eucrim
2010 / 3
THE EUROPEAN CRIMINAL LAW ASSOCIATIONS' FORUM

Focus: The External Dimension of Criminal Justice
Dossier particulier: La dimension extérieure de la justice pénale
Schwerpunktthema: Die Außendimension des Bereichs Strafjustiz

2010/3 ISSUE / ÉDITION / AUSGABE

Contents

News*

European Union

Council of Europe

Articles

The External Dimension of Criminal Justice

Imprint

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

Editorial

Dear Readers,

I am delighted to introduce this issue of *eucrim*, which is devoted to the external dimension of EU criminal justice. The importance of the topic is clear. A young woman stands on a street corner in an industrial town somewhere in the EU. She has been trafficked into the Union from a thousand kilometres outside its borders for sexual exploitation. She has a drug habit which feeds on cocaine shipped halfway across the world. Her exploiters channel the profits from her virtual slavery (and that of many others) through financial transactions that span the globe, corrupting and undermining institutions in doing so. Her presence creates danger and insecurity in the EU neighbourhoods where rival groups compete to monopolise "supply" from outside the Union.

The effects of organised crime are felt locally and in individual misery. However, it is a commonplace that, to organised criminal groups, crime is not local but global. For them, borders are only significant if they make the commission of offences or, importantly, their investigation and prosecution more difficult. The decision of the *eucrim* editors to consider the external dimension of EU criminal justice is timely. Awareness of the external dimension to EU criminal justice is not new. For example, since its inception in 2002 as the judicial cooperation unit of the EU, Eurojust has had the power to conclude agreements with third countries and organisations. There have been many concrete results of these agreements, including the presence of prosecutors from Croatia, Norway, and the USA at Eurojust to facilitate the investigation and prosecution of crime affecting the EU from outside its borders.

However, recent developments make the external dimension of EU criminal justice even more significant. The Stockholm Programme, building on the changes to the EU legal landscape introduced by the Lisbon Treaty, has devoted a chapter to the external dimension of freedom, security and justice. The crucial recognition is that "addressing threats, even far away from our continent, is essential to protecting Europe and its citizens." Whether in combating terrorism, trafficking in human beings, or trafficking in drugs, internal security and external security are inseparable.

From this follows the need for a common vision and cooperation between the European institutions involved in the external dimension of the EU. In practical terms, this means that the relevant bodies identified in the Stockholm Programme (Eurojust, Europol, Frontex, CEPOL, the Lisbon Drugs Observatory, and the European Asylum Support Office) must work closely together to ensure coherence and complementarity of effort, for example before and during negotiations of agreements with external partners.

Aled Williams

Against this background, the revised Eurojust Decision published in 2009, provides an illustration of the importance of the external dimension of EU criminal justice. Among other changes, it introduces a new power for the posting of liaison magistrates to third states. Under current arrangements, liaison magistrates act bilaterally: they are posted for the benefit of the Member State which seconds them. Subject to Council approval and appropriate data protection safeguards, in the future the Eurojust liaison magistrate will be able to act for the benefit of all EU Member States and citizens.

Practical work in meeting external threats is, of course, already ongoing. In a recent case, a drug trafficking network operating from Italy but with links to 42 countries worldwide was disrupted with the help of Eurojust and Europol. In September 2010, again in close coordination with Europol, Eurojust supported the national authorities from 11 Member States, together with Norway and Croatia in the dismantling of a significant criminal network exploiting intellectual property rights (with a potential loss of €6 billion within the EU) through global internet access. Close cooperation between national and EU bodies is the precondition for success in meeting external threats.

eucrim has established itself as an important forum where issues central to the future of EU criminal justice can be explored. I am confident that this issue on its external dimension will be a useful contribution to the discussion.

Aled Williams
President of Eurojust

European Union*

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

Foundations

Reform of the European Union

Negotiations on Accession to European Convention on Human Rights Started

7 July 2010 was the official start of the negotiations between the EU and the Council of Europe on acceding to the European Convention on Human Rights (ECHR). Secretary General of the Council of Europe, Thorbjørn Jagland, and Vice-President of the European Commission, Viviane Reding, met in Strasbourg to discuss how to proceed with this historical accession (see also eucrim 2/2010, p. 39 and eucrim 1/2010, p. 2-3).

The accession will be prepared by negotiating an agreement. Negotiators from the Commission and from the Council of Europe's Steering Committee for Human Rights are involved in the process. Ultimately, the agreement will have to be concluded between the 47 contracting parties of the ECHR and the EU, acting by unanimous decision of the Council of the EU and with the consent of the European Parliament. All Member States of the Council of Europe will have to ratify this agreement, even those who are also a Member State to the EU. (EDB)

➤eucrim ID=1003001

New EU Ambassador Presents Credentials to the US Administration

João Vale de Almeida, the first Ambassador of the EU to the US since the Lisbon Treaty entered into force, presented his credentials to President Barack Obama on 10 August 2010. The new Ambassador will be leading the EU's delegation to the US and has the same status as an Ambassador. In this capacity, he will represent not only the European Commission President, José Manuel Barroso, but also the President of the European Council, Herman Van Rompuy. He will work under the authority of the High Representative for Foreign Affairs and Security Policy, and Vice-President of the European Commission, Catherine Ashton. In his previous career, the new Ambassador was the Director General for External Relations and he was the most senior official under the authority of High Representative Ashton in the European Commission. (EDB)

➤eucrim ID=1003002

Enlargement of the European Union

Accession Negotiations Opened with Iceland

On 27 July 2010, during the first intergovernmental conference on the accession of Iceland to the EU, negotiations for the accession process were officially opened. The Belgian presidency prepared the EU Negotiating Framework, which sets out the guidelines for the upcoming discussions and pinpoints the areas where specific efforts are required. For Iceland, these areas (so-called chapters in the negotiation) are fisheries, agriculture and rural development, environment, free movement of capital, and financial services.

After a study of the acquis (the EU legislation that Iceland should comply with), which will run from November 2010 to mid-2011, the negotiation talks will be dealt with by focusing on the individual chapters. (EDB)

➤eucrim ID=1003003

Progress on Croatia's Accession to the EU

Croatia is making significant progress in its accession negotiations with the EU. On 27 July 2010, it was announced that a further two chapters were provisionally closed in the negotiations on Croatia's accession to the EU. Provisional agreement had been reached on financial control and food safety.

Three policy-related chapters that had not been touched upon yet were opened for discussion on 30 June 2010 and in-

* If not stated otherwise, the news reported in the following sections cover the period July–September 2010.

cluded competition, judiciary and fundamental rights, and foreign security and defence policy.

