general, the FRA opinion aims at balancing the fundamental right to the protection of personal data with other fundamental rights such as the freedom of expression.

Furthermore, the issue of the protection of certain categories of personal data in relation to non-discrimination is analyzed, as are the safeguards put in place by the reform proposals to ensure access to justice. (EDB)

➤eucrim ID=1204027

EDPS Opinion on Eurodac Access for Law Enforcement

On 5 September 2012, the EDPS released his opinion on the amended Commission proposal to grant law enforcement agencies access to Eurodac (see eucrim 3/2012, p. 104 ff). The data protection implications of this proposal are substantial, and the EDPS notes that he has not seen sufficient and up-to-date evidence that granting these access rights to a system set up for asylum and migration purposes would be a necessary and proportionate measure to take. He therefore calls upon the Commission to make a new impact assessment taking into consideration these elements.

In addition, the EDPS recommends, inter alia, clarifying that Eurodac data cannot be transferred to third states, informing the data subject concerning the law enforcement use of the data, and introducing judicial authorisation for access or at least an independent verification authority. (EDB)

➤eucrim ID=1204028

Commission Renegotiating CoE Data Protection Convention

On 19 November 2012, the Commission announced that it will be involved in renegotiations of the CoE's 1981 Data Protection Convention on behalf of the EU.

Simultaneously, the CoE is also revising its data protection legal framework. The 1981 Convention that is considered to be the basic legal instrument of data protection and that has been ratified by all EU Member States is thus being renegotiated. The Commission stated that it will ensure the Convention provides for a high level of protection of fundamental rights and freedoms with respect to the processing of personal data, which in turn reflects the EU's internal rules. (EDB)

➤eucrim ID=1204029

Interparliamentary Committee on Data Protection Reform

On 9 and 10 October 2012, the EP, together with representatives of the national parliaments, discussed the data protection reform proposals submitted by the Commission on 25 January 2012 (see eucrim 1/2012, p. 13).

Presentations by members of law enforcement and judicial, government, and academic institutions and agencies were given on several aspects of the reform package, followed by question and answer rounds. The main points of discussion included obtaining the data holder's explicit consent prior to processing, one single EU data protection regime, the disclosure and use of private-sector data for law enforcement purposes, the "right to be forgotten" for Internet users and the transfer of data to third states. (EDB)
➤eucrim ID=1204030

Freezing of Assets

Proposed Directive on Freezing and Confiscation of Proceeds of Crime – State of Play

With regard to the proposal for a new directive on freezing and confiscating the proceeds of crime, discussions in the Council on 25-26 October 2012 concentrated on the scope of extended confiscation. A note had been prepared for this discussion by the Cyprus presidency on 16 October 2012.

The concept of extended confiscation means that powers to confiscate are extended to assets that are not direct proceeds of the crime of which a person has been convicted. This has already been introduced in Framework Decision 2005/212/JHA. However, the Council's preparatory bodies suggested introducing a criterion limiting the scope of the extended confiscation. Several approaches were considered, e.g., a penalty threshold or limiting it to certain types of offences.

At a later date (3 December 2012), the Cyprus presidency succeeded in reaching a general approach, including a compromise on the scope of the extended confiscation by limiting it to serious criminal offences that are liable to give rise, directly or indirectly, to economic gain. Further, the non-conviction based confiscation has been limited to two specific circumstances, permanent illness and flight of the suspected or accused person. During the JHA Council of 6-7 December 2012, this general approach was endorsed. (EDB)
➤eucrim ID=1204031

Cooperation

Police Cooperation

8th Meeting of JIT Experts

On 18-19 October 2012, the 8th annual meeting of Joint Investigation Team (JIT) experts took place at Europol headquarters in The Hague.

The meeting focused on the evaluation of JITs. The experts agreed to establish a standard process for the evaluation of JITs in order to achieve consistency, save time, and allow for conclusions and identification of common obstacles and best practices. The JITs Network Secretariat, together with Eurojust and Europol, are now to develop a simple and structured template for this purpose.

Other subjects discussed concerned experience gained with JITs in a number of Member States, the work of the JIT Secretariat, and the planned use of an expert platform for exchange of non-personal information.

The meeting was attended by more than 100 participants from all 27 Member States, the Council, the European Commission, the European Anti-Fraud Office, the European Police College, the European Judicial Training Network, Eurojust, and Europol. It was organised by the JIT Network Secretariat with support from Europol and Eurojust. (CR)
➤eucrim ID=1204032

Police Officers in EU Crisis Management Operations: Rules of Engagement

On 24 September 2012, the Committee for Civilian Aspects of Crisis Management sent a note to the Political and Security Committee, including a compendium of principles for the use of force and consequent guidance for the issuing of rules of engagement (ROE) for police officers participating in EU crisis management operations. The objective of the compendium is to provide a general concept for the use of force and firearms by an EU police component in crisis management and to form a model for drafting future mission-specific rules of engagement. Rules of engagement are applicable to all police officers assigned by the Member States or Third States to an EU-led police mission.

The compendium explains the mandate, legal framework, and applicability of rules of engagement, the procedures that apply when dealing with ROE violation as well as regulations for the use of force, including firearms, e.g., for the use of batons, pepper spray, handcuffs, police dogs, and riot control agents. The level of force to be used by police officers is also outlined. (CR)
➤eucrim ID=1204033

Judicial Cooperation

Implementation Mutual Recognition of Supervision Measures and Alternative Sanctions

On 13 November 2012, the General Secretariat of the Council released a table overview of the implementation of Framework Decision 2008/947/JHA on application of the principle of mutual recognition to judgements and probation decisions with a view to the supervision of probation measures and alternative sanctions.

Member States needed to implement the framework decision by 6 December 2011 at the latest. (EDB)
➤eucrim ID=1204034

Council of Europe*

Reported by Dr. András Csúri

Foundations

Reform of the European Court of Human Rights

Translation of the Court's Information Material into Further Languages

On 6 December 2012, the Court released ten new language versions of its multimedia materials on the ECHR as well on admissibility conditions. A number of publications have been already translated into various official CoE languages and published on the Court's website in order to raise awareness of the Convention system, particularly among potential applicants.

The Court also plans to release translations into non-European languages (e.g., Chinese, Japanese, and Arabic) in the near future (for other translation-related news, see eucrim 3/2012 p. 106 and 2/2012 p. 61).

➤eucrim ID=1204035

Other Human Rights Issues

Albania Called Upon to Make Its Legal Aid System More Accessible

On 6 November 2012, Nils Muižnieks, the CoE Commissioner for Human Rights, released a letter regarding serious human rights concerns involving access to justice and a fair hearing in Albania. The Commissioner acknowledges the recent steps the country has taken to improve its free legal aid system; however, he remains concerned about the country's compatibility with CoE standards in this field. The letter highlights as main problematic areas the low rate of approved requests for free legal aid, the complicated procedures regarding the obtainment of free legal aid, and the selection of relevant lawyers. The current system of court fees (advance payment in regard to claimed value and adjudicated value in civil proceedings) as well as excessive lawyer fees may further preclude people in fragile economic or social situations from fully enjoying their human rights.

➤eucrim ID=1204036

Specific Areas of Crime

Corruption

GRECO Joint First and Second Evaluation Report on Liechtenstein

On 31 October 2012, GRECO published its first ever evaluation report on Liechtenstein. As usual, the report focused on two distinct areas in need of improvement: the criminalisation of corruption and the transparency of party funding.

Liechtenstein joined GRECO and ratified the CoE Convention on Corruption in 2010; therefore, it is still in the early stages of implementing effective anti-corruption measures. The report emphasizes that the current approaches do not take into account the various forms of bribery beyond strictly material ones. Further, it recommends reviewing the powers of the Prince regarding blocking and terminating any investigation or prosecution. The report also recommends keeping under review the appointment process concerning judges. GRECO further suggests introducing appropriate screening procedures for relevant positions in the public sector. It also recommends introducing a legal measure in the Criminal Code to enable the courts to prohibit a person found guilty of serious corruption offences from holding a leading position in a legal entity for a certain period of time.

GRECO made a total of 18 recommendations to the country and will assess the action taken during the second half of 2013.

➤eucrim ID=1204037

Fourth Round Evaluation Report on Latvia

On 17 December 2012, GRECO published its fourth round evaluation report on Latvia, which focuses on the prevention of corruption of members of parliament, judges, and prosecutors. The report states that, since the last evaluation report (see eucrim 1-2/2008, p. 50-51), Latvia has implemented a clear and comprehensive framework for regulating conflicts of interest of public officials. In addition, the country's anti-corruption agency uses this law well. GRECO's main recommendation is to abolish the system of administrative immunities, which could help dispel any idea that parliamentarians, judges, and prosecutors are above the law.

➤eucrim ID=1204038

CDPC Discusses Corruption in Sports

At its 63rd plenary session on 4-7 December 2012, the CDPC took note of information concerning a preliminary draft Convention against Trafficking in Human Organs, provided by the PC-TO. As a follow-up to the 31st CoE Conference of Ministers of Justice (Vienna, 19-21 September 2012) on "Responses of Justice to Urban Violence," the CDPC

* If not stated otherwise, the news reported in the following sections cover the period October – December 2012

aims to compile all possible existing CoE recommendations, other legal instruments, and international guidelines on juvenile offenders to find out whether there is need for the CDPC to develop new standards in the field.

The plenary also discussed the issue of dangerous offenders and the work of the PC-CP.

The integrity of sports remains an ongoing subject (see eucrim 3/2011 p. 117), including a possible CoE Convention against Manipulation of Sports Results and, notably, match-fixing as well as consideration of the feasibility of an Additional Protocol of the CoE Criminal Law Convention on Corruption to expand its scope of application to the private non-profit sector, notably sports.

Finally, the CDPC approved and welcomed the publication of guidelines on practical measures to improve co-operation in respect of the transfer of proceedings, including a model request template as a practical tool for practitioners in the field of co-operation in criminal matters.
➤eucrim ID=1204039

Money Laundering

Fourth Round Evaluation Report on Georgia

On 21 December 2012, the CoE's MONEYVAL published its fourth evaluation report on Georgia. The report is based on the on-site visit from 28 November to 13 December 2011 and sets out Georgia's levels of compliance with the FATF 40+9 Recommendations. It also provides suggestions on how certain aspects of the system could be strengthened.

The report lists the improvement in legislation regarding the criminalisation of ML and FT as well as the preventive measures taken by financial institutions. Progress has also been made in the effective use of the law, as significant sums have been confiscated since the last evaluation in 2005. Georgia has a solid framework for mutual legal assistance and exchanges information with international FIUs.

The system still lacks compliance, however, with key elements of the CoE standards in the field. Major loopholes have been identified in the transparency of legal entities, the lack of measures to prevent FT, and preventive measures for designated non-financial business and professions. The latter are not supervised, with the exception of notaries.

Furthermore, the country's FIU lacks sufficient information and analytical tools, which results in the poor quality of analysis of suspicious transaction reports.
➤eucrim ID=1204040

Procedural Criminal Law

CEPEJ: Plenary Meeting, 10th Anniversary and Report on Length of Court Proceedings

On 6 and 7 December 2012, the European Commission for the Efficiency of Justice (CEPEJ) held its 20th plenary meeting, at which it celebrated its 10th anniversary. It also adopted the new evaluation scheme of European judicial systems for the 2012-2014 cycle as well as the second edition of the report on "Length of court proceedings in the member states of the Council of Europe based on the case law of the European Court of Human Rights." Further, the implementation of a permanent observatory of justice in Europe was discussed.

The updated edition of the 2007 study on judicial lengths of proceedings in the ECtHR's case law concluded that the length of judicial proceedings remains a major concern. Since 2006, approximately one quarter of the annual total judgments found a violation of the ECHR in the excessive length of proceedings. The report underlined that the Court's judgments show a clear need for a "culture of expedition or dispatch," which requires proper judicial time management. The report stressed among other aspects the importance of mobilising all the parties to the court trial, to efficiently use information technology tools to facilitate the follow-up of proceedings, to better involve all legal professions who contribute to the proceedings, and to increase the courts cooperation with external institutions.
➤eucrim ID=1204041

Legislation

GRETA: Election of GRETA Members, Evaluation Visits and 15th Meeting

On 12-13 November 2012, the Committee of the Parties to the Convention on Action Against Trafficking in Human Beings held elections for 13 members of the GRETA. Five of the current members were re-elected, while eight new members were elected for the first time. The term of office runs for a three-year period from 1 January 2013 to 31 December 2016.

On its 15th meeting on 26-30 November 2012, GRETA adopted final evaluation reports in regard to France, Latvia, Malta, and Portugal and exchanged views with judges from the ECtHR concerning the Court's jurisprudence on Article 4 of the ECHR.

In addition, GRETA carried out first round evaluation visits to Slovenia (10-13 December 2012) and Luxembourg (11 to 14 December 2012) regarding the implementation of the CoE Convention on Action against Trafficking in Human Beings.

Finally, Switzerland and Germany became the 38th and 39th Parties to the Council of Europe Convention on Action against Trafficking in Human Beings. Switzerland and Germany ratified the Convention on 17 and 19 December 2012, respectively, which will enter into force for both states on 1 April 2013. The Convention entered into force on 1 February 2008 and was last ratified in 2010 by the Netherlands (see eucrim 1/2010 p. 24.).
➤eucrim ID=1204042

Addressing Organised Crime in Fraud Cases – Developing a More Efficient Legal Framework

Deniz Genç

The European Union has adopted and developed a comprehensive framework to combat offences affecting its financial interests over the years. It established a specific investigative service, the European Anti-Fraud Office (OLAF) in 1999, which is competent to conduct administrative investigations when there is suspicion of fraud or any illegal activity affecting the budget of the Union.[1] OLAF can fully independently conduct internal investigations (i.e., inside any European institution or body funded by the EU budget) and external investigations (i.e., at the national level if the EU's financial interests are affected); to this end, it cooperates closely with competent national authorities as well as with European agencies and institutions. The Court of Auditors audits the EU's finances and acts as their guardian. Also, Eurojust and Europol, as judicial and police agencies, play a role in the area of fraud connected to the EU budget and cooperate with OLAF for the purpose of its investigations.

OLAF is competent to conduct administrative investigations with regard to any offence affecting the financial interests of the European Union: typical offences involve, among others, VAT fraud, customs fraud, corruption of civil servants, fraud affecting structural funds, and cigarette smuggling. OLAF also provides assistance and coordinates in cases of euro counterfeiting and money laundering. These offences often have a transnational dimension but also links with criminal networks that are structured, organised, and whose activity is not limited to fraud but includes many serious crimes (human and drug trafficking, etc.). Indeed, offences affecting the Union's financial interests can be part of organised crime. To this end, the legal framework of OLAF specifies that cases presenting links to organised crime are a priority.[2] Also, and due to the nature of these offences, cooperation and coordination with Eurojust and Europol are essential to ensure an efficient response.