Since the start of the negotiations in 2005, 33 chapters have been opened. Provisional agreement has been reached on 22 chapters so far. (EDB)

➤eucrim ID=1003004

Schengen

Bulgaria and Romania Closer to Acceding to the Schengen Zone

On 1 July 2010, the Council Decision was published in the Official Journal on the application of the provisions of the Schengen acquis relating to the Schengen Information System (SIS) in Bulgaria and Romania. The Decision was adopted on 29 June 2010 after the Council had verified that both States fulfilled the data protection requirements for connecting to the SIS.

The Decision states that, from 15 October 2010, the provisions of the Schengen acquis relating to SIS will apply to the Republic of Bulgaria and Romania reciprocally and in their relations with the other states that have joined SIS. From this date on, both Bulgaria and Romania will be able to enter data into SIS and use data stored in the system. From 29 June 2010, SIS data may already be transferred to the both states. (EDB)

➤eucrim ID=1003005

Institutions

Council

Council Establishes the European External Action Service

At the meeting of the General Affairs Council on 26 July 2010, the Council adopted a decision establishing the organisation and functioning of the European External Action Service (EEAS). The EEAS will serve as the EU's diplomatic corps and will assist High Representative of the Union for Foreign Affairs and Security Policy, Catherine Ashton, in fulfilling her mandate. The EEAS will be a functionally autonomous body of the EU under the authority of the High Representative. While the High Representative will be responsible for shuttle diplomacy and conflict resolution, the administration of the EEAS will be handled by an Executive Secretary-General. The External Action Service will work in close cooperation with the Member States' diplomatic bodies, drawing its staff from the Commission and the Council as well as from the national diplomatic services. The EEAS will also monitor the intelligence gathering services from the Commission and Council (the Council's Joint Situation Centre and the Commission's Crisis Room), the newly formed Situation Centre.

Although the decision establishing the EEAS is a milestone for the EU's foreign policy, there is still a lot to be done on the road to a fully operational EU diplomatic corps. Within the next months, priorities will be given to discussions on budgetary issues as well as on personnel and organisational matters. (ST)

➤eucrim ID=1003006

Commission

DG Justice and Fundamental Rights and DG Home Affairs Launch New Websites

Following the division of the Directorate-General (DG) for Justice, Freedom and Security into the DG Justice and Fundamental Rights and the DG Home Affairs (see also eucrim 2/2010, p. 40), both DGs launched new websites in early August 2010. The websites provide information on the DGs, their policies, funding, and other information on their fields of activity. (ST)

➤eucrim ID=1003007

Court of Justice of the EU (ECJ)

Germany's Constitutional Court Limits Its Own Powers

On 6 July 2010, the Federal Constitutional Court of Germany ruled on a case concerning its powers of revision over judgments delivered by the ECJ. The complainant had lost her case before the German Federal Labour Court, which had formed its decision by taking recourse to a previous ECJ judgement (the *Mangold* case, C-144/04). The complainant claimed before the Federal Constitutional Court that the ECJ had overstepped its competencies in the *Mangold* judgment, and the Federal Labour Court therefore should not have based its decision on the *Mangold* case. The Federal Constitutional Court now ruled that it was of no relevance whether the ECJ had made a wrong decision in the *Mangold* judgment or not. The Federal Constitutional Court finds that its own powers of revision are limited to cases in which actions of EU bodies obviously violate their competencies and the actions in question lead to an undue and excessive shift of power detrimental to the Member States. Since this was not the case in the *Mangold* judgment, the Federal Labour Court had to deliver its judgment in line with the ECJ's ruling. (ST)

➤eucrim ID=1003008

OLAF

Commission Reopens Discussions on OLAF Reform

On 6 July 2010, Algirdas Šemeta, European Commissioner for Taxation and Customs Union, Audit and Anti-Fraud, presented a reflection paper on the reform of OLAF. According to the paper, the need exists for OLAF to be equipped with more appropriate tools to fight fraud, corruption, or other illegal activities detrimental to the financial interests of the EU. The paper puts several actions

up for discussion, such as measures to accelerate the duration of investigations, to increase efficiency, and to improve cooperation between OLAF, the Member States, and other European bodies. Another major part of the paper focuses on independence and control of OLAF, e.g., further clarification of the role of the supervisory committee, strengthening defence rights, and the implementation of a review procedure scrutinizing potential violation of procedural rights. The paper is intended to serve as a basis for discussion with the other EU bodies and eventually lead to a draft text for an OLAF reform proposal. (ST)
➤eucrim ID=1003009

Europol

Joint Report on the State of Internal Security in the EU

For the first time, in July 2010, Europol, Eurojust, and Frontex have published a joint report that gives a current assessment of the principal threats to the EU's internal security. The report, which is primarily based on the agencies' main strategic documents − Europol's Organised Crime Threat Assessment (OCTA) and Terrorism Situation and Trend Report (TE-SAT) as well as Frontex's Annual Risk Analysis (ARA) (see also eucrim 2/2010, p. 43 and 1/2010, p. 6-7) − offers a short analysis of the specific threats posed by organised crime, terrorism, and illegal migration. It finds evidence that these threats are growing in scale, sophistication, and complexity and generating exceptionally high criminal profits, especially with regard to crimes committed via the Internet. The report also finds significant common features among these threats, e.g.:

- Their transnational nature;
- The high mobility of the organised criminal groups;
- The use of well-established routes connecting external feeders with internal criminal hubs;
- The exploitation of poorly integrated communities and key facilitators.

In order to react effectively, it argues for a concerted, holistic EU response. Besides the findings already mentioned, other key findings of the report include the following:

- Its affluent consumer base and open business environment makes the EU particularly vulnerable to organised crime;
- Violent separatist groups and Islamist extremists remain active and pose a clear threat to internal security;
- Most threats to its internal security are generated outside the EU;
- Key hubs in and around the external border of the EU have developed as the principal staging posts for the inward flow of illicit goods and trafficked persons/illegal aliens from other parts of the world;
- Vulnerabilities in the transport sector are exploited to compromise border security;
- Cybercrime has become both a direct threat to security as well as an increasingly important facilitator for most forms of organised crime and terrorism;
- Systematic violence and corruption at the hands of organised crime groups, terrorist groups and street gangs have become an increasing threat to European citizens and businesses. (CR)

➤eucrim ID=1003010

Frontex

First Pilot Frontex Operational Office

On 2 August 2010, Frontex Executive Director, Ilkka Laitinen, and the Greek Minister of Citizen Protection, Michalis Chrisochoidis, signed an agreement for Greece to host the first pilot Frontex Operational Office (FOO) in the Hellenic Coast Guard Headquarters in Piraeus.

The idea to set up specialised branches was supported by a feasibility study that Frontex had commissioned in 2009. It concluded that Frontex could benefit from such an enhanced local presence as this would lead to an improved understanding of local conditions, enhanced effectiveness in the use of risk information, and increased communication between Member States and Frontex (see eucrim 4/2009, p. 127).

The pilot FOO will cover the external border areas of Greece, Cyprus, Italy, and Malta. Its interests will include all operational spheres including sea, land, and air borders. The Piraeus pilot FOO went into operation on the 1st of October 2010, with an evaluation to be conducted after nine months. (CR)
➤eucrim ID=1003011

Development of the Amended Frontex Regulation

On 20 July 2010, the Belgian Presidency suggested a set of amendments and changes to the current proposal for a Regulation amending the Frontex Regulation to the Working Party on Frontiers/Mixed Committee (see eucrim 1/2010, p. 9-10 and 2/2010, p. 51) discussed in its meeting on 22 July 2010. Changes and amendments suggested by the Belgian Presidency mainly concern the provision regulating technical equipment (Art. 7) as follows:

- To provide funds for the acquisition of equipment in the Agency's budget;
- To foresee the drawing up of a model agreement regulating the terms of use of the equipment;
- To plan the contributions of Member States to the pool and the deployment of the technical equipment for specific operations on the basis of annual bilateral negotiations and agreements between the Agency and Member States;
- To foresee the possibility to revise the minimum amount of equipment in case it proves insufficient.

Other changes concern the provision of information exchange systems (Art. 11), security rules on the protection of classified information and non-classified sensitive information (Art. 11b), facilitation of operational cooperation with third countries, and coopera-

tion with competent authorities of third countries (Art. 14). (CR)
➤eucrim ID=1003012

Enhanced Processing of Personal Data

The question of additional possibilities for Frontex to process personal data was the central issue of two reports on the Agency in the past months.

On the one hand, in his opinion of 26 April 2010 concerning the collection of names and certain other relevant data of returnees for Joint Return Operations (JRO), the European Data Protection Supervisor agreed that some processing of personal data is necessary for a proper execution of the Agency's task in the context of the JRO. However, given the sensitivity of the data and activities concerned, he suggests considering a more specific legal basis than Art. 9 of Regulation (EC) No 2007/2004 and considering the inclusion of such a legal basis in the context of the ongoing revision of the Frontex Regulation. On the other hand, in its analysis and assessment of the Frontex Annual Activity Report 2009 of 28 June 2010, the Frontex Management Board concluded that the processing of personal data is crucial for Frontex from a strategic perspective. In addition, the Agency's effectiveness could already be increased under its current mandate by enriching intelligence and intelligence products with personal data.

Other findings of the Frontex Management Board's analysis and assessment of the Annual Activity Report 2009:

- Frontex carried out its activities more efficiently in 2009 as its number of operational days increased by 73% (from 2937 days in 2008 to 2088 days in 2009);
- Frontex' financial input only increased by 25% (from €70 million in 2008 to €88 million in 2009).

While the overall assessment of the Agency finds it to be working effectively and fulfilling its task of enabling Member States' border control and border management authorities to work more effectively, some drawbacks remain, especially with regard to the efficiency of internal control standards and the difficulty of attracting skilled personnel to its location in a prompt and timely manner. (CR)
➤eucrim ID=1003013

Action for Annulment: Council Decision 2010/252/EU

On 14 July 2010, the European Parliament brought an action for annulment under Art. 263 TFEU against the Council of the EU before the Court of Justice.

In its action, the European Parliament asks the Court of Justice to annul Council Decision 2010/252/EU of 26 April 2010 supplementing the Schengen Borders Code as regards the surveillance of the sea external borders in the context of operational cooperation coordinated by Frontex, on the grounds that it exceeds the scope of Art. 12(5) of the Schengen Borders Code by adopting additional measures for border surveillance.

Based on Chapter III of the Schengen Border Code, which regulates the control of external borders and refusal of entry, Art. 12 states that the main purpose of border surveillance is to prevent un-authorised border crossings, to counter cross-border criminality, and to take measures against persons who have crossed the border illegally.

The contested decision lays down rules for sea border operations coordinated by Frontex, including measures for interception of ship or other seacraft as well as guidelines for search and rescue situations and for disembarkation in the context of sea border operations coordinated by the Agency.

In its action, the European Parliament claims that these rules on interception, search and rescue, and disembarkation exceed the scope of the notion "surveillance" defined by Art. 12. Furthermore, the EP would even modify essential provisions of the Schengen Borders Code, while modification of essential provisions is reserved for the legislator (Arts. 12(5), 33(2)).

In case the Court of Justice annuls the contested decision, the European Parliament suggests that the Court exercise its discretion to maintain the effects of the decision until such time as it is replaced (Art. 264(2) TFEU). (CR)
➤eucrim ID=1003014

Specific Areas of Crime / Substantive Criminal Law

Corruption

Fighting Corruption and Fraud in Bulgaria and Romania

On 20 July 2010, the Commission published its annual reports under the co-operation and verification mechanism in Bulgaria and Romania. The Commission's analysis of both countries is based on an assessment of progress by the Bulgarian and Romanian authorities and on information by Member States, international organisations, independent experts, and other sources as well as on responses given by both countries to a detailed questionnaire prepared by the Commission. Besides the analysis of the state-of-play, the reports include specific recommendations for each country. However, the reports show major differences between the countries as regards reform efforts and achievements.

The report on Bulgaria highlights the country's serious steps towards a reform of the judiciary. Bulgaria has improved its penal procedures and presented a higher number of indictments for cases involving high-level corruption and organised crime compared to the previous Commission analysis.

Recently, in June 2010, it introduced a new strategy for judicial reform, showing political will to efficiently tackle corruption and organised crime. Nevertheless, the report indentifies the need for Bulgaria to work on addressing conflict-of-interest cases related to the business interests of local politicians and their families. The report also claims that, even cases of convictions for serious

crimes, the perpetrators are often still at large as they appeal their sentence and the judges generously decide that this freedom would not interfere with the appeal process. The Commission recommends using existing legislation more efficiently and considering the retention of people convicted of serious crimes in detention, as is practised in other Member States.