The existence of a link between fraud connected to the EU budget and organised crime has been acknowledged for a long time. Both Europol's Organised Crime Threat Assessments (OCTA) and Eurojust's Annual Reports, as well as the OLAF Reports, highlight the important links between certain criminal activities, e.g., fraud, corruption, cigarette smuggling, euro counterfeiting and money laundering, and organised crime. However, this link is not always made in practice. The main shortcomings result from the difficulties in agreeing on a single and common definition of organised crime and the difficulties in applying its criteria. As a direct consequence, many offences are not qualified as organised crime where they should have been. It is therefore difficult to fight these offences and these criminal networks properly but also to assess with precision how many investigations conducted at the EU level by OLAF implied organised criminal groups and how much of the EU budget has been defrauded by them. This should not, however, affect the imperative of improving the current legal framework and instruments in order to fight fraud offences with a link to organised crime even more efficiently.

I. A Wide Range of Definitions of "criminal organisation"

The Preamble of the Convention on the protection of the European Communities' financial interests of 26 July 1995[3] already refers to organised crime: the Member States acknowledged the potential existence of a link between fraud affecting the Union's financial interests and activities conducted by criminal organisations.[4] Furthermore, the Annual Reports on the fight against fraud presented by the Commission in the 1990s corroborated this by reporting fraud cases in which organised criminal networks were involved and had defrauded the Union's budget. The links between organised crime and fraud connected to the Union's budget were explicitly acknowledged and highlighted for some time, but after 9/11, the focus on organised crime started to decline in favour of terrorism. Terrorism cases do not present such obvious reasons for links with fraud as organised crime cases, with the exception of a few cases (e.g., cigarette smuggling cases in Northern Ireland). Offences affecting the Union's budget still indicated links with organised crime, however, and organised crime was defined as one of the key threats in the European Security Strategy.[5]

In 2008, the Council adopted a Framework Decision on the fight against organised crime.[6] A common definition at the Union's level is thus laid down. Under the Framework Decision, a criminal organisation is "a structural association, established over a period of time, or more than two persons acting in concert with a view to committing offences which are punishable

by deprivation of liberty or a detention order of a maximum of at least four years or a more serious penalty, to obtain, directly or indirectly, a financial or other material benefit."[7] This definition focuses on a few specific elements:

- A structured organisation of more than two people;
- Existing for a certain period of time;
- The commission of criminal offences punishable by imprisonment for a certain period;
- A benefit that can be of financial nature.

However, different definitions of organised crime can be found. The United Nations Convention against Transnational Organised Crime of 15 November 2000 gives a similar definition of "organised criminal group" that also focuses on the same above-mentioned four elements with more or less emphasis.[8] But organised crime is an evolving and adapting phenomenon whose definition can differ from time to time but also depending on the particular perspective from which it is viewed. Therefore, its legal definition has to be sufficiently broad in order to allow for various forms of criminality to qualify as such, but not so broad so as not to cover any differences in categories of criminal activity or offence. Also, the definition should be drawn up in such a way that different categories of legal entities, not only natural persons but also legal persons, are covered as well as different levels of hierarchy.

Furthermore, when analysing the practice of EU agencies and institutions involved in the fight against organised crime, it has been found that not one common definition of organised crime is shared by them. Eurojust uses the definition set up in the Framework Decision. In contrast, Europol, OLAF, and the Court of Auditors do not use this particular definition or any definition at all. Indeed, Europol uses a body of characteristics to qualify an offence as an organised crime, some of them being mandatory, but neither OLAF nor the Court of Auditors has a working definition of organised crime. Moreover, use of the qualification of an offence as a "serious crime" by certain bodies can be seen as duplication and lead to confusion. This heterogeneous legal environment of course contributes to the difficulty of assessing the percentage of fraud cases where a link with organised crime exists as well as the amount of EU money that has been defrauded by organised criminal networks.

It should still be noted that, ultimately, the definition used by Europol shares the main elements of the definition in the Framework Decision. Indeed, among the body of criteria, four characteristics are mandatory and they correspond exactly to the four above-mentioned elements of the definition in the Framework Decision.[9] However, the difference is that Europol requires additional criteria to qualify an offence as organised crime.

Therefore, the definition laid down in the Framework Decision on organised crime can be used as the common basis for analysis of the activities of the European agencies and institutions in fighting fraud to the EU budget committed by criminal organisations.

II. The Links between Organised Crime and Fraud Cases in Practice

In 2011, the European Parliament presented a study entitled "How does organised crime misuse EU funds,"[10] which was based on publicly available information from OLAF, Eurojust, Europol, and the Court of Auditors. OLAF then conducted an internal analysis of its role as regards organised crime. The study underlined the difficulty of ascertaining to which extent organised crime defrauds the EU budget. This is due to both the lack of reliable information on the extent of misuse of EU funds by organised criminal groups and the lack of reliable information on how organised criminal groups misuse EU funds. The study, however, still highlighted the strong involvement of organised criminal groups in offences affecting the Union's financial interests and pointed out the need for the EU agencies and institutions to focus more on organised crime in a cooperative manner.

The internal analysis conducted by OLAF analysed a sample of cases closed in 2009 and 2010: it consisted of 375 final case reports having a final impact of approximately €1750 million. The cases were analysed in order to detect the possible existence of an organised crime dimension, using the definition laid down in the Council Framework Decision. In the end, links with organised crime were found in 35 cases, the total impact on the EU budget being just over €750 million. In terms of percentages, cases having connections with organised crime amounted to somewhat less than 10% of all cases and the financial impact to above 40% of the EU budget. Already, only these numbers show to which extent organised criminal groups damage the Union's financial interests: the impact of the cases concerned on the EU's budget is four times greater than the impact of other cases.

Two things should be noted. First, this internal analysis is based only on cases where a link with organised crime has been established, and they only represent a small percentage of the real activity of criminal organisations in relation to fraud offences. Indeed, sometimes the connection to organised crime is not made and these cases escape the qualification. A significant number of fraud cases in general are also not reported or investigated. Secondly, however, the EU agencies and institutions do not have, *in fine*, the competence to qualify an offence as organised crime: only criminal courts have the power to le-

gally qualify criminals as constituting a criminal organisation. Therefore, these numbers do not depict the reality of the final convictions for organised crime in fraud-related cases.

After more in-depth analysis of the 35 above-mentioned cases of the internal analysis conducted by OLAF in 2011, one can notice that almost all the major sectors of fraud are concerned:[11] agriculture, cigarettes, customs, direct expenditure, EU institutions, structural funds, trade, and VAT.[12] However, not all sectors attract criminal organisations in the same measure. Indeed, the only VAT case closed in 2009 showed links with organised crime as did a significant number of cigarette smuggling cases and trade cases closed in 2009 and 2010.

Also, it appears that the involvement of a criminal organisation is more important in certain sectors than in others, such as in cigarette smuggling cases. Moreover, and as stated in the OLAF Report for 2011, "cigarette smuggling is almost exclusively the domain of organised crime groups;"[13] the OCTA 2011 (Organised Crime Threat Assessment) make the same remark on cigarette smuggling.[14] Organised criminal groups are also very active in VAT fraud and in counterfeiting, which can impact customs duties. Moreover, counterfeiting of the euro is a major sector of activity of organised criminal groups, as is money laundering.[15]

Besides, a distinction can be pinpointed between different organised criminal groups and their structures: indeed, different types of organised criminal groups operate in different sectors, which makes their countering even more difficult. For example, those groups involved in euro counterfeiting are usually organised in a specialised structure where cells operate under a clear and strict mandate and independently of one another in order to minimise risk. In the area of VAT fraud, it is proven that criminal groups work with each other, sharing knowledge, information, and intelligence, and even invest in one another's activities. Intelligence on criminal organisation and their structure is mainly collected and analysed by Europol at the European level, but a better exchange of information and intelligence on this matter would help the other bodies and improve their work as well as the fight against organised crime in general.[16]

However, as far as information given to OLAF by the national criminal courts, no conviction for criminal association was pronounced in the majority of the 35 cases: as stated previously, only criminal courts can legally decide if an offence qualifies as an organised crime, and they are not bound by the suggestions made by OLAF. It should be mentioned, however, that the Framework Decision on the fight against organised crime has not been properly implemented throughout the Union. Moreover, in some Member States, committing a crime within a criminal organisation is penalised as an aggravated circumstance whereas in others it is a specific conduct penalised as a separate offence; this difference in the legal systems of the Member States heightens the difficulty in assessing the number of convictions for criminal association on cases transferred by OLAF. Both the lack of a working definition within OLAF and the insufficient implementation of the Framework Decision in the Member States contribute to the limited number of convictions for criminal organisations in fraud-related cases transferred to competent national authorities by OLAF. The European Parliament, in a resolution on organised crime in the European Union,[17] pointed out this issue and suggested that the Commission table a proposal for a Directive "which contains a less general definition of organised crime and manages better to identify the key features of the phenomenon" as well as the identification of "habitual offences committed by organised crime."

III. Recommendations: How to Better Fight Criminal Organisations in Fraud Cases

Of course, the fight against organised crime is and will remain a priority for OLAF investigations and for other European agencies' and institutions' activities; there is no questioning the importance of the fight against organised crime in the light of the risk it presents to the security of European citizens and the significant impact it has on the Union's financial interests. However, and as illustrated in the previous section and the internal analysis conducted by OLAF in 2011, the means currently available at the EU level are neither efficient enough yet, nor is the emphasis put on organised crime.

In 2011, the European Commission therefore adopted a communication on its Anti-Fraud Strategy (CAFS) with the objective "to improve prevention, detection and the conditions for investigations of fraud and to achieve adequate reparation and deterrence."[18] The role of OLAF is highlighted, as it plays a central role by conducting administrative investigations and by supporting other Commission Services in the prevention and detection of fraud, including organised crime. The CAFS sets among its guiding principles fraud prevention, an effective investigation capacity, and good cooperation between internal and external actors. It pinpoints the need to develop specific sectorial anti-fraud strategies at the Commission Service level, with OLAF playing a proactive role in helping the concerned Services in the development and implementation of such strategies.

Mostly, the CAFS acknowledges the need to reinforce and intensify cooperation between the EU agencies and institutions by increasing the pooling and exchange of information. OLAF

should share its operational experience and best practices with other EU institutions and agencies but also with the Member States authorities concerned with protecting the Union's financial interests, and specific cooperation with these authorities should be established as well. A Fraud Prevention and Detection Network will be developed and organised by OLAF as a centre of expertise providing support and advice to other Commission's services, based on best practices and fraud risk assessments. Besides, the CAFS also foresees the development of improved fraud risk analyses and intelligence gathering and sharing, notably by the collection and analysis of cases in concrete sectors of EU funding and smuggling. The identification of fraud risk areas will thus be facilitated and formalised. The use of IT tools and fraud indicators is recommended as well as the development of secure platforms for the exchange of data. OLAF's operational experience can serve as the basis for the identification and definition of such indicators and best practices.

Other means are necessary in order to develop a comprehensive framework to fight organised crime more efficiently. First of all, one single definition of organised crime should be used at the EU level by the different agencies and institutions involved in combatting it, and it should be the one laid down in the Framework Decision on the fight against organised crime. As mentioned, Eurojust already uses this definition and Europol's definition is quite similar. OLAF does not formally use a specific definition of organised crime of its own. The internal analysis on cases presenting links with organised crime was based on the definition of the Framework Decision. Also, this definition is the only one enshrined in a legal instrument at the EU level.

This point is important for OLAF investigations but also to improve the cooperation between OLAF, Europol, and Eurojust. For OLAF investigations, it would help in further assessing the impact of organised crime on the Union's financial interests and the role of OLAF when it comes to countering it. The spectrum for analysis of the cases would then be larger and more efficient for future detection of the phenomenon and for its prevention. Also, a common definition would improve cooperation with Eurojust and Europol in so far as the communication and information exchange on cases between these bodies would be enhanced and lead to a more efficient system.

Secondly, and to complement the setting-up of a working definition for OLAF investigations, OLAF's cooperation with Europol should be increased by focusing more on organised crime; this is foreseen in the CAFS and in the legislation on reform of OLAF. Support and the exchange of information on how to identify and detect criminal organisations in fraud cases could only be an added value for OLAF investigations and for Europol's activities as well. As mentioned above, Europol has a specific mandate concerning the fight against organised crime and is quite active in collecting intelligence concerning these organisations. Its experience is an added value in the fight against organised crime in general. This should be combined with the experience and expertise developed by OLAF and Eurojust and the close and structured cooperation they have developed with national authorities.

The setting-up of a European Public Prosecutor's Office (EPPO) for the protection of financial interests would be a significant improvement in this area. The EPPO would be competent to investigate, prosecute, and bring to court cases of offences affecting the Union's financial interests.[19] It would constitute the prosecution services corresponding to what OLAF is currently competent for (administrative investigations). It would be of great added value for the protection of the EU budget but also in the fight against organised crime considering the extent of the implication of criminal organisations in defrauding the Union's budget; as the internal analysis conducted by OLAF showed, the fight against offences affecting the Union's financial interests also includes the fight against organised crime − in so far as both are connected. The setting-up of the EPPO could help fight organised crime since investigations in anti-fraud cases would then be carried out from a European and potential cross-border perspective and would not be limited to a national context anymore.

In the end, the entire policy area of the protection of the Union's financial interests is relevant. Its reform will not only be of added value for the economy of the Union, but it will impact on many policy areas, notably on increasing police and judicial cooperation between and with the authorities of the Member States and on the fight against transnational crime. Several initiatives have been announced by the Commission.

The legal framework of OLAF is being reformed; the reform is to be adopted in early 2013 by the European Parliament, although the changes it brings about have already been implemented in OLAF. Finally, a package on strengthening the legal framework of the protection of the Union's financial interests is under preparation. The proposal for a Directive for protection by criminal law is currently being discussed at the Council; the Directive will define at the European level offences and levels of sanctions in the area of the protection of the Union's financial interests, including aggravated sanctions in case of offences committed in a criminal organisation.[20] A proposal to set up the EPPO is to be tabled in 2013, together with the reform of Eurojust according to Article 85 TFEU.

In the area under discussion, it is very important to address the link between organised crime and corruption. In June 2011, the

Commission adopted the anti-corruption initiative: a periodic reporting mechanism assessing the Member States' efforts to tackle corruption. The idea is to pinpoint the difficulties and problems regarding corruption in the Member States but also to propose solutions. It is believed that this instrument will facilitate the exchange of best practices and reinforce mutual trust between Member States. The anti-corruption initiative is part of a wider anti-corruption package, the following instruments being based on the findings of these reports. Other proposals can be mentioned: the revision of the legal framework on the confiscation and recovery of assets; the revision of the public procurement directive, which was defined as a priority in the CAFS; the strengthening of the Commission's cooperation with Europol, Eurojust, and the European Police College (CEPOL).