The report on Romania shows that Romania has made little progress in reforming the judiciary. The report stresses that Romania has shown insufficient political commitment in support of the reform process, and its judiciary and disciplinary procedures urgently require improvement. Romania has introduced new legislation, which, according to the report, restricts the transparency of dealings by public officials and hinders measures to fight corruption.

Therefore, the Commission even sees Romania at risk of breaching its accession commitments. It recommends that Romania rethink its political path and strengthen the commitment of the judiciary to reform. The Commission will provide its next assessment of progress in mid-2011. (ST)

➤eucrim ID=1003015

Corruption One of the Main Reasons for Economic Crisis in Greece?

Several news journals reported on a hearing before the European Parliament on 1 July 2010. During the hearing, Aris Syngros, head of Transparency International's office in Greece, presented the results of a survey (based on telephone interviews with over 6000 individuals), which estimates the costs of corruption. Transparency international, a global civil society organisation leading the fight against corruption, carried out the survey in 2009 and now presented its alarming results. 9.3% of households reported that they were asked to pay a bribe in order to speed up administrative processes, get fair treatment in hospitals, or avoid a penalty for traffic offences. The average bribe paid in 2009 for public services was €1,355. Transparency International estimates the total costs of bribes paid by Greek citizens for public and private services at nearly €800 million a year, not including high-level corruption cases or big tax evasion schemes. Aris Syngros notes that "corruption is one of the main reasons why we have this economic crisis in Greece. It's not the only one, but it's a very important one." (ST)

➤eucrim ID=1003016

Counterfeiting & Piracy

Article 29 Working Party on ACTA

On 15 July 2010, the Art. 29 Working Party on Data Protection (WP29) published a letter to EU Trade Commissioner, Karel De Gucht, pointing out several concerns on the new Anti-Counterfeiting Trade Agreement (ACTA, see also eucrim 1/2010, p. 10). Though not explicitly included in the ACTA draft, WP29 fears that the agreement could encourage the parties to voluntarily include blocking of internet access and monitoring of the online activities in order to enable identification of alleged infringers on national legislation.

Also, WP29 is concerned about the planned notice-and-take-down procedure, which would oblige providers of online services to block access to content uploaded by users, in case a third party claims that his/her rights have been violated by making the content available. WP29 is concerned that this might lead to excessive disclosure of individuals' data to third parties.

Finally, WP29 criticizes that the provisions on border searches by customs are not specific enough, which might entail serious breaches of an individual's fundamental rights. WP29 is asking the parties to bear these concerns in mind when continuing to work on the draft text of the Anti-Counterfeiting Trade Agreement. (ST)

➤eucrim ID=1003017

New Agreement on Illegal Trade of Tobacco Products

On 15 July 2010, the Commission and the British American Tobacco (BAT) signed a cooperation agreement on jointly fighting the illicit trade in tobacco products. BAT will work with the Commission, OLAF, and the Member States' law enforcement authorities to help in the fight against contraband and counterfeit cigarettes. The agreement was initiated by BAT and foresees several ways for BAT to participate in the fight against cigarette smuggling and counterfeiting, e.g.:

- By contributing a total of USD 200 million (€134 million) to the EU and the Member States over the next 20 years;
- By strengthening its own review process for selecting and monitoring customers;
- By improving BAT's product tracking procedures;
- By extensively sharing its information on any illegal activities with the respective EU bodies.

BAT also guarantees making available additional funds in the event of future seizures of its genuine products in the EU. (ST)

➤eucrim ID=1003018

Annual Report on EU Customs Actions to Enforce Intellectual Property Rights

On 22 July 2010, the Commission published its annual report on EU Customs actions to enforce intellectual property rights (IPR). Overall, customs registered 43,572 cases of detentions of goods suspected of IPR infringements at the EU's external borders, compared to 49,381 cases recorded in 2008. 118 million goods suspected of infringing IPRs were detained in 2009, which is a decrease in the number of articles by 18% compared to 2008 (178 million articles). Overall, 64% of goods suspected of infringing IPRs were sent to the EU from China. The main categories of goods detained are:

- Cigarettes (19% of all detentions);
- Other tobacco products (16%);
- Labels and tags (13%);
- Medicines (1%).

Project Report

SUPPORT TO THE ECONOMIC AND FINANCIAL CRIMES COMMISSION (EFCC) AND THE NIGERIAN JUDICIARY

Report from the Project "Support to the EFCC and the Nigerian Judiciary", UNODC, 2006–2010

The project "Support to the EFCC and the Nigerian Judiciary" is a 24,7 Million Euro project, primarily funded by the European Union under the 9th European Development Fund. The project, which was launched in 2006 and will be completed in 2010, is implemented by the United Nations Office on Drugs and Crime (UNODC).

The project supported the Economic and Financial Crimes Commission, which was set up in 2003 by the Nigerian Government with the mandate to prevent and combat economic and financial crimes in the crucial phase of the EFCC's initial process of institution building. Specific project interventions included the strengthening of the operational capacities of the agency, the provision of specialised training for staff and management, the delivery of basic operational equipment, the strengthening of the EFCC's Training and Research Institute, as well as the creation of a forensic laboratory and the mentoring of its staff. The project further provided the EFCC with a state-of-the-art IT-system and helped developing and implementing custom-made specialised database applications – goAML and goCASE – used in case management and financial intelligence analysis. Moreover, the project assisted the agency in policy, advocacy, and outreach through the conduct of several assessments of the nature, scope, and frequency of corruption and the provision of support in the development of a national anti-corruption strategy. The project has also helped with promoting the establishment of a national network of civil society organisations advocating for the fight against corruption and governance reforms as well as with the development of specialised non-conviction based asset forfeiture draft legislation aimed at further enhancing the effectiveness of law enforcement action against corruption.

The project also assisted the Nigerian Judiciary and other justice sector stakeholders in the strengthening of integrity and capacity of the justice system at the federal level and within 10 Nigerian states. In this regard, the project helped to prepare the ground for several reform policies primarily focusing on improving governance, accountability and transparency of justice sector institutions. A large-scale assessment of justice sector integrity and capacity was carried out providing basic data allowing for the measuring of progress in the various areas of reform. The data was also used in the development of action plans at state level aimed to enhance public access to justice, in particular by prisoners awaiting trial, to improve speed and quality of justice delivery, and to increase accountability, integrity, impartiality and independence of the courts. Subsequently, the implementation of these action plans was supported through policy and technical advisory services, training of the respective authorities, and the provision of equipment. The implementation of these plans is still being monitored.