Many improvements are needed and can realistically be provided to establish a more efficient framework for the concerned bodies in order for them to exercise their respective competences and mandates. They will lead to better transmission of information between European bodies but also with and between national authorities.

Deniz Genç
Unit Policy Development, OLAF

1 OLAF was set up by the Commission Decision of 28 April 1999; its competences are defined by Regulation 1073/1999, O.J. L 136, 1999, p. 1.
2 OLAF, Investigation Policy Priorities for 2012.
3 O.J. C. 316, 1995, p. 49.
4 Ibid.: "Nothing that fraud affecting Community revenue and expenditure in many cases is not confined to a single country and is often committed by organized criminal networks".
5 European Council, *A Secure Europe in a Better World – European Security Strategy*, 12 December 2003 (Not published in the *Official Journal of the European Union*).
6 Council Framework Decision 2008/841/JHA, O.J. L 300, 2008, p. 42.
7 Article 1 of Council Framework Decision 2008/841/JHA.
8 Article 2(a) of United Nations Convention against Transnational Organised Crime: "organised criminal group" shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit.
9 „A structured organisation of more than two people; an existence enshrined in time; the commission of an offence punishable by imprisonment for a certain period; and a benefit that can be of financial nature."
10 European Parliament, DG for Internal Policies, Policy Department D: Budgetary Affairs, "How does organised crime misuse EU funds", 2011.
11 Sectors where no connection with organised crime was found in cases closed in 2009 and 2010: alcohol (but no case was closed in 2009 and 2010), EU bodies and agencies, external aid and precursors.
12 It should be kept in mind that this analysis is based only on cases closed during the years 2009 and 2010. Therefore, general conclusions cannot be drawn on this sole basis.
13 OLAF Report 2011, p. 27: http://ec.europa.eu/anti_fraud/documents/reports-olaf/2011/olaf_report_ 2011_en.pdf.
14 OCTA 2011, p. 32: https://www.europol.europa.eu/sites/default/files/publications/octa2011.pdf.
15 OLAF is not competent to investigate cases of euro counterfeiting or money laundering but still plays a major role by providing technical assistance and coordination.
16 OCTA 2011, *op. cit.* (fn. 14).
17 European Parliament, Resolution of 25 October 2011 on organised crime in the European Union.
18 European Commission, Communication on the Commission Anti-Fraud Strategy, 24.06.2011, COM(2011) 376 final.
19 Article 86 of the Treaty on the Functioning of the European Union.
20 This Directive aims at replacing and reinforcing the legal framework set up by the 1995 Convention and its Protocols.

The Evolving Structure of Online Criminality

How Cybercrime Is Getting Organised

Dr. Tatiana Tropina

The increasing dependency of society on information technologies raises concerns over vulnerabilities in cyberspace and the "dark side" of information networks. The growth of digital operations in legitimate markets is one of the vital factors for economic development. However, as markets and trade have always attracted criminals seeking benefits from illegal activities, digital networks have become a key enabler for the growth of cybercrime, both with regard to committing traditional crimes over the Internet and to developing new forms of computer misuse.

Cybercrime has been evolving in parallel with society's use of digital networks, reacting to every development in the legal sector with new approaches to committing offences. In

the past decade, cybercrime has gone through a transformation process from fragmented acts committed by individuals to increasingly sophisticated and highly professionalised activity. Moreover, cybercrime is believed to be at the stage of a fast expanding illegal industry where criminal activities are conducted by professional networks as long-term sustainable operations. Due to the newness of the phenomenon, there is still a considerable lack of research on how these networks in cyberspace are structured and how they operate. However, it is currently under discussion that we are witnessing the emergence of a new type of organised criminal groups that operates solely in cyberspace: groups that have not yet been consolidated into a stable system but are dangerous nonetheless.

This article seeks to contribute to the current research on this problem by examining the question of the possible transformation of cybercrime into a global, fast-expanding, profit-driven illegal industry with a new type of organised criminal groups thriving behind it. Firstly, the paper puts the issue of increasingly organised online criminality into the context of a general debate about organised crime in cyberspace. Secondly, it analyses the business models of the underground economy of cybercrime. The third part of the paper focuses on the structure of the online criminal groups and their way of functioning. The paper concludes by indicating the legal problems of tackling organised cybercrime.

I. "Organised Crime" in Cyberspace or "Organised Cybercrime"? Two Sides of the Coin

In the early days of cybercrime, the scene was mainly dominated by young hackers illegally accessing computer systems and breaking security measures just for fun or to demonstrate their technical skills.[1] With the development of the digital economy, both the criminal landscape and the motivation of offenders have changed dramatically. High rewards combined with low risks have made digital networks an attractive environment for various types of profit-driven criminals thriving on cybercrime.

The ongoing debate about the use of global information networks by organised criminal groups revolves around two issues: cyberspace as a *new medium* for traditional organised criminal groups and cyberspace as an enabler for the *new form* of organised crime. On the one hand, it is believed that cyberspace can be used by traditional organised criminal groups to carry out their operations.[2] On the other hand, it is argued that online criminals are nowadays shaping the new type of organised criminal networks.[3]

The problem of cyberspace as a *new medium* is related to the possibility of traditional organised criminal groups to use digital networks for their illegal activity. The basic reason for this discussion is the general assumption that traditional organised crime always seeks "safe havens" offered by countries with weak governments and unstable political regimes.[4] Cyberspace with its anonymity, absence of borders, and the opportunity to commit offences without being physically present at the crime scene constitutes a perfect environment, especially when criminals can operate from countries that do not have proper legal frameworks and technical capabilities to fight cybercrime.[5] While it is obvious that traditional organised criminal groups can benefit significantly from the use of information and communication technologies,[6] it is still not clear to what extent cybercrime can be attributed to the traditional organised criminal groups. McCusker[7] argues that this debate represents a tension between logic and pragmatism, where logic postulates that traditional organised crime will engage in criminal activities in a digital environment as it would in any low-risk and high-reward illegal business in the physical world; pragmatism, in turn, questions the necessity for traditional organised crime to step into this area and its capability to secure a return on investment and to produce the desired economic benefits.

A decade ago, Williams[8] argued that, despite growing evidence that traditional organised crime groups use digital networks, organised crime and cybercrime would never be synonymous because the former would be operating offline and most cybercrimes would be committed by individuals rather than organised structures. Brenner[9] also pointed out that there were indications that online crime was reaching the gang level of organisation. Though the landscape of cybercrime has changed a lot since then, there is still no clear concept of the synergy between organised crime and cyberspace. Moreover, it is very hard to fit cybercrime into the traditional concept of organised crime with its hierarchical homogenous structures.

To avoid confusion in the debate on organised crime in the digital world, it is necessary to distinguish between two different phenomena, namely, migration of traditional organised crime in cyberspace and organised groups focused on committing cybercrimes. The former is evident: The Internet has already become a tool for facilitating all types of offline organised criminality, including child abuse, illicit drug trafficking, trafficking in human beings for sexual exploitation, illegal migration, different types of fraud, and counterfeiting. It provides anonymity in communication, greater possibilities for advertisement and product placement as well as new money laundering schemes.[10] However, some studies suggest that, in the current era of organised crime, exploitation of cyberspace by traditional organised criminal groups coexists alongside organised structures operating solely in global information networks and committing only cybercrimes.[11] Thus, we are

witnessing the evolution of a *new form* of the organised crime. Recent reports produced by security companies highlight the professionalization and sophistication of cyber attacks and financial crimes committed in cyberspace by these groups, suggesting that this new type of organised crime is characterised by different, constantly evolving structures and new ways of using hi-tech tools to gain illegal profit.

These two tendencies – the shift of organised criminality into cyberspace and the emergence of a new form of organised crime – do not exclude each other. They go hand in hand, giving rise to the synergy between traditional organised crime and criminal structures operating online. However, while the first phenomenon – namely, the use of cyberspace by traditional crime to facilitate its activities – has already been broadly discussed in the academic literature, there is a lack of research examining the new forms and structures of organised crime online. This paper focuses on the latter issue, providing analysis of the model and structure of these new criminal groups committing crimes mostly or solely in cyberspace.

II. Ecosystem of Cybercrime: Business Model of Operations

1. Business Models of Cybercrime

Illegal activities online, e.g., credit card fraud, trading compromised users' accounts, and selling banking credentials and other sensitive information, have given rise to the increasingly sophisticated and self-sufficient digital underground economy.[12] Specific Internet forums and communication channels are used as underground marketplaces to trade illegal goods and services.[13] Any data traded on these shadow platforms has its own monetary value.[14] This value represents an illicit commodity, intangible and easily transferrable across borders. It drives the development of illegal markets: Specific criminal activities have been developed and are being constantly improved in order to steal sensitive information (e.g., phishing, pharming, malware, tools to attack commercial databases). Online criminality includes a broad spectrum of economic activity, whereby various offenders specialize in developing specific goods (exploits, botnets) and services such as malicious code-writing, crimeware distribution, lease of networks to carry out automated attacks or money laundering.[15]

Cybercriminals are increasingly structuring their operations by borrowing and copying business models from legitimate corporations. Cybercrime business models were similar to those of high-technology companies in the early 1990s because digital criminality was still in its infancy. But since the early 2000s, cybercriminals have developed patterns imitating the operations of companies such as eBay, Yahoo, Google, and Amazon.[16] One factor indicating the current maturation of the cybercrime industry is the degree of professionalization of IT attacks, e.g., fraudulent activities like classic phishing, which is becoming the greatest identity-theft threat posed to professional businesses and consumers.[17] Another factor is the increasing specialization of perpetrators,[18] which means that cybercrime involves the division of labour. Other factors include the sophistication, commercialization, and integration[19] of cybercrime.[20]

It is argued, though, that there is a difference between cybercrime business models and legitimate business in terms of core competences and important sources: While the latter is aimed at creating the most value for customers, cybercrime involves defrauding prospective victims and minimizing the risk of having illegal operations uncovered.[21] However, if one considers cybercrime as a model establishing a relationship between the supplier of illegal tools and services and the customer who uses these tools to commit the crime against the victim, this difference does not have much significance: Cybercrime business models are focused on providing the most value for the "consumers," who are not the victims of crimes but the criminals using the tools.

2. "Criminal-to-Criminal" and "Crime-as-Service" Models

Technological developments, research, innovation, and the transformation of value chains into value networks has driven the globalization of the legal sector and has affected their organisations, making them more decentralized and collaborative with regard to external partners. In the same way, innovation has fuelled the creation of new patterns in criminal ecosystems with regard to product placement, subcontracting, and networking.[22] Cybercriminals employ schemes similar to the legitimate B2B (business-to-business) models for their operations, such as the highly sophisticated C2C (criminal-to-criminal) models, which make stolen data and very effective tools for committing cybercrime available through digital networks.[23] Computer systems' vulnerabilities and software are exploited to create crimeware: "malware specially developed with the intention of making a profit and which can cause harm to the user's financial well-being or valuable information."[24] These crimeware tools, e.g., viruses, Trojans, and keyloggers, offer criminal groups the flexibility to control, steal, and trade data.

Automation plays a significant role in the development of C2C models. Automation tools use technology to avoid the operational requirement for physical groupings and force of numbers.[25] The core of automation is a system of botnets: networks of compromised computers that can be remotely controlled by

the perpetrators and used as "zombies". Users are usually not aware that their computers are infected with the malware and serve criminal networks. With a botnet, cybercriminals can make use of many compromised and controlled computers at the same time to launch large-scale attacks on private and corporate systems, send spam, disseminate malware, and scan for system vulnerabilities. Without botnets, they would have to target victims and machines manually and individually, which would make attacks too costly and time-consuming.[26] In this regard, the possibility to infect computers and turn them into "zombie" networks has been one of the main factors in transforming some types of cybercrime, such as phishing, into a worldwide underground ecosystem that is run, supposedly, by organised groups.[27]

Crimeware is also used to deploy *Crime-as-a-Service (CaaS)* as a part of C2C business models – the system of trading and delivering crimeware tools. The trading of botnets has become a high-revenue activity in the underground economy, specifically concerning Crime-as-a-Service models. Criminal organisations offer botnets at relatively low cost, profiting from the turnover based on the number of "customers." Moreover, as one of the logical shifts in adopting business models from the legal economy, criminals have started employing the policy of price differentiation, moving from static pricing lists to the flexible pricing schemes with discounts and bonuses.[28] In addition, they nowadays offer different packages of the same products, depending on the service. For example, in 2012, the basic package of Distributed Denial of Service (DDoS) bot Darkness by SVAS/Noncenz cost $450. The same botnet was offered also under "Bronze," "Silver," "Gold," and other options that included, depending on the price, free updates, password grabbers, unlimited rebuilds, and also discounts for other products.[29] The costs of DDoS attacks vary from $5 for one hour to $900 for one month of persistent attack. 5–15% discounts are offered on the return policy base.[30] These costs are relatively low compared to the criminals' financial gain: The estimated revenue of criminal groups using botnets range from tens of thousands to tens of millions of dollars.

In addition to the botnet trade, there is another emerging core service related to Crime-as-a-Service models of operations, namely, Pay-Per-Install (PPI) service, which has become a key and growing area of the underground economy.[31] This service was developed to meet one of the vital demands of the illegal market – infection of computer systems via digital networks. It outsources the dissemination of malware by determining the raw number of victims' computers that should be compromised within the scope of the "customer's" budget.[32] A single PPI service can partner with thousands of affiliates which are paid for the number of malware installs. A typical affiliate can supply more than 10,000 installs per month, which can generate millions of infected computers for illegal business, including thousands of affiliates.[33] This business may be very profitable for affiliates: e.g., Trend Micro reported on an affiliate that generated $300,000 from rogue AV[34] installs in only one month.[35]

As yet another advanced step in the development of the underground economy, tools-supplying business models are also used to share the techniques to commit cybercrimes. For instance, by creating "customer" systems where instruments are available on demand, the owners of the server with crimeware allow "users" to just log into the server and choose from the range of tools suitable for fraud, phishing, and data-stealing and then download them. Less skilled criminals can buy tools to identify vulnerabilities, compromise systems, and steal data. More sophisticated offenders can purchase malware or develop custom tools and scripts on their own. When user data is stolen, criminals can use crimeware servers to commit organised attacks. These servers also enable controlling compromised computers and managing the stolen data.[36] Furthermore, the next generation of business models has started offering such services as licensed malware and technical support for illegal software and tools.[37]

3. Money Laundering and Money Mules

The final and essential part of the cybercrime business model is monetization of illegal commodities (stolen data and information). For this purpose, cybercriminals use "money mules." Mules are usually recruited via spam or false job offers that promise a high commission: between 3% and 5% of the total money laundered.[38] The goal is to open a bank account or sometimes use a person's personal account to transfer cash, very often in different jurisdictions than those in which the crimes have been committed.[39] The mules are the visible "face" of organised cybercrime[40] because they are indentifiable individuals turning data into money and thus can be easily captured by law enforcement. Some studies consider them to be further victims of cybercrime because they might not be aware of the fact that they are taking part in criminal operations.[41]

It has been argued that "money mules" are the main bottleneck of the underground economy of cybercrime.[42] Cybercriminals face the same problem as any organised criminal group with a cash-out operation involving money mules: there are not enough of them in service. The ratio of stolen account credentials to available mule capacity with regard to digital crimes could be as high as 10,000 to 1.[43] The lack of money mules is attributed to the fact that they can usually operate for only a very short time before they are either abandoned by their han-

dler or discovered by law enforcement. As the underground digital economy continues to expand, it will be increasingly challenging for criminals to maintain the necessary supply level of this temporary "workforce" to profit fully from their illegal activities. Many sophisticated techniques have already been developed to deceive people into being hired as mules, e.g., masking the supposed illegal activities as legitimate services like looking for help in a job search.[44] It is very likely that the scam techniques for hiring money mules will continue to develop.

III. Criminal Networks in Cyberspace: Reconsidering the Traditional Concept of Organised Crime Structure

Though it is already evident that cybercrime is evolving into a big profit-driven illegal industry, it is still not clear to which extent this market is dominated by organised structures and to which extent they can be considered organised crime. Indeed, it is very hard to fit the new form of organised online criminality into the traditional concept of organised crime because the structure of these new groups differs from what is traditionally attributed to the organised crime. Traditional organised criminal groups are considered to be ethnically homogeneous, formally and hierarchically structured, multi-functional, bureaucratic criminal organisations.[45] In contrast, cybercrime has never gone through this stage of organisation during its development. It has moved from individual and fragmented criminal activities to the models employed in modern corporate business,[46] but the structure behind this criminal business marks "the cleanest break to date from the traditional concept of organised crime groups as hierarchical."[47] The most common view on the structure of organised criminal groups is that they represent flexible networks formed by high-skilled, multi-faceted cybercriminals.[48]

As it was mentioned above, the Internet is used either as a medium or as a sole platform for operation by both new and old types of organised crime. They can coexist without disturbing each other because of the very specific characteristics of Internet crime. One of the core characteristics of traditional organised criminal groups is that they violently maintain a monopoly over their assets and territory in order to control certain scarce or illegal commodities on the black market.[49] The commodity on the illegal market is stolen, intangible data that circulate in borderless cyberspace. Obviously, cybercrime groups do not require control over a geographical territory – the concept of geographical control would not work due to the specific environment where the operations are taking place. Furthermore, cybercrime does not require a lot of personal contacts between members or enforcement of discipline between criminals. Again, any discipline would be hard to enforce in cyberspace due to the lack of control mechanisms. Thus, the groups operating in cyberspace have less necessity for a formal organisation.

Moreover, the classic hierarchical structures of organised criminal groups may even be unsuitable for organised cybercrime.[50] The new type of organised crime in the digital environment is less competitive[51] and its model of competition is rather similar to the modern corporate world as regards pricing strategies, service-based competition, innovation, and "customer care" policy. The power of the criminal group lies in the strength and sophistication of its software, not in the number of individuals.[52] From this point of view, automation techniques to commit cybercrimes played a vital role not only in the development of the underground criminal industry, but also in becoming one of the core factors determining the structure of the groups: with automation, the power focus shifted from people to technical tools.

Online criminal groups are believed to be more flexible compared to traditional organised criminal groups, allowing for the incorporation of members for limited periods of time based on their flexibility.[53] These networks are structured on a "stand alone" basis, as members of the groups are often not supposed to meet.[54] They mostly rely solely on electronic communication, and sometimes members do not have even virtual contact with their fellow members. It is assumed that the majority of them carry out criminal activities using a number of web-based forums devoted to online crime[55] or Internet Relay Chats (IRC),[56] anonymous channels where members know each other only by their nicknames.

Both web forums and IRC channels are operated by administrators and both serve the same goal of being a platform for illegal activities. However, forums seem to be a more sophisticated way of organising criminal activity online, because they have a peer-review process that every potential vendor needs to go through before status is granted – in order to ensure that only trustworthy people obtain access to the illegal goods and services traded on the underground markets.[57] In contrast, virtually anyone can use IRCs for advertising purposes, which makes them more likely to admit law enforcement agents or unreliable (to other criminals) criminals. As a solution, IRCs offer services to check the validity of the data offered for sale.[58]

Speculation and debate as to the professionalism and organisation of criminal groups online are actually fuelled by the nature of such forums, because they can be considered more as tools for collaboration between individuals loosely connected to each other than as platforms for highly organised groups.[59] Nevertheless, it is obvious that there is a certain level of organisation occurring on these platforms, at least on the adminis-

trative level. Yet recent studies contradict the assumption that organised crime in global networks is organised only on an administrative level or relates only to flexible non-hierarchical "networks" with no links to traditional organised crime. They point out that there is already a movement toward long-term organised criminal activities in cyberspace.[60] For example, Symantec experts state that there is significant evidence that organised crime is involved in many cases involving the online underground economy.[61]

Concerning the size of the cybercrime groups (or networks), the estimates vary from 10 to several thousand members, when the affiliated networks are incorporated into the bigger and more complex structures. Regardless of the number of members and affiliates, virtual criminal networks are usually run by a small number of experienced online criminals who do not commit the crimes themselves but rather act as entrepreneurs.[62] The criminal structures collaborate in teams where the roles are defined and the labour is divided.[63] For instance, the first group writes a malicious code, such as a "Trojan"; the next group is responsible for the distribution and use of the malicious software on the Internet; yet another group collects data from the illegal platforms and prepares everything for the identity theft. These data may then be used by other groups of offenders: they can be either sold or supplied as a part of collaboration efforts.[64] The leading members of the networks divide the different segments of responsibility (spamming, controlling compromised machines, trading data) among themselves. There are some "elite" criminal groups that act as closed organisations and do not participate in online forums because they have enough resources to create and maintain the value chains for the entire cycle of cybercrime themselves and therefore have no need to outsource or to be involved as outsiders in other groups.

Due to the fact that the cybercrime industry, though already powerful, is still in the early stage of its development, there is a lack of data related to this phenomenon, especially concerning the actual level of its organisation. Thus, the main problem of assessing the structure of organised cybercrime groups is that there is much more information about what they are doing – or can possibly do – and what harm they can cause than about *who* is behind those groups.[65] Moreover, it is assumed that a single individual or group of perpetrators can play separate or simultaneous roles (developers of malware, buyers, sellers, enablers, administrators) in the cybercrime economy, which makes the structure of the illegal market "complex and intertwined."[66] Recent studies on organised criminality have pointed out that in its new eradigital crime is being organised, though it has not yet been consolidated.[67] Thus, we are now witnessing the process of evolution of organised cybercrime – and the results are still unforeseeable.

IV. Conclusion: Addressing the Problem

Fighting cybercrime has always been a complex task. It extends beyond national borders and spans different jurisdictions.[68] Committing crime in cyberspace is easy, fast, and relatively safe for cybercriminals: Intangible computer data can be quickly and easily transferred around the globe via computer networks and offenders have no need to be present at the same location as the target.[69] At the same time, cybercrime investigations take a lot of time and effort due to the international scale of the crime.[70] While the information society struggles with the problem of harmonisation of cybercrime legislation and cooperation on an operational level to investigate crimes and prosecute cybercriminals, organised criminal groups in cyberspace, both traditional ones and those operating solely online, remain – and probably will continue to remain – several steps ahead of legislators and law enforcement agencies. C2C networks are very likely to continue benefiting from anonymous communication, automation of attacks, and the difficulties that law enforcement agencies experience in determining locations: Servers with crimeware could be in one country, while members of the network could be in another one, targeting victims across the world.

In addition to strengthening the current legal frameworks, updating old legislation, and harmonising laws on an international level, what is needed is also cross-sector cooperation on the national level as well as international cooperation in detecting, investigating, and preventing e-crimes committed by organised criminal groups.[71] The development of a comprehensive understanding and a forward-looking approach are required, since organised cybercrime seems to be a moving target. The main goal is to tackle not only the top of the iceberg, like money mules, but also those who are behind the visible face of the underground economy. In this regard, study of the organised online crime phenomenon should help to determine the core nodes of the networks: e.g., targeting the writers of malicious codes is more effective than targeting affiliates operating in the "pay per install" market. Legal frameworks and operational measures aiming to take down botnets' control-and-command centres might be more effective than tackling those who are at the end of botnet distribution chain.

In borderless cyberspace, international collaboration between the states is the key. While some states just do not have the necessary tools to respond to the activities of organised cybercriminals, or may be lacking the technical skills or facing legal drawbacks,[72] organised cybercrime can always find safe digital havens. The development of a common understanding that no country can be safe alone in the global ICT network is very important. The problem of legal harmonisation can be solved only on the global level.[73]

Since there is no clear understanding of the phenomenon of organised criminal groups in cyberspace yet, it is very hard to tackle this developing problem. The process of elaboration of specific legal strategies to tackle online organised criminal groups is still merely in its infancy. With the absence of a global strategy to counter organised cybercrime, the problem is very likely to deepen in the foreseeable future. With the development of ICT networks and the opportunities they offer, organised criminal groups will benefit from the entire range of tools and models available to legitimate economic sectors. The availability of information not only makes them more accessible to organised groups but also easier for them to foster and automate their fraud-committing activities. It can also link more opportunistic criminals to existing criminal networks.

Cybercrime might be going through a transformation into an organised illegal industry, where syndicates are highly sophisticated and very hard to identify. Some cybercrime industries might end up being run solely by organised criminal groups that are constantly seeking the newest technical solutions and the creation of new markets. As a result, it is likely that the cybercrime environment will soon be dominated by criminal organisations, as cybercrime networks that have already become international will multiply opportunities and reach a global scale by exploiting the weaknesses of legal frameworks while searching for safe havens in countries with fewer resources to detect and fight them. In this regard, the problem should be addressed by developing long-term responses that include coordination and a harmonisation of efforts on both the national and international levels.

Dr. Tatiana Tropina
Max Planck Institute for Foreign and International Criminal Law

1 SecureWorks (2010). The Next Generation of Cybercrime: How it's evolved, where it's going. Executive Brief. Available at: secureworks.com.
2 Williams, P. (2002). Organized crime and cyber-crime: Implications for business. Available at: http://www.cert.org/archive/pdf/cybercrime-business.pdf; UNODC, 2010. Globalisation of Crime. A Transnational Organised Crime Threat Assessment. Available at: http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf; McCusker, R. 2006. Transnational organised crime: Distinguishing threat from reality. *Crime Law and Social Change* 46, 257–273.
3 BAE Systems Detica. 2012. Organised crime in the digital age: The real picture. Executive Summary. Available at: http://www.baesystemsdetica.com/uploads/resources/ORGANISED_CRIME_IN_THE_DIGITAL_AGE_EXECUTIVE_SUMMARY_FINAL_MARCH_2012.pdf.; Ben-Itzhak, Y. 2008. Organized cybercrime. *ISSA Journal* (October). Available at: https://dev.issa.org/Library/Journals/2008/October/Ben-Itzhak-Organized%20Cybercrime.pdf; Rush, H. et al. 2009. Crime online. Cybercrime and Illegal Innovation. NESTA Research Report. July. Available at: http://www.eprints.brighton.ac.uk/5800/01/Crime_Online.pdf; KPMG. 2011. Cyber crime – A growing challenge for governments. Issues monitor. Vol. 8, 3. July, p. 5; Council of Europe. 2004. *Summary of the organised crime situation. Report 2004: Focus on threat of cybercrime*. Council of Europe Octopus Programme. Strasbourg, September 6. Available at: http://www.coe.int/.
4 Williams (2002) *op. cit.* (fn. 2) p. 2.
5 Goodman, M. (2010). International dimensions of cybercrime. In: S. Ghosh and E. Turrini (eds.): *Cybercrimes: A multidisciplinary analysis*. Berlin and Heidelberg: Springer-Verlag; Rush et al. (2009), *op. cit.* (fn. 3) p. 3.
6 Shelley, L. (2003). Organized crime, terrorism and cybercrime. In: Bryden and Fluri (eds.): *Security Sector Reform: Institutions, Society and Good Governance*. Baden-Baden: Nomos Verlagsgesellschaft, p. 307, Williams (2002), op. cit. p. 2.
7 McCusker (2006), *op. cit.* (fn. 2) p. 257.
8 Williams (2002) *op. cit.* (fn. 2) p. 1.
9 Brenner, S. (2002). Organized cybercrime? How cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law & Technology* 4(1) (Fall). p. 25.
10 Goodman (2010), *op. cit.* (fn. 5) p. 313; Europol. 2011. Threat assessment (abridged). Internet facilitated organised crime. iOCTA. File No.: 2530–264. The Hague. January 7. Available at: https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf. p. 5.
11 BAE Systems Detica (2012) *op. cit.* (fn. 3) p. 2; Ben-Itzhak (2008), *op. cit.* (fn. 3)
12 Europol (2011), *op. cit.* (fn. 10) p. 4.
13 Fallmann, H., G. Wondracek, and C. Platzer (2010). Covertly probing underground economy marketplaces. Vienna University of Technology Secure Systems Lab. Available at: http://www.iseclab.org/papers/dimva2010_underground.pdf. p. 1.
14 For example, credit card details cost $2-$90 per item; prices for bank account credentials with guaranteed balance range from $80 to $700 according to Panda Security (2010). Prices for different credentials vary, depending on the amount of funds available, the location, and the type of account: corporate accounts might cost more than double that of personal bank accounts; EU accounts are advertised at a considerably higher cost than their US counterparts, according to Symantec (2008).
15 Cardenas, A. et al. (2009). An economic map of cybercrime. The 37th Research Conference on Communication, Information and Internet Policy (TPRC). Arlington, VA: George Mason University Law School. September. p. 1; Europol (2011), *op. cit.* (fn. 10) p. 4.
16 Kshetri, N. (2010). The global cybercrime industry. Berlin and Heidelberg: Springer-Verlag. p. 190.
17 BSI (Bundesamt für Sicherheit in der Informationstechnik) (2011). Available at: https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile. p. 4
18 BKA (Bundeskriminalamt). 2010. Cybercrime. Bundeslagebild 2010. Available at: http://www.bka.de/nn_193360/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true.
19 Offences subsequently lead to other offences, for example, attacks lead to stealing information, and then stolen information can be sold and used by those who bought it to commit fraud.
20 Grabosky, P. (2007). The internet, technology, and organized crime. *Asian Criminology* 2, p. 156.
21 Kshetri (2010), *op. cit.* (fn. 16) p. 189.
22 Rush et al. (2009), *op. cit.* (fn. 3) p. 37.
23 Ben-Itzhak (2008), *op. cit.* (fn. 3) p. 38.
24 ESET (2010). 2010: Cybercrime coming of age. White paper. January, 2010. Available at: http://go.eset.com/us/resources/white-papers/EsetWP-Cybercrime-ComesOfAge.pdf. p. 4.
25 Europol (2011), *op. cit.* (fn. 10) p. 6.
26 Ibid.
27 Barroso, D. (2007). Botnets – The silent threat. ENISA Position Paper No. 3. Available at: http://www.dihe.de/docs/docs/enisa_pp_botnets.pdf. p. 7.
28 Danchev (2010). Study finds the average price for renting a botnet. Available at: http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528