Five years into implementation, the project has been able to aid counterpart institutions in making significant achievements. Until today, the EFCC has received more than 5000 petitions and its investigations have led to more than 400 convictions. Another impressive achievement is the recovery of 6,5 billion USD of criminal proceeds. At the political level, the Financial Action Task Force (FATF) has removed Nigeria from the list of non-cooperating countries and territories. Subsequently, formal monitoring of Nigeria's compliance with the 40+9 FATF recommendations was ended and the Nigerian Financial Intelligence Unit (NFIU) was admitted to join the Egmont Group. As a whole, Nigeria was able to consistently improve its standing in several global governance indicators, such as the Global Corruption Barometer, the Corruption Perception Index of Transparency International, and the World Bank Governance Indicators (e.g., according to the Global Corruption Barometer, 29% of respondents claimed that they had paid a bribe in 2005, as opposed to 17% in 2009). Moreover, EFCC enjoys a high level of acceptance among Nigerian citizens, as shown by the results of a public perception survey conducted by the project in 2009, in which 72% of respondents confirmed that the "EFCC meets my expectations fully or partially".

With regard to the justice sector, a study conducted in 2007/08 which has been assisted by the project confirmed extraordinary improvements made in the period from 2002 to 2007. More specifically, access to justice by citizens had increased significantly with the average time that prisoners had to spend in remand reducing from 30 months in 2002 to less than 12 months in 2007. Another change can be seen in a raise of the general awareness of prisoners with regard to bail with 68% of the respondents being aware of their right to apply for bail in 2007, as opposed to only 43% in 2002. Prisoners also had better access to legal assistance, with 56% being represented by a lawyer compared to only 38% in 2002. Concerning timeliness and quality of justice delivery, similar progress could be observed. The average number of months that it had taken participants in legal proceedings to resolve their legal matters had reduced from 27 months in 2002 to a little over 12 months in 2007. The courts' administrative departments have also improved, with 87% of judicial officers finding the record-keeping efficient or very efficient, as opposed to only 44% sharing this opinion in 2002. As regards the prevalence of corrupt practices, in 2002, 77% of lawyers and 43% of parties involved in court proceedings claimed that within the last 12 months prior to the interview they had been approached for the payment of a bribe in the context of a court case. Being asked the same question in 2007, only 16% of the lawyers and only 2% of the other participants admitted that they had been approached for the payment of a bribe. With respect to the independence, impartiality and fairness of the courts, in 2002 19% of the judges felt that judicial appointments were politically influenced and not based on merit, while 50% of the lawyers claimed to know of judicial decisions that had been influenced by politics. However, in 2007, findings seemed to suggest that judicial independence had been strengthened – with 24% of lawyers stating that they were aware of a judicial decision during the last 12 months which in their opinion had been influenced by politics, and 8% of judicial officers claiming to be aware of a judicial appointment having been influenced by political considerations rather than merit.

All of these improvements have helped to enhance public confidence in the justice system. By 2007, the percentage of people who stated that they had not used the courts during the last two years despite a need to do so had decreased from 42% in 2002 to 36% in 2007. At the same time, the number of respondents indicating that they would use the courts again based on their (positive) experience increased from 58% in 2002 to 69% in 2007.

The project is on target for achieving its various objectives. The project's activities will be closed in November 2010. Its tasks are currently handed over to the beneficiary in order to enhance the local ownership and ensure sustainability.

For more information on the above project please see http://www.nji.gov.ng or contact:

Mr. Claudi Ferrer
Project Officer
Delegation of the European Union to Nigeria
claudi.ferrer-savall@ec.europa.eu

Dr. Oliver Stolpe
Senior Project Coordinator
"Support to the EFCC and the Nigerian Judiciary"
United Nations Office on Drugs and Crime
Oliver.stolpe@unodc.org

Counterfeit products for daily use, which may pose a danger to citizens' health, account for 17 million items (18%) (e.g., food and beverages, health and beauty care items, electrical household goods and toys). The main difference compared to 2008 is a significantly lower amount of interceptions involving DVDs/CDs (5% of total in 2009 compared to 44% in 2008). (ST)
➤eucrim ID=1003019

Organised Crime

EU Internal Security Strategy Operational by 2014

On 15 July 2010, the Interior Ministers of the EU decided to put in place an operational European security strategy by 2014. The Internal Security Strategy set up under the Spanish Presidency shall now be brought to the next level, with the Belgian Presidency being tasked to begin developing an operational plan. To this end, the Belgian Presidency is planning to develop and test a "policy cycle" consisting of four major phases:

- Analysis of the situation;
- Identification of the priorities;
- Drafting, implementing, and monitoring action plans;
- Evaluation phase.

In the process, both Europol and COSI (the Council's Standing Committee on Internal Security, see also eucrim 4/2009, p. 123) shall play a key role.

In a first step, the Belgian Presidency has identified illegal arms trafficking as a criminal cross-border phenomenon for which COSI shall draw up an operational action plan by December 2010, focusing on the possibilities for harmonisation of legislation relating to the sale and classification of arms. A second phenomenon identified by the Presidency is itinerant gangs for which the Presidency would like to draw up a common definition and harmonise an action plan. (CR)
➤eucrim ID=1003020

Towards an EU Internal Security Strategy

On 20 July 2010, the Commission published a communication outlining achievements, upcoming challenges, and initiatives in EU counter-terrorism policy. The communication lists the existing measures to prevent, protect, pursue, and respond to terrorist threats. It also identifies future challenges in areas, such as radicalisation, crisis management, and response. Some of the necessary future measures enumerated in the communication are:

- Proposals for improving EU-wide control of access to dangerous substances and for enhancing public transport security;
- Rapid crisis coordination and cooperation;
- A review of the EU strategy to counter radicalisation and recruitment.

The communication is intended to serve as a basis for the EU Internal Security Strategy which, although initially tabled for autumn 2010, is now planned to be put in place by 2014. (ST)
➤eucrim ID=1003021

Environmental Crime

New Regulation on Illegal Timber Imports on the Way

On 7 July 2010, in line with the EU-Republic of Congo Agreement on fighting illegal timber exports signed in May 2010 (eucrim 2/2010, p. 47), the EP adopted a legislative resolution on a new regulation laying down the obligations of operators who place timber and timber products on the market. The new regulation will ban the sale of illegally harvested timber and introduce new traceability measures and sanctions. As regards penalties, the regulation foresees fines proportionate to the environmental damage, the value of the timber or timber products concerned, and the tax losses and economic detriment resulting from the infringement. In case of repeated serious infringements, the fines

shall be gradually increased, e.g., seizure of the timber and timber products concerned and/or immediate suspension of the authorisation to trade.