29 McAfee (2012). McAfee Threats Report: First Quarter 2012. Available at: http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q1-2012.pdf.
30 Danchev (2012). DDoS for hire services offering to 'take down your competitor's web sites' going mainstream. Avaliable at: http://blog.webroot.com/2012/06/06/ddos-for-hire-services-offering-to-take-down-your-competitors-web-sites-going-mainstream/.
31 SecureWorks (2010), *op.cit.* (fn. 1).
32 Caballero, J., C. Grier, C. Kreibich and V. Paxson (2011). "Measuring pay-per-install: the commoditization of malware distribution," Proceeds of the USENIX Security Symposium, August 2011. Available at: http://www.icir.org/vern/papers/ppi-usesec11.pdf.
33 SecureWorks (2010), *op.cit.* (fn. 1).
34 Anti-Virus software.
35 Trend Micro (2010). The business of cybercrime. A complex business model. Focus Report Series. January. Available at: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_business-of-cybercrime.pdf.
36 SecureWorks (2010), *op.cit.* (fn. 1); Ben-Itzhak (2008), op.cit. (fn. 3) p. 38.
37 SecureWorks (2010), *op.cit.* (fn. 1)
38 Panda Security (2010). Panda Security Report. Cybercrime Black Market: Uncovered. Available at: http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf.
39 Council of Europe (2012). Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction. Available at: http://www.coe.int/t/dghl/monitoring/moneyval/typologies/MONEYVAL(2012)6_Reptyp_flows_en.pdf; Kshetri (2010), *op.cit.* (fn. 16) p. 177.
40 Europol (2011), *op.cit.* (fn. 10)
41 Panda Security (2010), *op.cit.* (fn. 38).
42 Council of Europe (2012), *op.cit.* (fn. 39).
43 Cisco (2011). Cisco 2010 annual security report. Highlighting global security threats and trends. Available at: http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf. p. 9.
44 Ibid.
45 Council of Europe (2004), *op.cit.* (fn. 3) p. 2.
46 Rush et al. (2009), *op.cit.* (fn. 3) p. 42.
47 Europol (2011), *op.cit.* (fn. 10) p. 5.
48 UK Home Office. 2010. Cybercrime strategy. Stationery office limited on behalf of the controller of Her Majesty's Stationery Office. p. 12.
49 Rush et al. (2009), *op.cit.* (fn. 3) p. 35.
50 Council of Europe, (2004), *op.cit.* (fn. 3) p. 7.
51 UK Home Office (2010), *op.cit.* (fn. 48) p. 13.
52 Brenner (2002), *op.cit.* (fn. 9) p. 27; Choo, K., and R. Smith (2007). Criminal exploitation of online systems by organised crime groups. *Asian Criminology* 3: 37–59. p. 41.
53 United Nations. 2010. Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime. Working Paper prepared by the Secretariat. Twelfth United Nations Congress on Crime Prevention and Criminal Justice. V.10-50382 (E) 100210 110210. Salvador, Brazil. April 12–19. p. 10.
54 Choo, K. 2008. Organised crime groups in cyberspace: A typology. *Trends Organ Crim* 11, p. 7.
55 Symantec. 2008. Symantec report on the underground economy: July 7–8. November. Available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf. p. 5, Rush et al. (2009), *op.cit.* (fn. 3).
56 Fallmann et al. (2010), *op.cit.* (fn. 13), p. 1.
57 UK Home Office (2010), *op.cit.* (fn. 48) p. 12.
58 Rush et al. (2009) *op.cit.* (fn. 3) p. 50.
59 Symantec (2008), *op.cit.* (fn. 55) p. 5.
60 BAE Systems Detica (2012), *op.cit.* (fn. 3).
61 Symantec (2008), *op.cit.* (fn. 55).
62 UK Home Office (2010), *op.cit.* (fn. 48).
63 Rush et al. (2009) *op.cit.* (fn. 3) p. 42.
64 BSI (2011), *op.cit.* (fn. 17) p. 4.
65 Rush et al. (2009), *op.cit.* (fn. 3).
66 Trend Micro. 2006. Phishing. A trend micro white paper. November. Available at: http://www.antiphishing.org/sponsors_technical_papers/trendMicro_Phishing.pdf. p. 6.
67 BAE Systems Detica (2012), *op.cit.* (fn. 3) p. 2; Symantec (2008), *op.cit.* (fn. 55).
68 Hunton, (2009), *The growing phenomenon of crime and the internet: A cybercrime execution and analysis model.* In: Computer Law&Security Review, Vl. 25, Issue 6, p. 533.
69 Gercke, M. 2012. Understanding cybercrime: A guide for developing countries. ITU, Geneva; Joffee, (2010), Cybercrime: the global epidemic at your network door. In: Network Security 01/2010; 2010.
70 Bradbury, (2012), *When borders collide: legislating against cybercrime*. In: Computer Fraud & Security, Vol. 2012, No. 2. (February 2012), pp. 11-15.
71 Europol (2011), *op.cit.* (fn. 10).
72 Goodman (2010), *op.cit.* (fn. 5).
73 Sieber, U. (2008). *Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law.* In: M. Delmas-Marty, M. Pieth, and U. Sieber (eds.): *Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law.* Collection de L'UMR de Droit Comparé de Paris. Paris: Société de législation comparée, 127–202.

Anti-Money Laundering: New Obligations Imposed by the 2012 Guardia di Finanza Circular in Italy

Dr. Maria Cristina Bruno

The initial source of the money laundering legislation that is still in full development is Directive 1991/308/EU (also known as the "first directive") on prevention of the financial system from laundering the proceeds of criminal activities. Directive 2001/97/EU (the "second directive") on the subject of prevention of employment of the financial system for laundering the proceeds of illicit activities demands a higher standard of obligations on the part of the Member States and extends the scope of the subjects upon whom such obligations are imposed.

Italian Legislative Order 231/2007 brings into effect the Directive 2005/60/EU (the "third directive"). It introduces nu-

merous new features applicable to professional persons[1] and imposes upon them somewhat burdensome obligations, the practical implementation of which is not always fully clear. The Guardia di Finanza (Italian Finance Police) recently intensified their monitoring of the legality of professionals' operations insofar as they are viewed as one of the possible laundering channels. Their offices and chambers, in fact, constitute meeting places in which clients and financial brokers can collaborate. In some cases, the business transacted therein may be directed toward the concealment of dirty money.

I. Professional Persons

Ministerial Order of 4 May 2012[2] prescribes that certified public accountants and accounting professionals may report suspected laundering operations to the Consiglio Nazionale[3] (C.N.) instead of the Unità di Informazione Finanziaria (U.I.F.)[4] if they know, suspect, or have plausible reasons for suspecting that laundering or funding of terrorism operations are in progress or have been implemented or attempted. The C.N. forwards these reports to the U.I.F. and ensures the anonymity of the informant. The anti-money laundering provisions require that certified professionals fulfill several functions when submitting such reports:

Consultative functions

- in connection with the promulgation by the Ministry of Justice of provisions requiring registration for professional persons;
- in connection with the periodic updating of the grounds for suspicion by the Ministry of Justice as proposed by the U.I.F.

Active collaborative functions

- supplying the U.I.F. with information and other forms of collaboration as needed;
- forwarding, within the time limits that have been laid down, any notifications of suspicious operations received from their members.

Surveillance and checking functions

- promoting and checking compliance, from professional persons, with their anti-money laundering obligations;
- adoption of sufficient staff training measures.

Their power of surveillance is not exclusive, however, insofar as inspections can also be carried out by the Nucleo Speciale di Polizia Valutaria della Guardia di Finanza (N.S.P.V., G.d.F.).[5]

II. Checks by the Guardia di Finanza

The Italian police forces endowed with an important role in preventing and countering employment of the financial system for recycling operations and the funding of terrorism are the N.S.P.V. and the Direzione Investigativa Antimafia (D.I.A.).[6] They are entrusted with the task of undertaking the in-depth investigation of the reports received from the U.I.F. by means of the anti-money laundering legislation.

1. The Guardia di Finanza's Powers and Limits

Legislative Order 231/2007[7] has conferred upon the Guardia di Finanza:

a) the freedom to avail itself of data in the client register of banks, as part of its in-depth investigation of notifications and anti-money laundering inspections;

b) the possibility to delegate such investigation to all its sections;

c) electronic transmission of reports of suspicious operations and exchanges of information;

d) the possibility to investigate persons subject to surveillance on the part of other authorities.

If its inquiries disclose taxation offences, the N.S.P.V. may take direct and independent action insofar as it is both a tax and a currency police offence.

2. Ways and Means of Checking Professional Persons

The checking of professional persons may be the outcome of:

- a report made by a professional person himself to the U.I.F. with respect to operations and/or services called for by one of his clients who felt at risk of money laundering or funding of terrorism;
- inquiries by the N.S.P.V. relating to a client of the said professional for the purpose of acquiring information possessed by the latter;
- an assumption of failure to report, by a professional person, with respect to operations and services furnished to a client who is already the subject of an investigation;
- investigation of the limitation of the use of cash by a client;
- inspections undertaken to determine the correct application of the anti-money laundering regulations.

As to the investigations that may be generated by a report to the U.I.F. concerning a suspect operation, the procedure lays down that, upon receipt of a report, the N.S.P.V. shall conduct a preliminary check in the form of a pre-investigative analysis. This step may lead to:

- no further assessment of the report because the amount of the operation and the reason for it, along with other features of the case, are not sufficient to support assumptions of money laundering;

- no further development of the report because the matter is already the subject of judicial proceedings;
- in-depth examination of the report.

In the latter case, the professional person may be required to produce copies of all documentation in his possession relating to the operation thus reported as well as information on all the operations registered and identified; next, the firm's premises may be accessed for further examination and investigation that may reveal breaches of the anti-money laundering regulations, evidence, and elements pointing to the commission of crimes, situations of significance in taxation terms, etc.

It should be recalled that criminal acts stemming from crime may relate to "bodies endowed with a legal personality," associations, foundations, joint-stock companies and partnerships, public bodies, foreign companies operating in Italy, and individual firms.

Decision No. 18941/2004 of the Corte di Cassazione (Supreme Court of Appeal) initially ruled that administrative liability could only be attributed to bodies endowed with a legal personality in a company or having a mixed form, resulting in the exclusion of individual firms. In Decision No. 15657 of 21.04.2011, however, this Court altered course and held that an individual firm can be likened to a legal person and absorbs the natural person who actually runs the business.

3. Anti-Money Laundering Inspections

For their so-called "sampling" anti-money laundering inspections, the N.S.P.V. or the Italian Finance Police use the powers they employ for their in-depth examination of reports of suspect operations.

In the case of professional persons, such inspections set out the following:
a) to check their correct and exact compliance with the obligations imposed by the anti-money laundering legislation;
b) to counter laundering of illicit earnings at the preliminary stage;
c) to prevent, seek out, and repress administrative and criminal offences emerging during the checking operations.

During the course of an inspection, as a first step a professional person will be required to produce the documents relating to his clients and to allow consultation of his Archivio Unico Informatico (A.U.I.)[8] or its paper copy. Duly authorized police officers may enter the professional's premises, look for papers and exchanges of information (e-mail inspection), and finally issue a report in two copies. In keeping with the provisions of form 6 (checking of legal and accounting professionals),[9] they will continue by calling for the list of the general particulars of the person's clients with indication of the date on which they did business. The next step is monitoring whether the business relationship was sufficiently screened in advance, together with the list of operations and professional services rendered, subdivided according to purpose of the amounts involved. Attention will be paid to operations and services relating to clients whose names appear most frequently, or those who have made conferments or capital contributions to companies with goods in kind for amounts patently out of proportion to their market value, or those who have availed themselves of services directed to structured financing of transnational significance.

Other selection criteria will focus on clients with criminal, tax, or police records for offences for the purpose of gain, with evident incongruity between the amount of the operation undertaken and their earning capacity and, lastly, those classified as "persons politically exposed", trustee companies, etc.

The second step is acquisition of all the documentation held by the professional person (including e-mails) followed lastly by processing of all the material collected. An examination will be made of the identification and verification of the client and the effective proprietor in terms of time, ways and means of execution, and acquisition of the information concerning the purpose and nature of the services. These measures may result in the detection of:
- administrative breaches;[10]
- situations of substantial importance in taxation terms for use in a subsequent review of the client's fiscal position;
- criminal offences, with forwarding of the information to the Director of Prosecutions.

The G.d.F. will devote particular attention to assumptions of criminal liability regarding a client who has deliberately omitted or falsified information about the reason and the nature that is expected from the professional service, whether alone or in collusion with the professional person's associates or employees.[11]

III. Administrative Sanctions

- Failure to comply with an order to suspend the suspicious operation: fine between €5000 and €200,000;
- Failure to abstain from the establishment or cessation of a continuous relationship, execution of professional operations or services that directly or indirectly involve trustee companies, trusts, anonymous companies, or companies controlled by holders of bearer shares located in countries listed by the Ministry for the Economy and Financial Affairs:
  – fine of €5000 for operations not exceeding €50,000

– fine ranging from 10 to 40% for operations exceeding €50,000
– fine ranging from €25,000 to €250,000 if the amount of the operation is not determined or not determinable;

■ Failure to keep a clientele register and/or to adopt other ways and means of registration: fine of €5000 to €50,000;

■ Failure to report suspected operations: fine ranging from 1 to 40% of the amount of the operation not reported;

■ Breach of the obligations to inform the U.I.F.: fine of €5000 to €50,000;

■ Failure to notify the relevant Ministry of infractions encountered: fine ranging from 3 to 30% of the amount of the operation, the balance of the bank book or the account.

IV. Criminal Sanctions

■ Omitted, tardy, or incomplete registration: fine of €2600 to €13,000;

■ Breach of the obligation to identify the client: fine of €2600 to €13,000;

■ Discharge of identification and registration obligations by resorting to fraudulent practices, e.g., impeding identification of the author of an operation constitutes an aggravating circumstance that doubles the penalties imposed;[12]

■ Omission of communications by a board of auditors, surveillance committee, management supervision committee, the body named in sect. 6, first para., and all persons charged with the inspection of management: imprisonment up to one year and a fine of €100 to €1000;

■ Violation of the prohibition of the communication of a completed report of a suspected operation other than in the cases envisaged by Legislative Order No. 231/2007: arrest for 6 months to one year and fine of €5000 to €50,000.