Since the text is the outcome of a political agreement with the Council, it is expected to be formally adopted soon. (ST)
➤eucrim ID=1003022

Wastewater Treatment – Fines for Belgium, Warning for Luxembourg

On 24 June 2010, the Commission announced that it would take actions against Belgium and Luxembourg for not complying with the 1991 Urban Wastewater Treatment Directive, which had to be implemented by 30 June 1993.

The Commission is referring Belgium to the ECJ because some 40 areas still remain listed as not complying with EU legislation. Since the ECJ has already ruled on the cases related to these Belgian areas, the Commission is now asking the Court to impose a lump-sum fine of more than €15 million and a daily penalty payment of nearly €62,000.

Luxembourg has just received a final warning over the same issue, for also not complying with EU legislation despite a prior ECJ ruling. If Luxembourg continues to fail to comply with the previous ECJ judgment, it faces being referred to the ECJ as well. (ST)
➤eucrim ID=1003023

Illegal Migration

Vice-President Reding Assesses the Situation of Roma in France

On 25 August 2010, Vice-President of the Commission and Commissioner for Justice, Fundamental Rights and Citizenship, Viviane Reding, published a statement on the situation of the Roma people in Europe. In the statement, the Vice-President focuses on the situation of the Roma people in France and the country's recent campaign to deport Romanian and Bulgarian Roma following raids of illegal camps in France. Reding has announced an analysis of the situation in France, especially with respect to the compatibility of the latest measures with EU law. She calls on all Member States to participate in a dialogue on how to best integrate the Roma in the Member States' societies and advises all parties to take the Roma's situation seriously and to end "discriminatory and partly inflammatory" rhetoric.

On 29 September 2010, Reding presented her assessment of the situation of the Roma in France, which led to the Commission's decision to send a formal notice to France asking for full transposition of the Free Movement Directive (2004/38/EC) into national law. The letter of formal notice will be sent in the context of the October 2010 package of infringement procedures unless France presents draft transposition measures and a detailed transposition by 15 October 2010. (ST)
➤eucrim ID=1003024

Cases of Illegal Border-Crossing Drop by Half

Data from Eurodac (the EU's fingerprint database for asylum and migration purposes) released on 3 August 2010, show that the number of migrants illegally entering the EU dropped 50% in 2009, mainly resulting from Italy's and Spain's new cooperation agreements with third countries.

Italy and Spain are shipping back thousands of people attempting to illegally enter the EU to third countries before they even land. Especially the Italy-Libya pact to send migrants picked up at sea to detention centres in Libya has led to a significant decrease in the number of cases of illegal migration in Italy, with a total of 7,300 cases in 2009 compared to 32,052 the year before. Spain has also reported a large drop in arrivals, from 7,068 in 2008 to 1,994 in 2009. For 2010, the numbers are expected to decrease even further. Human rights organisations criticize the Italy-Libya pact as a convenient way for Italy to evade the obligations that ensue from actual landings of illegal migrants on its territory. (ST)
➤eucrim ID=1003025

Procedural Criminal Law

Procedural Safeguards

Proposal for an EU Letter of Rights

On 20 July 2010, the Commission adopted a proposal on a Directive on the right to information in criminal proceedings. Following the proposed Directive on the right to translation and interpretation, this is a second step in ensuring fair trial rights as laid down in the Roadmap on Procedural Rights that was included in the Stockholm Programme (see also eucrim 4/2009, p. 134 and p. 157-161 and eucrim 3/2009, p. 72).

The proposed Directive on the right to information in criminal proceedings lays down rules concerning the rights of suspected and accused persons to be informed about their rights and the charges in criminal proceedings against them. This will include a so-called Letter of Rights, a brief outline of a person's rights when he is arrested, that is similar to the American "Miranda Rights." It will include mention of the persons' rights

- To a lawyer;
- To be informed of the charge(s);
- Where appropriate, to have access to the case file;
- To interpretation and translation for those who do not understand the language of the proceedings;
- To be brought promptly before a court following arrest.

These rights are already included in the EU Charter of Fundamental Rights and the European Convention on Human Rights and represent the minimum standard that should apply in all Member States. Member States are free to draw up their own Letters of Rights (possibly including more than the above-

mentioned minimum standard) as long as accurate information about these core fair trial rights is included. National law enforcement authorities should have the letter at their disposal in all commonly spoken languages in their respective localities. The Commission's proposal provides a model in 22 languages to limit translation costs.

A separate version of the Letter of Rights should be made by the Member States for persons subject to European Arrest Warrant proceedings. For both the regular Letter of Rights and for the Letter of Rights to be used in cases of a European Arrest Warrant, templates have been annexed to the proposed Directive for use by Member States. (EDB)
➤eucrim ID=1003026

Data Protection and Information Exchange

Temporary EU Official Supervising Transatlantic Data Transfers

On 1 August 2010, the Agreement on the transfer of bank data in the fight against terrorism between the EU and the US entered into force (see also eucrim 2/2010, p. 48-50.; eucrim 1/2010, p. 13 and eucrim 4/2009, p. 135-136). One of the safeguards that the European Parliament required the agreement to provide was the appointment of an "independent EU person" to supervise any searches made by US authorities.

Due to the lengthy procedure (estimated at 2-3 months) for the hiring process, European Commissioner for Home Affairs, Cecilia Malmström, announced at a press briefing on 27 August 2010 that an interim official has been appointed to start monitoring the Terrorist Finance Tracking Program (TFTP) searches. The official, whose name will not be made public, has the authority to block specific or all searches that are not performed in accordance with the agreement.

The Commissioner stated that the appointment of a permanent official is in preparation and will be carried out shortly. (EDB)
➤eucrim ID=1003027

Article 29 Working Party Speaks Out Against Data Retention Directive

During their meeting from 12-14 July 2010, the EU Member State data protection authorities (united in the Art. 29 Working Party) adopted a report on Directive 2006/24/EC, also known as the Data Retention Directive. The report was based on a joint inquiry conducted by the Art. 29 Working Party that focused on the implementation of the Directive. The inquiry included questions on security measures and prevention of abuse, compliance with storage limit obligations, and the types of retained information.

The results showed considerable discrepancies in the retention periods utilized by the Member States' telecom and Internet service providers, varying from 6 months to 10 years. Additionally, more data are being retained than is allowed in accordance with the Directive, e.g., data relating to the content of communication.

The report concludes by making recommendations to the Commission to improve the Directive. These recommendations include increased harmonisation, reduced maximum retention period, no additional retention obligations for service providers, more secure data transmission, and standardised handover procedures.