Practical Measures for the Avoidance of Sanctions

According to the specialized media, a very large number of professional offices are running the risk of closure as the result of anti-money laundering sanctions. In most cases, the regulations are being poorly applied due to insufficient and/or false information.

An inspection has the following ascertainment objectives:

■ sufficient verification of the business relationship;

■ storage of data and the corresponding establishment of a client's file;

■ preparation of the business relationship register or the A.U.I. and recording of the data;

■ effective reporting of operations suspected of money laundering or the funding of terrorism;

■ communication to the M.E.F.[13] of instances of the wrongful employment of cash.

With regard to client identification, the G.d.F. determines whether it has been founded on reliable documents, whether the identity of the actual proprietor has been ascertained and checked, and whether information has been gathered concerning the purpose and nature of the professional service requested as well as the subsequent monitoring of the information during the course of the relationship. As to the recording of data, the aim is to determine whether it has been completed within the required term of 30 days, following acceptance of the professional engagement, or whether this information can be derived from any subsequent knowledge of the operations, or from the termination of the professional service.

The G.d.F. primarily looks for instances of failure to report to the U.I.F. and determines the pathway that led the professional person to remain unaware of the suspicious nature of a particular service. As matters now stand, the professional person's greatest risk stems from the acquisition of insufficient information about a new client. It is thus advisable to draw up an appropriate risk profile right from the start and to review it from time to time. In the case of suspicious operations forwarded by a professional person, the G.d.F. makes sure they are handled in accordance with the confidentiality provisions.[14] A final check to which a professional person may be subjected relates to the limitation of the use of cash. Salva Italia Order No. 201/2011 of 06.12.2011 prescribes immediate application of the limit of €1000.

Persons indicated in sect. 51 of Legislative Order 231/2007, which comprises professionals, are required to communicate and notify breaches to the M.E.F. The M.E.F., after checking the completeness of the report, has 90 days to inform the author of the breach that the G.d.F. will be notified. This is followed by a preliminary examination during which memorials by the defense may be lodged. A sanction is then imposed or the case is dismissed on the merits and shelved for procedural reasons. The proceedings end with termination. Following notification of the decision and expiry of the time for lodging an appeal, the office must send a letter calling for payment prior to the possible entry of the case on the lists by Equitalia.[15]

V. Anti-Money Laundering Reporting and Questions of Confidentiality and Professional Secrecy

The right to secrecy is a special form of the right to confidentiality. It safeguards a person's interest by not allowing others to know an item of information or private data. Pro-

fessional secrecy involves features that may have an impact on a professional's deontological, criminal and civil liability. Particular attention is obviously directed at the question of secrecy in the case of data and information of which a professional person has gained knowledge via a fiduciary relationship established with his client for the purpose of fulfilling a professional engagement.

The substantial breach of a right inflicted by the anti-money laundering and antiterrorism legislation thus has an impact on rights that our judicial system views as worthy of protection.What is at stake, indeed, is the fair and reasonable equilibrium that needs to be established between common values, so as not to sacrifice civil rights and freedoms to ensure public order and national security. One cannot overlook the fact that the question of the relationship between the anti-money laundering legislation and professional secrecy is not confined to safeguarding the right to defend oneself and have access to justice – it extends to the protection of a citizen's right for access to the law. Resorting to a legal consultant to secure a better understanding of rules and regulations is a vital right.

The anti-money laundering and antiterrorism legislation is thus compelled to prescribe that reports to the U.I.F. do not constitute breaches of the obligations of confidentiality and professional secrecy. Hence, they do not give rise to any kind of liability, whether civil, criminal, or administrative for professional persons and their employees and collaborators, provided that such reports are made as follows:

- for the purposes envisaged by the legislation: professionals are required to be familiar with the legislation in order to avoid unwarranted reports that could harm the client and obviously expose the incautious informant to criminal sanctions as well as those inflicted for his unjustified breach of the obligation of professional secrecy;
- in good faith: the considerations set out above have a greater impact whenever an unjustified report is presented in good faith and not as the outcome of ignorance or carelessness.

Even so, the fact remains that the rules laid down in Legislative Order No. 231/2007 "unload" upon professional person's substantial and often unreasonable obligations that conflict with the interests of their clients and assurances of anonymity.

VI. Conclusions

In view of the limits arising from the anti-money laundering legislation, the European Commission has set out to revise the "third directive," which is centered on the aspects associated with reporting obligations and their link with the safeguarding of personal data, together with corrective measures designed to strengthen the relationships between the regulating authorities. Furthermore, the Italian governing body of the Gruppo d'Azione Finanziaria Internazionale (G.A.F.I.)[16] has given the green light for the publication of its new indications drawn up to define the worldwide standards to be applied in the fight against money laundering and due to become law in many countries.

The new text furnishes more incisive tools for countering the illicit use of the financial system. It promotes greater transparency on the part of legal persons and identifies international cooperation as the key to the struggle against financial crime.

Dr. Maria Cristina Bruno
Certified Public Accountant, Tax Consultant, Journalist, Vice-President, Centre for Criminal Tax Law (C.D.P.T.), based in Turin (Italy)

1 For the purpose of this article, the term "professional persons" refers to natural and legal persons as meant by article 2 of Directive 2005/60/EU.
2 Gazzetta Ufficiale (Official Gazette) No. 110,12.05.2012.
3 National Council.
4 Financial Information Unit.
5 Special Currency Police Unit of the Italian Finance Police.
6 Antimafia Investigation Board.
7 D.Lgs. Decreto legislativo (Legislative Order).
8 Centralised Computer Archive.
9 G.d.F. Circular No. 83607, 19.03.2012.
10 Sects. 57 and 58 of Legislative Order No. 231/2007.
11 Sect. 55 para. 3 of Legislative Order No. 231/2007.
12 Sect. 55 paras. 1-2-4 of Legislative Order No. 231/2007.
13 Ministero Economia e Finanze (Ministry for the Economy and Financial Affairs).
14 Communication U.I.F. 23.04.2012.
15 Equitalia is a national tax collection agency.
16 Financial Action Task Force – F.A.T.F.

Legal Nature of European Union Agricultural Penalties

Comments on the ECJ Ruling in Case C-489/10 Ł. Bonda

Dr. Justyna Łacny / Dr. hab. Monika Szwarc

Excluding a farmer from receiving a single area payment in a given year and reducing the payment he could claim within the following years, imposed as a penalties for the breach of the EU agricultural provisions, do not constitute criminal sanctions. They are specific administrative instruments applied against the farmer who had decided to participate in an agricultural aid scheme. In such a case, the *ne bis in idem* principle does not apply. Thus, exclusion and reduction of agricultural payments do not preclude sentencing the farmer in criminal proceeding for the same breach of the EU agricultural provisions. This conclusion follows from the judgment of the European Court of Justice (ECJ) delivered on 5 June 2012 in case C-489/10 criminal proceedings against Ł. Bonda.

I. Background of the *Bonda* Case

In May 2005, Łukasz Bonda, a Polish farmer, submitted an application to the local agricultural paying agency[1] for a single area payment for 2005. In his application for payment, he overstated the area used for agriculture by giving a figure of 212.78 hectares instead of 113.49 hectares. The paying agency discovered the false information and reduced the single area payment available to him for 2005 up to the amount of the difference between the real area and the area declared. It also excluded him from payments for the three years following the year 2005. Exclusion and reduction were imposed on the basis of Art. 138 (1) paragraph 2 and 3[2] of Regulation 1973/2004.[3] Then, the Prosecutor initiated a criminal proceeding against Ł. Bonda and, on 14 July 2009, the District Court convicted him of subsidy fraud, defined in Art. 297(1) of the Polish Criminal Code.[4] The District Court stated that Ł. Bonda made a false declaration to obtain an unjustifiably high amount of a single area payment and sentenced him to eight months of imprisonment, suspended for the three years, and a fine of 1600 Polish zloty (approx. € 400). The farmer appealed to the Regional Court, which set the contested judgement aside. The Regional Court stated that the criminal proceeding was inadmissible because administrative penalties, consisting of exclusion and reduction, had already been imposed on Ł. Bonda for the same act. In consequence, due to the *ne bis in idem* principle, as envisaged in Art. 17(1)(11) of the Criminal Procedure Code (CPC),[5] it discontinued the criminal proceeding. The Principal Public Prosecutor filed an appeal against this verdict to the Supreme Court, arguing that the Regional Court infringed Art. 17(1)(11) CPC. The Supreme Court considered that in order for such a statement to be made, it must determine whether the proceedings launched by the agricultural paying agency may be regarded as criminal proceedings within the meaning of Art. 17 (1)(11) CPC. It declared that, while a literal interpretation of this provision requires the question to be answered in the negative, it must be interpreted in the light of Art. 4(1) of Protocol No. 7 to the European Convention of Human Rights (ECHR) establishing the *ne bis in idem* principle. Considering that the legal nature of the exclusion and reduction imposed on the basis of Art. 138 (1) paragraph 2 and 3 of Regulation No. 1973/2004 must be assessed, the Supreme Court referred a preliminary question to the ECJ, asking whether these provisions constitute criminal penalties.

As the preliminary question of the Polish court considered only the legal nature of the penalties envisaged in Art. 138 (1) of Regulation 1973/2004, the ECJ limited its considerations to this issue. The ECJ ruling, however, raises a fundamental question of application of the *ne bis in idem* principle in the national case. Therefore, commentary on the *Bonda* case requires a twofold approach: it must focus on the legal nature of penalties imposed for the breach of the EU agricultural provisions as well as on application of the *ne bis in idem* principle.

II. Penalties Imposed for Breaches of the Union's Agricultural Legislation

1. Case-law of the European Court of Justice on Penalties Imposed for Breaches of the Union's Agricultural Legislation

The ECJ had many occasions to express its view on the legal nature of penalties imposed for breaches of the EU agricultural provisions. Already in the 90s, in the case C240/90 *Germany*

v Commission, it stated that temporary exclusion of an operator from an aid scheme due to the irregularities committed by him does not constitute a criminal sanction.[6] Then, in case C210/00 *Käserei Champignon Hofmeister,* the ECJ analysed whether a penalty established in agricultural regulation could be regarded as being of a criminal nature. The case concerned provisions establishing a fine as a penalty for false declarations in an application for an export refund. The question arose as to whether such a fine had to be assessed in the light of the *nulla poena sine culpa* principle. The ECJ answered this question in the negative, explaining that the penalty at issue was an integral part of the export refund scheme and not of a criminal nature.[7]

Analysing the legal nature of the penalties, the ECJ underlines that exclusion, as a type of a penalty foreseen in the EU agricultural legislation, may be imposed only on a farmer who has chosen to take advantage of an agricultural aid scheme.[8] In such a case, proceedings launched against farmers under EU legislation are not of a criminal nature. The ECJ also examines the objectives of the penalties. It states that exclusion is intended to combat numerous irregularities, which are committed within the framework of EU agricultural aid. Because these irregularities weigh heavily on the EU budget financing implementation of the Common Agricultural Policy (CAP), exclusions are of such a nature as to jeopardise the actions undertaken by the EU's institutions in the agricultural field, stabilise markets, support the standard of living of farmers, and ensure that supplies reach consumers at reasonable prices.[9] Moreover, under EU agricultural aid, schemes granting the aid are subject to the condition that the beneficiary offers all guarantees of probity and trustworthiness. The penalty imposed in the event of non-compliance with these requirements therefore intends to ensure the sound financial management of EU public funding.[10]

In the above-mentioned jurisprudence, the ECJ applied two conditions that are decisive for claiming that agricultural penalties, *in casu* exclusions and reductions, are not of a criminal nature; thus, they are administrative ones. Firstly, they may be imposed only on farmers who, on the basis of their own decisions, participate in the agricultural aid schemes. Secondly, the ECJ aligned the administrative nature of penalties with their objectives. They are intended to ensure that goals of the CAP are accomplished and that the EU funds allotted for its implementation are spent properly, so that the financial interests of the EU are duly protected, as required by Art. 325 of the Treaty on the Functioning of the European Union (TFEU). From this perspective, the ECJ declares that penalties imposed for breaches of the EU agricultural provisions constitute "a specific administrative instrument forming an integral part of the scheme of aid."

The same rationale was applied in the *Bonda* case. The ECJ reiterated that only farmers who have applied for a single area payment under Regulation No. 1973/2004 and provided false information in the application for aid can be subject to the exclusions and reductions foreseen in this Regulation. The ECJ also found that exclusions and reductions constitute a specific administrative instrument forming an integral part of an aid scheme intended to ensure the sound financial management of EU public funds. The ECJ also reiterated Regulation No. 2988/95 on the protection of the EU's financial interests,[11] which, as a horizontal (general) legal act, applies to all EU policies, including CAP. This Regulation foresees that the total or partial removal of an advantage granted by EU rules, even if the operator has wrongly benefited from only a part of that advantage, as well as the exclusion from or withdrawal of an advantage for a period subsequent to that of the irregularity, constitutes administrative penalties (Art. 5(1) (c) and (d) of Regulation No. 2988/95). This Regulation also foresees that the administrative penalties laid down in pursuance of the CAP objectives form an integral part of the aid schemes; they have a purpose of their own and may be applied independently of any criminal penalties, if and in so far as they are not equivalent to such penalties (Art. 6(1) to (5) of Regulation No. 2988/95).

2. Legal Notion of "Criminal Proceedings" in the Case-law of the European Court of Human Rights (ECtHR)

After excluding the criminal nature of exclusions and reductions foreseen in Art. 138 (1) paragraph 2 and 3 of Regulation No. 1973/2004 in the context of its own case-law, the ECJ analysed whether the same conclusion would be valid if conditions formulated in the case-law of the European Court of Human Rights (ECtHR) would apply. The ECJ made this reference because the *ne bis in idem* principle is established both in Art. 50 of the Charter of the Fundamental Rights (Charter)[12] and in Art. 4 (1) of Protocol No. 7 to ECHR. This analysis allowed the ECJ to comply with the requirement of homogeneity, which stipulates that rights contained in the Charter are to have the same meaning and scope as the corresponding rights guaranteed by the ECHR, as interpreted by the case-law of the ECtHR (Art. 6 (1) third subparagraph Treaty on European Union and Art. 52 (3) of the Charter).[13]

As a point of departure, the ECJ took the *Engel* case,[14] in which the ECtHR formulated a concept of "criminal proceedings" within the meaning of Art. 4 (1) of Protocol No. 7. According to this judgement, three conditions are decisive for stating that proceedings are of a criminal nature. The first is the legal classification of the offence under national law, the second is the very nature of the offence, and the third condition

relates to the nature and degree of severity of the penalty that the person concerned is liable to incur.