With this report, the Art. 29 Working Party calls upon the Commission to take the findings of the report into account when making the decision on whether or not to amend or repeal the Data Retention Directive. (EDB)
➤eucrim ID=1003028

Commission Wants Stronger Data Protection Authorities

Commissioner for Justice, Fundamental Rights and Citizenship, Viviane Reding, met with the Art. 29 Working Party on 14 July 2010. Presenting the Commission's opinions on reworking the legal framework on data protection, both parties discussed giving national data protection authorities more powers, including sanction and enforcement powers. Additionally, the strengthening of data subjects' rights and the development of one all-embracing legal framework for data protection were among the topics discussed.
➤eucrim ID=1003029

On 24 June 2010, the Commission took action on its opinion with regard to strengthening the national data protection authorities and announced that it requested that the UK take measures to strengthen the powers of its data protection authority. The Commission had previously requested that the UK bring its data protection legislation and its application by the national courts in line with the provisions of Directive 95/46/EC.

What still needs to be improved is the power of the Information Commissioner's Office. This office is, to date, unable to assess the adequacy of the level of data protection of third states and to perform random checks (and possibly enforce penalties) on processors of personal data. With regard to the UK courts, they should not have the power to refuse the right to have personal data rectified or erased and to restrict the right to compensation for moral damage in cases of misuse of personal data.

The UK must inform the Commission within two months of the measures taken to ensure full compliance with Directive 95/46/EC. (EDB)
➤eucrim ID=1003030

Inventory of EU Instruments on Information Management

The Commission presented a communication to the European Parliament and to the Council on information management in the area of freedom, security and justice. On 20 July 2010, an inventory was published listing all EU instruments covering information gathering, storage and exchange for the purposes of law enforcement, and migration manage-

ment. The instruments in the overview include those that are in force and those that are in implementation or under consideration as well as initiatives that were recently taken under the Stockholm Programme.

Since the abolishment of internal borders with the creation of the Schengen zone, a number of legal instruments has been developed. With this overview, the Commission aims to contribute to an informed policy dialogue with all stakeholders and to improve coherency in the approach to the exchange of personal data in criminal matters. Moreover, the communication provides for reflection on the possibility of a European Information Exchange Model based on an evaluation of the existing measures of information exchange. Thus, the analysis of these measures is followed by the principles of policy development based on which new initiatives should be developed and current instruments should be evaluated.

The annexes to the communication provide examples of information exchange based on the instruments that are in force and a table of all instruments, illustrating their background, purpose, structure, data protection provisions, etc. (EDB)

➤eucrim ID=1003031

Commission Releases Data Protection Studies

The Commission published the final report of a study on the new challenges to data protection. A range of topical working papers and country reports are attached to this final report. The final report was finalised in January 2010 and released in July 2010.

The final report is entitled "Comparative study on different approaches to new privacy challenges in particular in the light of technological developments" and covered the Czech Republic, Denmark, France, Germany, Greece, and the UK; outside Europe, it included the US, Australia, Hong Kong, India, and Japan. The study encompasses a comparative analysis of the possibilities that different regulatory and non-regulatory systems (EU and third states) offer in response to challenges posed by technological developments. It also contains an analysis of Directive 95/46/EC with regard to its adequacy to protect personal data in this new environment. The study concludes by formulating recommendations for amending the legal framework on data protection, including the Directive.

The reports form a basis for two actions included in the Action Plan implementing the Stockholm Programme (see also eucrim 1/2010, p. 2) that should be dealt with by the Commission in 2010. The Lisbon Treaty also called for a redevelopment of the structure of the EU legal framework for data protection. (EDB)

➤eucrim ID=1003032

Proposal for a Large-Scale IT Agency – Opinion of Committee on Budgets

In her report for the Committee on Budgets of 15 July 2010 on the amended proposal for a regulation establishing an agency for the operational management of large-scale IT systems in the area of freedom, security and justice, rapporteur Jutta Haug raised several questions. First, with regard to the agency's budget, she expressed her surprise that the overall amount deemed necessary for the Visa Information System (VIS), SIS, and Eurodac and the creation of the IT agency perfectly matches the amounts initially foreseen in the financial planning and bears no savings or extra costs. Secondly, concerning the recruitment of staff for the agency, the rapporteur criticises that no transfer of posts from the Commission to the agency is foreseen and that the outsourcing of tasks to the agency seems to be used to free some posts that will be assigned to other priorities.

Finally, the impact assessment provided by the Commission is perceived as incomplete, out-dated, and partly inadequate as it did not sufficiently explain why such an agency was needed to accomplish a technical task that, until now, has fallen under the Commission's remit, the assessment does not clearly present the overall budgetary impact of the creation of such an agency, etc. In order to avoid such a situation in the future, the rapporteur suggests that the European Parliament consider the possibility that the Commission send its impact assessment and/or cost-benefit analysis concerning the creation of a new agency to the Court of Auditors, so that the Court may give an opinion as to their consistency.

Following up on its critics, the opinion includes a list of amendments to be incorporated in the report of the responsible Committee on Civil Liberties, Justice and Home Affairs. (CR)

➤eucrim ID=1003033

Victim Protection

Commission Plans Package of Victims' Rights and Launches Public Consultation

On 15 July 2010, the Commission launched a public consultation to obtain feedback from citizens, organisations, associations, bodies, institutions, and experts on victims' issues and victims' rights.

The Commission plans to develop a comprehensive package of rules and practical measures aiming to support victims throughout criminal proceedings. In order to draft a proposal in the first half of 2011, the public consultation was open until 30 September 2010. It focuses on five areas of victims' needs: recognition, protection, support, access to justice, and compensation. With regard to the area of protection, the progress made under the Spanish presidency on the proposed Directive for a European Protection Order (see also eucrim 4/2009, p. 138) will be taken into consideration when developing the package of victims' rights. (EDB)

➤eucrim ID=1003034

Freezing of Assets

EU Terrorist Lists Prior to June 2007 Declared Invalid

On 29 June 2010, the Court of Justice ruled on a preliminary question brought before it by the Oberlandesgericht Düsseldorf, Germany. The question concerned the lists of persons and entities linked with terrorist groups that the EU had adopted based on a number of UN Resolutions (see also eucrim 4/2009, p. 138-139 and 1-2/2008, p. 33). In several judgments, the General Court (previously known as the Court of First Instance) had annulled the inclusion of certain persons and entities because of failure to comply with basic procedural safeguards. Therefore, the Oberlandesgericht Düsseldorf asked the Court of Justice whether the inclusion of the organisation Devrimci Halk Kurtulus Partisi-Cephesi (DHKP-C) in this list was also illegal.