As regards the legal classification of the offence under national law (the first *Engel*'s condition), the ECJ stated that, in the *Bonda* case, "national law" in the meaning of the case-law of the ECtHR must be equated with "EU law." Then, the ECJ found that, under EU law, the exclusion and reduction provided for in Art. 138 (1) paragraph 2 and 3 of Regulation No. 1973/2004 are not regarded as being criminal in nature. As concerns evaluation of the very nature of the offence (the second *Engel*'s condition), the ECJ stated that it must be ascertained whether the purpose of the applied exclusion and reduction is punitive. It then declared that they are applicable only to farmers who have recourse to the aid scheme set up by that regulation and that the purpose of these exclusion and reduction is not punitive. They are essentially aimed at protecting the management of EU funds by temporarily excluding a recipient who has made incorrect statements in his application for aid. In addition, a reduction in the amount of aid that may be paid to the farmer for the three years following the irregularity is not absolute, as it is subject to the submission of an application in respect of those years. Thus, if the farmer makes no application for the three following years, the reduction is rendered ineffective. This is also the case if the farmer no longer satisfies the conditions for granting of the aid. Finally, the reduction also becomes partly ineffective if the amount of aid the farmer can claim in respect of the following years is lower than the amount of aid to be withheld pursuant to the measure reducing the aid wrongly paid. The ECJ declared that these arguments exclude the punitive nature of penalties foreseen under the Regulation No. 1973/2004. Finally, the ECJ evaluated the nature and degree of the severity of the penalties that the farmer concerned is liable to incur (the *Engel*'s third condition). The sole effect of the exclusion and reduction is to deprive the farmer of the prospect of obtaining aid. Therefore, the exclusion and reduction cannot be equated with criminal penalties. The ECJ concluded that the characteristics of the applied exclusion and reduction exclude the possibility to consider them criminal penalties.

III. The Ne Bis in Idem Principle

As explained previously, the Polish Criminal Procedure Code considers the *ne bis in idem* principle to be an obstacle to continuing criminal proceedings. According to Art. 17(1), points (7) and (11) of the CPC, "proceedings shall not be initiated, and those initiated shall be discontinued, if: criminal proceedings concerning the same act and the same person have been definitively concluded or those already initiated are continuing (…), there are other circumstances excluding prosecution." For this reason, the Supreme Court asked the ECJ to specify the nature of the penalties envisaged in Art. 138(1) of Regulation No. 1973/2004. As the ECJ ruled that the penalties in question are of an administrative nature, the imposition of administrative penalties on the farmer is not an obstacle to continuing a criminal procedure against him.

The case, nevertheless, raises issues of different nature, as the *ne bis in idem* is not only the principle of Polish criminal procedure but also constitutes an international legal standard. In its preliminary question, the Supreme Court indicated only the ECHR standard (Art. 4 of Protocol No. 7 to the ECHR) and made no reference to the Charter (Art. 50 of it). Nonetheless, the *Bonda* case concerned the application of EU law in the national system of the Member State, which implied the application of the Charter. In consequence, two questions should be answered: the first concerns application of Art. 50 of the Charter to the *Bonda* case; the second refers to interpretation of that article.

Answering the first question, it should be kept in mind that, according to Art. 51(1) of the Charter, the Member States are obliged to respect provisions of the Charter, including Art. 50, only to the extent "they are implementing Union law." This proviso has been interpreted by the ECJ as follows:
1) either that the national provision constitutes "a measure implementing EU law" or is "connected in any other way with EU law;"[15]
2) or that the case "is covered by European Union law."[16]

In the *Bonda* case, the paying agency directly applied Art. 138 (1) of Regulation No. 1973/2004, and the criminal court applied Art. 297(1) of the Polish Criminal Code, which implements the Convention on the Protection of the European Communities' Financial Interests.[17] For this reason, Advocate General Kokott rightly pointed out that "if the obligation can thus arise from the European Union law for the Member States to provide for criminal penalties in respect of risks to the financial interests of the Union in connection with agricultural aid, then conversely the possible limits to this obligation must also arise from European Union law and in particular from the fundamental rights of the European Union. The European Union law obligation to impose criminal penalties for infringements of European Union law can only exist to the extent that the fundamental rights of the persons concerned, which are guaranteed at European Union level, are not affected."[18]

In the context of application of the Charter before the Polish criminal court, another problem arises, concerning the possible limitative character of Protocol No. 30 on the application of the Charter of Fundamental Rights of the European

Union to Poland and to the United Kingdom.[19] In particular, attention shall be paid to Art. 1(1) therein, stating that "The Charter does not extend the ability of the Court of Justice of the European Union, or any court or tribunal of Poland or of the United Kingdom, to find that the laws, regulations or administrative provisions, practices or action of Poland or of the United Kingdom are inconsistent with the fundamental rights, freedoms and principles that it reaffirms."

This clause, however, should not be interpreted as granting to the Member States concerned an opt-out, excluding the application of the Charter on their territories. This view was consequently supported by the Advocates General Trstenjak (case C-411/10 *N.S. and others*[20]) and Kokott (case C-489/10 *Bonda*[21]). It was also expressly confirmed by the ECJ in case C-411/10 *N.S. and others*, when it stated that "Protocol (No. 30) does not call into question the applicability of the Charter in the United Kingdom or in Poland." The ECJ declared that Art. 1(1) of Protocol (No. 30) explains Art. 51 of the Charter with regard to the scope thereof and does not intend to exempt Poland or the United Kingdom from the obligation to comply with the provisions of the Charter or to prevent a court of one of those Member States from ensuring compliance with those provisions.[22]

Apart from the reference to the Charter, it must be underlined that the *ne bis in idem* principle was included in the EU provisions concerning the protection of the EU's financial interests long before the Charter entered into force. The tenth recital in the preamble to Regulation No. 2988/95, reiterated by the ECJ in *Bonda* case, states: "… not only under the general principle of equity and the principle of proportionality but also in the light of the principle of *ne bis in idem*, appropriate provisions must be adopted while respecting the *acquis communautaire* and the provisions laid down in specific Community rules existing at the time of entry into force of this Regulation, to prevent any overlap of Community fines and national criminal penalties imposed on the same persons for the same reasons." After the Charter entered into force, the ECJ confirmed, in the context of national proceedings concerning the imposition of penalties for the breach of EU law on the protection of the EU's financial interests, that the *ne bis in idem* principle is enshrined in Art. 50 of the Charter.[23] For these reasons, the Supreme Court could rather seek to establish the Charter standard of the *ne bis in idem* principle on the basis of Art. 50 of the Charter (as proposed by the AG J. Kokott) instead of referring to the national standard enshrined in the Polish Criminal Procedure Code.

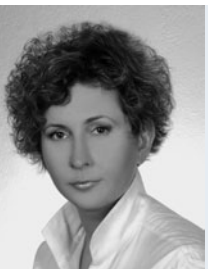
This conclusion leads to the second question concerning the interpretation of Art. 50 of the Charter, stating that "No one shall be liable to be tried or punished again in criminal proceedings for an offence for which he or she has already been finally acquitted or convicted within the Union in accordance with the law." Interpretation of this Article necessitates an integrative approach, including both the jurisprudence of the ECtHR and of the ECJ. On the one hand, according to Art. 52 (3) of the Charter (mentioned earlier in this text), the *ne bis in idem* principle enshrined in Art. 50 of the Charter must be interpreted with reference to Art. 4 of Protocol No. 7 to the ECHR. Possible doubts arise from the fact that this Protocol has not been ratified by all Member States of the Union so far, and the ratifications completed by some of them were made conditional to reservations. This means that the standard established by Art. 4 of Protocol No. 7 is not commonly and unconditionally adopted by all the Member States. Luckily, these doubts are not valid in the case of Poland, which ratified Protocol No. 7, and it entered into force on its territory on 1.3.2003. Moreover, the circumstances concerning the ratifications of Protocol No. 7 by the Member States did not prevent the ECJ from referring to the ECHR standard when it recognized the *ne bis in idem* principle as a general principle of EU law in competition law cases (on the basis of Arts. 101 and 102 TFEU as well as Regulation No. 1/2003). In this context, the ECJ has consistently held that "the principle of *non bis in idem*, which is a fundamental principle of Community law also enshrined in Art. 4(1) of Protocol No. 7 to the ECHR, precludes, in competition matters, an undertaking from being found guilty or proceedings from being brought against it a second time on the grounds of anti-competitive conduct in respect of which it has been penalised or declared not liable by a previous unappealable decision."[24] Still, it must be emphasized that the ECJ referred to the ECHR standard, established in Art. 4(1) of Protocol No. 7, in the context of obligations imposed on the institutions of the EU (the Commission) and not on the Member States. It may also be surprising that the principle has been recognized in the context of proceedings (and penalties), which are considered to be of an administrative and not of a criminal nature.

On the other hand, interpretation of Art. 50 of the Charter cannot ignore the jurisprudence of the ECJ, confirming the obligation of Member States to respect the *ne bis in idem* principle within the framework of judicial cooperation in criminal matters. The interpretation given by the ECJ to the *ne bis in idem* principle enshrined in Art. 54 CISA[25] and on the grounds of the European Arrest Warrant[26] has been construed in an autonomous way, without reference to the ECHR standard. This may be explained, however, by the fact that the criminal nature of the national proceedings in which the principle was invoked was not in question. For this reason, the jurisprudence of the Court concerned mostly the "*idem*" and not "*bis*."

IV. Conclusion

The *Bonda* case confirms the ECJ jurisprudence concerning the legal character of penalties imposed for the breach of EU agricultural law. From this point, the question of the Supreme Court was not as problematic as it appeared, because the ECJ applied its earlier case-law. It was, however, interesting to see how the ECJ adopts the integrative approach, applying the rules concerning the "criminal nature" of penalties formulated by the ECtHR.

The *Bonda* case is also attention-grabbing from the point of view of what the ECJ *did not* state, namely whether the *ne bis in idem* principle applies in this particular case. Taking into account earlier jurisprudence of that same Court concerning the interpretation of Art. 51(1), the answer to this question should be affirmative. In consequence, the Polish Supreme Court should apply – in parallel – Art. 50 of the Charter and Art. 4 of Protocol No. 7 to the ECHR. The *Bonda* case also shows that the ECJ is willing to accept an integrative approach when interpreting EU law with reference to human rights issues, accepting the jurisprudence of the ECtHR concerning the *ne bis in idem* principle.



Dr. Justyna Łacny
Institute of Law Studies, Polish Academy of Sciences,
justyna.lacny@onet.pl

Dr. hab. Monika Szwarc
Institute of Law Studies, Polish Academy of Sciences,
monika.szwarc@post.pl

1 District Office of the Agricultural Restructuring and Modernisation Agency.
2 This provision foresees that: 1. Except in cases of force majeure or exceptional circumstances as defined in Art. 72 of Regulation (EC) No. 796/2004, where, as a result of an administrative or on-the-spot check, it is found that the established difference between the area declared and the area determined, within the meaning of point (22) of Art. 2 of Regulation (EC) No. 796/2004, is more than 3% but no more than 30% of the area determined, the amount to be granted under the single area payment scheme shall be reduced, for the year in question, by twice the difference found. If the difference is more than 30% of the area determined, no aid shall be granted for the year in question. If the difference is more than 50%, the farmer shall be excluded once again from receiving aid up to an amount which corresponds to the difference between the area declared and the area determined. That amount shall be off-set against aid payments to which the farmer is entitled in the context of applications he lodges in the course of the three calendar years following the calendar year of the finding.
3 Commission Regulation (EC) No. 1973/2004 of 29 October 2004 laying down detailed rules for the application of Council Regulation (EC) No. 1782/2003 as regards the support schemes provided for in Titles IV and IVa of that Regulation and the use of land set aside for the production of raw materials, O.J. L 345, 20.11.2004, pp. 1–84. This regulation was compelled by the Commission Regulation (EC) No. 1121/2009 of 29 October 2009 laying down detailed rules for the application of Council Regulation (EC) No. 73/2009 as regards the support schemes for farmers provided for in Titles IV and V thereof (O.J. L 316, 2.12.2009, p. 27). Presently binding regulation does not foreseen exclusions and reductions commented in the *Bonda* case. Nonetheless, ECJ's rationale applied in that case should be taking into consideration when application of the *ne bis in idem* principle is considered.
4 „A person who with the intention of obtaining for himself or another person from a bank or organisational entity carrying on a similar economic activity on the basis of a law, or from a body or institution in receipt of public funds, a credit, pecuniary loan, guarantee, warranty, letter of credit, grant, subsidy, confirmation by a bank of an obligation under a guarantee or warranty or a similar financial provision for a specific economic aim, an electronic payment instrument or public order, submits a document that is forged, altered, attests falsehoods or is dishonest, or a dishonest written statement concerning circumstances of essential importance for obtaining the said financial support, payment instrument or order, shall be liable to a penalty of deprivation of liberty for a period of three months to five years".
5 "Proceedings shall not be initiated, and those initiated shall be discontinued, if: (...) criminal proceedings concerning the same act and the same person have been definitively concluded or those already initiated are continuing (...)".
6 Case C240/90 *Germany v Commission* [1992] ECR I5383, para. 25.
7 Case C210/00 *Käserei Champignon Hofmeister* [2002] ECR I6453, para. 25.
8 *Käserei Champignon Hofmeister*, para. 41; Case 137/85 *Maizena and others* [1987] ECR 4587, para. 13; *Germany v Commission*; para. 26.
9 *Käserei Champignon Hofmeister*, para. 38.
10 *Käserei Champignon Hofmeister*, para. 41
11 Council Regulation (EC, Euratom) No. 2988/95 of 18 December 1995 on the protection of the European Communities' financial interests (O.J. L 312, 23.12.1995, p. 1).
12 "No one shall be liable to be tried or punished again in criminal proceedings for an offence for which he or she has already been finally acquitted or convicted within the Union in accordance with the law."
13 Case C400/10 *McB* [2010] ECR I0000, para. 53; Case C256/11 *Dereci and Others* [2011] ECR I0000, para. 70.
14 *Engel and Others v. the Netherlands*, 8 June 1976, §§ 80 to 82, Series A no. 22.
15 Case C-339/10 *Estov,* 12.11.2010, para. 14; Case C-457/09 *Chartry,* 1.03.2011, para. 25.
16 Case C-256/11 *Dereci,* 15.11.2011, para. 72.
17 A case involving implementation of EU law will not always be a clear-cut case as the opinion of the AG in case C-617/10 *Aklagaren v. Hans Akerberg Fransson* reveals.
18 Opinion of 15.12.2011 in case C-489/10 *Bonda,* para. 19.
19 O.J. C 83, 30.3.2010, p. 313.
20 Opinion of 22.09.2011 in case C-411/10, *N.S. and others,* para. 169.
21 Opinion of 15.12.2011 in case C-489/10 *Bonda,* para. 23.
22 Case C-411/10, *N.S. and others*, 21.12.2011, paras. 119-120.
23 Case C-150/10 *Beneo-Orafti*, 21.07.2011, nyr., para. 68.
24 Case C-238/99 *P LVM and others v. Commission*, 15.10.2002, para. 59; Case C-289/04 P *Showa Denko v. Commission*, 29.06.2006, para. 50; case 308/04 P *SLG Carbon v. Commission,* 29.06.2006, para. 26.
25 Joined cases C-187/01 and C-385/01 *Gözütok and Brügge,* 11.2.2003, ECR 2003, p. I-1345; case C-469/03 *Miraglia,* 10.3.2005, ECR 2005, p. I-2009; case C-436/04 *Van Esbroeck,* 9.3.2006, ECR 2006, p. I-2333; case C-467/04 *Gasparini, 28.*9.2006, ECR 2006, p. I-9199; case C-150/05 *Van Straaten,* 28.9.2006, ECR 2006 p. I-9327; case C-288/05 *Kretzinger,* 18.7.2007, ECR 2007, p. I-6441; case C-367/05 *Kraaijenbrink*, 18.7.2007, ECR 2007, p. I-6619; case C-297/07 *Bourquain*, 11.12.2008, ECR 2008, p. I-9425.
26 Case C-66/08 *Kozlowski*, 17.7.2008, ECR 2008, p I-6041; case C-261/09 *Mantello*, 16.11.2010, nyr.

Previous Issues of eucrim

3/2012 | Liability of Legal Persons
- Guest Editorial by *Prof. Paola Severino*
- Unternehmensstrafbarkeit im europäischen und internationalen Recht – *Dr. Marc Engelhart*
- Cosmetic Use and Lack of Precision in Compliance Programmes: Any Solution? – *Prof. Dr. Adán Nieto Martín*
- Compliance Programmes and "Organisational Faults" in Italian Legislation – *Nicola Selvaggi*
- Liability of Legal Persons and Collective Entities for Environmental Crimes in Italian Law – *Grazia Maria Vagliasindi*
- Investigations on Social Networks – *Klaus Hoffmann*

2/2012 | European Public Prosecutor
- Guest Editorial by Prof. (em.) *Dr. Dr. h.c. mult. Klaus Tiedemann*
- The Initiative for a Directive on the Protection of the EU Financial Interests by Substantive Criminal Law – *Dr. Lothar Kuhl*
- A Decentralised European Public Prosecutor's Office – *Dr. Simone White*
- L'Espace judiciaire pénal européen : une vision se concrétise – *Francesco de Angelis*
- Naming and Shaping: The Changing Structure of Actors Involved in the Protection of EU Finances – *Dr. András Csúri*
- From Europol to Eurojust: towards a European Public Prosecutor *Valentina Covolo*

1/2012 | Corruption and Fraud
- Guest Editorial by *Marin Mrčela*
- Monitoring International Instruments against Corruption – *Lorenzo Salazar*
- The Reform of the EU's Anti-Corruption Mechanism – *Alexandre Met-Domestici, Ph D.*
- Criminal Law in European Countries: Combating Manipulation of Sports Results – Match-fixing – *Carlo Chiaromonte*
- The European Union and the UN Convention against Corruption – *Martin Příborský*
- Unjustified Set-Off as a Criminal Offence in Italian Tax Law – *Enrico Mastrogiacomo*
- Administrative and Criminal Sanctions in Polish Law – *Dr. Agnieszka Serzysko*

4/2011 | Sanctions
- Guest Editorial by *Prof. Dr. Dr. h.c. José Luis de la Cuesta*
- The Civil Asset Forfeiture Approach to Organised Crime – *Dr. Jon Petter Rui*
- The Isolation of Dutch Environmental Criminal Law – *Rob de Rijck*
- Terrorism Lists and Freezing of Assets – Getting Behind Appearances – *Réno Pijnen*, LL.M, M.Phil.

3/2011 | Information and Investigations
- Guest Editorial by *Prof. Udo Helmbrecht*
- Associations for European Criminal Law and the Protection of the EU Financial Interests – Guiding Principles
- Die Verwendung fiktiver Identitäten für strafprozessuale Ermittlungen in sozialen Netzwerken – *Stefan Drackert*
- Procedural Rights of Persons under Investigation by OLAF – *Voislav Stojanovski*

2/2011 | Victims of Crime
- Guest Editorial by *Morten Kjaerum*
- The European Protection Order – *Teresa Jiménez Becerril / Carmen Romero Lopez*
- The Status of the Victim in European Union Criminal Law – *Dr. Massimo Fichera*
- Minors as Victims in the Age of Information and Communication Technologies – *Emmanouil Billis / Panagiotis Gkaniatsos*
- Rights of Victims in Slovenian Criminal Law According to the EU Framework – *Sabina Zgaga*

1/2011 | The Implementation of Legal Instruments
- Guest Editorial by *Giovanni Kessler*
- Different Implementations of Mutual Recognition Framework Decisions – *Dr. Annika Suominen*
- "Yes we can!" – The UK Bribery Act 2010 – *Dr. Simone White*
- Gegenseitige Anerkennung von Geldstrafen und Geldbußen in Deutschland – *Dr. Christian Johnson / Dr. Stefanie Plötzgen-Kamradt*
- Transposing the Framework Decision on Combating Racism and Xenophobia into the Greek Legal Order – *Athanasios Chouliaras*
- Payment of Fiscal and Social Debts with Seized Money in Belgium – *Francis Desterbeck*

4/2010 | Procedural Rights in Criminal Proceedings
- Guest Editorial by Prof. *Dr. Ulrich Sieber*
- The Directive on the Right to Interpretation and Translation in Criminal Proceedings: Genesis and Description – *Steven Cras / Luca de Matteis*
- The Procedural Rights Debate: A Bridge Too Far or Still Not Far Enough? – *Wendy De Bondt / Prof. Dr. Gert Vermeulen*
- Effective Remedies for the Violation of the Right to Trial within a Reasonable Time in Criminal Proceedings – *Dr. Inmaculada Ramos Tapia*

3/2010 | The External Dimension of Criminal Justice
- Guest Editorial by *Aled Williams*
- Der Europäische Auswärtige Dienst und seine Potentiale in Bezug auf die Gemeinsame Innen- und Justizpolitik – *Elmar Brok/ Christiane Ahumada Contreras*
- Transatlantic Counter-Terrorism Cooperation after Lisbon – *Prof. Dr. Valsamis Mitsilegas*
- The Global Challenge of Cloud Computing and EU Law – *Laviero Buono*
- Passenger Name Record Agreements: The Umpteenth Attempt to Anticipate Risk – *Dr. Francesca Galli*

2/2010 | The Lisbon Treaty
- Guest Editorial by by *Viviane Reding / Algirdas Šemeta*
- The Lisbon Treaty – A Critical Analysis of Its Impact on EU Criminal Law – *Dr. Ester Herlin-Karnell*
- Solutions Offered by the Lisbon Treaty – *Margherita Cerizza*
- European Criminal Justice under the Lisbon Treaty – *Dr. Agnieszka Serzysko*
- The Cooperation and Verification Mechanism in Bulgaria – *Gergana Marinova / Iskra Uzunova*

1/2010 | Data Protection
- Guest Editorial by *Peter Hustinx*
- Data Protection in the EU: Challenges Ahead – *Viviane Reding*
- Transatlantic Adequacy and a Certain Degree of Perplexity – *Dr. Els De Busser*

4/2009 | Impacts of the Stockholm Programme
- Guest Editorial by *Beatrice Ask*
- In Memoriam Franz-Hermann Brüner – *Dr. Lothar Kuhl/Harald Spitzer*
- The EU Roadmap for Strengthening Procedural Rights of Suspected or Accused Persons in Criminal Proceedings – *Prof. Dr. Mar Jimeno-Bulnes*
- Asset Recovery: Possibilities and Limitations – *Francis Desterbeck / Delphine Schantz*

3/2009 | Evidence Gathering and Joint Investigation Teams

- Guest Editorial by *Rob Wainwright / José Luís Lopes da Mota*
- The Collection of Evidence by OLAF and Its Transmission to the National Judicial Authorities – *Dr. Joaquín González-Herrero González / Maria Madalina Butincu*
- The Difficulties of Joint Investigation Teams and the Possible Role of OLAF – *Stefan de Moor*
- Gemeinsame Ermittlungsgruppen – Herausforderungen und Lösungen – *Dr. Ralf Riegel*
- Transnational Gathering of Evidence in Criminal Cases in the EU de lege lata and de lege ferenda – *Dr. Arkadiusz Lach*
- The Global Economic Crisis – Protecting Financial Interests in the European Union – *Dr. Wolfgang Hetzer*

1-2/2009 | The Development of European Criminal Procedure Law

- Guest Editorial by *Prof. Lech K. Paprzycki*
- Rules on the Application of ne bis in idem in the EU – *Dr. Katalin Ligeti*
- Mutual Recognition of Judicial Decisions in Criminal Matters with Regard to Probation Measures and Alternative Sanctions – *Hanna Kuczyńska*
- Vers la mort annoncée du juge d'instruction en France – *Elisabeth Schneider*
- The Constitution says yes [but …] to the Lisbon Treaty – *Dr. Marianne Wade*

3-4/2008 | Tenth Anniversary of the European Anti-Fraud Office

- Guest Editorial by *Dr. Ingeborg Gräßle*

The Context of OLAF's Work

- The Approximation of National Substantive Criminal Law on Fraud and the Limits of the Third Pillar – *Dr. Bernd-Roland Killmann*
- La protection des intérêts financiers de l'UE: un grand avenir derrière elle … – *Lorenzo Salazar*
- Die geltenden primär- und sekundärrechtlichen Rahmenbedingungen des EG-Finanzschutzes – *Thomas Wahl*

OLAF's Achievements

- OLAF and the Push and Pull Factors of a European
- Criminal Justice System – *Dr. Marianne Wade*
- The Protection of the euro against Counterfeiting – *Yannis Xenakis / George Kasimis*
- Beiträge des OLAF zur Bekämpfung der Korruption – *Dr. Wolfgang Hetzer*

Optimising OLAF

- The Developments in the Case Law of the Community Courts with Regard to OLAF Investigations – *Lucia Balogová*
- The Judgment of the Court of First Instance in the Case Franchet and Byk v European Commission – *Dr. Simone White*
- Communicating OLAF: A Major Legal Challenge – *Dr. Jörg Wojahn / Dr. Alessandro Butticé*
- Réussites et Défis de l'Office Européen de Lutte Antifraude – *Jean-Pierre Pétillon*

OLAF's Interplay with National Law and Institutions

- The Possible Legal Position of OLAF with Regard to the Polish Criminal Procedure – *Dr. Małgorzata Wąsek-Wiaderek*
- The Principle of Specialisation – The Enforcement of PFI Instruments in Romania – *Corina Badea / Karoly Benke*
- Experiences with the Protection of the Financial Interests in the Czech Republic – *Prof. Dr. Jaroslav Fenyk / Ing. Petr Sedláček*
- OLAFs österreichische Partner – *Mag. Severin Glaser*

OLAF's Future Role and the European Public Prosecutor

- The Reform of OLAF – *Andreea Staicu*
- The Shaping and Reshaping of Eurojust and OLAF – *Prof. Dr. John A.E. Vervaele*
- The Future of the European Union's Financial Interests – *Dr. Lothar Kuhl*

1-2/2008 | The Future European Criminal Law Framework

- Guest Editorial by *José Luís Lopes da Mota*
- Eurojust – The Heart of the Future European Public Prosecutor's Office – *José Luís Lopes da Mota*
- La perspective de réforme des traités européens et la lutte contre la fraude – *Prof. Dr. Lorenzo Picotti*
- Folgen der Bindung des mitgliedstaatlichen Strafgesetzgebers an die europäischen Regelungen und das Verhältnismäßigkeitsprinzip – *Dr. Nuria Pastor Muñoz*
- EU Terrorism Lists in the Eye of the Rule of Law – *Dr. Frank Meyer, LL.M.*

3-4/2007 | National Implementation of International Criminal Law Standards

- Guest Editorial by *Siim Kallas*
- Criminal Law Protection of the EU's Financial Interests in Croatia – *Prof. Dr. Zlata Đurđević*
- The Effective Implementation of International Anti-Corruption Conventions – *Bryane Michael / Habit Hajredin*
- The Implementation of the European Arrest Warrant in the Republic of Slovenia – *Dr. Katja Šugman Stubbs*
- The Nordic Answer to the European Arrest Warrant: The Nordic Arrest Warrant – *Prof. Dr. Asbjørn Strandbakken*

1-2/2007 | National Implementation of "Third Pillar" Legislation

- Guest Editorial by *Franco Frattini*
- Der Kommissionsbericht über die Umsetzung der Instrumente zum Schutz der Finanzinteressen der Europäischen Gemeinschaften – *Dr. Bernd-Roland Killmann*
- The Level of Implementation of the Convention on the Protection of the EC's Financial Interests and of the Follow-up Protocols in the Czech Republic – *Prof. Dr. Jaroslav Fenyk*
- Why Delays the Ratification of the PFI Convention in Hungary? – *Prof. Dr. Ákos Farkas*
- The Implementation of the European Arrest Warrant into National Law – *Isabelle Pérignon*
- Euroscepticism versus Building a Common System for the Surrender of Fugitives – *Eugenio Selvaggi*

3-4/2006 | EC Competences in Criminal Matters

- Guest Editorial by *Franz-Hermann Brüner*
- The European Community and Harmonization of the Criminal Law Enforcement of Community Policy – *Prof. John A.E. Vervaele*
- Case C-176/03 and Options for the Development of a Community Criminal Law – *Dr. Simone White*
- The Community Competence for a Directive on Criminal Law Protection of the Financial Interests – *Dr. Lothar Kuhl / Dr. Bernd-Roland Killmann, M.B.L.-HSG*
- Die Frage der Zulässigkeit der Einführung strafrechtlicher Verordnungen des Rates der EG zum Schutz der Finanzinteressen der Europäischen Gemeinschaft – *Dr. Ingo E. Fromm*

1-2/2006 | The European Arrest Warrant

- Guest Editorial by *Prof. Dr. Ulrich Sieber*
- European Arrest Warrant and the Principle of Mutual Recognition – *Prof. Carlos Gómez-Jara Díez*
- Les juridictions belges et le mandat d'arrêt européen – *Dr. Anne Weyembergh*
- Der Europäische Haftbefehl und seine Umsetzung in das französische Recht – *Peggy Pfützner, LL.M*
- Notes sur la loi italienne portant mise en oeuvre du mandat d'arrêt européen – *Prof. Stefano Manacorda*
- Das Urteil des polnischen Verfassungsgerichtshofs über den Europäischen Haftbefehl – *Dr. Barbara Nita*
- Europäischer Haftbefehl im Interim – *Dr. Heiko Ahlbrecht*

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 h

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.