Two of DHKP-C's members who collected donations were prosecuted for membership in a terrorist group. The organisation has remained on the list since 2002. Until June 2007, decisions to add persons and entities to the list were adopted without advising them of the specific reasons for their inclusion. This was considered illegal by the General Court, leading to the Council amending its procedure regarding entries on the list. The adoption of an updated list on 29 June 2007 marked the date prior to which persons and entities on the list could not verify whether their inclusion was well founded or not. Thus, the Oberlandesgericht asked the Court of Justice whether the inclusion of the DHKP-C must, with regard to the period prior to 29 June 2007, also be held illegal, despite the fact that the DHKP-C has not sought annulment of that inclusion.

The Court of Justice ruled that is at the discretion of the national court (in this case the Oberlandesgericht Düsseldorf) to decline to apply the Council Decisions and the attached terrorism lists that were adopted before June 2007. This means that the inclusion of DHKP-C on this list cannot form any part of the basis for criminal proceedings against the two defendants in respect of the period prior to 29 June 2007. (EDB)

➤eucrim ID=1003035

Commission Reports on Poor Implementation of Framework Decision on Confiscation

On 23 August 2010, the European Commission presented a report on the implementation of Framework Decision 2006/783/JHA90 on the application of the principle of mutual recognition to confiscation orders.

Illegal goods are easily moved across borders and in this way, the offenders escape criminal prosecution in another Member State. This means that large amounts of money do not flow back to the Member State they originated from. Under the above-mentioned Framework Decision, a confiscation order issued by the authorities of one Member State can be sent to the authorities of another. The receiving authority can directly carry out the confiscation, according to its own national rules, without any further formalities. However, by February 2010 (closing date for research to be submitted for the report), fourteen Member States had not yet implemented the aforementioned Framework Decision.

In accordance with the existing rules, Member States may refuse to carry out confiscation orders in limited circumstances, e.g. violation of double jeopardy or excessive delays between the facts and final conviction. This report shows that 24 Member States have added further reasons for refusing to carry out other states' confiscation orders.

In accordance with the existing rules, Member States may refuse to carry out confiscation orders in limited circumstances, e.g. violation of double jeopardy or excessive delays between the facts and final conviction. This report shows that 24 Member States have added further reasons for refusing to carry out other states' confiscation orders.

Lack of trust in each other's criminal justice systems still seems to be the underlying cause. The development of legal instruments to protect the rights of accused and suspected persons in criminal proceedings, such as the Directive on the right to translation and interpretation in criminal proceedings (see also eucrim 1/2010, p. 14-15) and the letter of rights (see p. 93 in this issue of eucrim), is aimed at solving this issue. (EDB)

➤eucrim ID=1003036

Cooperation

Police Cooperation

Operation "Hermes"

Under the Belgian Presidency, the Belgian Integrated Police are planning to organise a joint operation in a large number of Member States as the second phase of a larger operation called "Hermes." The operation follows two objectives: The first aim is to establish a more detailed and complete image of the routes of illegal immigration and the smuggling of human beings within the Schengen area, in collaboration with non-Schengen Member States. The second goal is to actively promote and valorise the European police networks Tispol (European Traffic Police Network), Aquapol (European partnership of water police forces and inland navigation inspectorates), and Railpol (European network of Railway Police Forces).

The operation aims to respond to the shortage of statistics on flows of illegal immigration within the EU that have resulted from the abolition of systematic controls at internal borders. In the longer term, the operation shall contribute to political discussions and possibly lead to further political conclusions.

The operation consists of two phases: In the first phase, Member States were asked to provide a number of national statistics, which will feed into a Euro-

pean map giving a clear overview of the flows of illegal immigration. In the second phase, a number of large-scale coordinated actions will be organised simultaneously in all participating Member States in order to test the data from the first phase in practice. These operations will be coordinated through the above-mentioned three European police networks. The first phase is nearing completion. (CR)
➤eucrim ID=1003037

Judicial Cooperation

Cross-Border Enforcement: Traffic Offences

The Belgian Presidency has put the improvement of road safety in the EU and, in particular, the matter of cross-border enforcement high on its agenda. Cross-border enforcement in this context means that Member States exchange information in order to prosecute and punish EU citizens for every road offence committed in another Member State (as long as fines are concerned).

Activities under the Belgian Presidency include the organisation of a two-day conference on road safety to take place in Brussels from 14-15 October 2010. The conference will look at the initiatives of several Member States so far to prevent and push back cross-border traffic issues, such as speeding, driving under the influence (of alcohol and drugs), not using a seat belt, and failing to stop at a red light.

The sensitive issue of cross-border enforcement has been under discussion for years. A first step was taken in 2008 with the proposal for a directive facilitating cross-border enforcement in the field of road safety. The Framework Decision of 24 February 2005 on the application of the principle of mutual recognition to financial penalties also covers penalties imposed in respect of road traffic offences. Currently, the Commission is investigating a possible next step by considering the amendment of existing directives or the initiation of a new one. (CR)
➤eucrim ID=1003038

Financial Penalties – German Implementation

The German Bundestag adopted the German law implementing Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties. Under the Framework Decision, competent authorities of the Member States are asked to recognise and execute financial penalties of more than €70 issued by the authorities of other EU Member States.

Due to various constitutional issues raised by the German Länder, however, final enforcement of the law will need more time. Furthermore, additional laws need to be adopted in order to satisfy the German principle of "Halterhaftung," meaning that, in Germany, the owner of a car can only be held liable for infractions he or she committed him/herself and not for those committed by another driver with his/her car (except for violations of parking rules). German implementation of the 2005 Framework Decision, which required implementation by 22 March 2007, has already been delayed for several years. (CR)
➤eucrim ID=1003039

European Arrest Warrant

Practical Operation of the EAW in 2009

On 12 July 2010, the Council's General Secretariat published the Member States' responses to its questionnaire on the practical operation of the EAW in the year 2009. The questionnaire asked for quantitative information on the practical operation of the EAW in 2009 as well as the grounds for refusal applied in 2009 in addition to any other information regarding the operation of the EAW. No figures were provided by the UK and not all questions answered by all EU Member States.

According to the replies regarding the issuing of an EAW, of the Member States that replied, the three that issued by far the most EAWs in 2009 were Poland, Germany, and France with 4844, 2433, and 12,240 EAWs issued, respectively, while all other Member States were far below the 1000 mark. Poland and Germany transmitted 3907 and 2200 EAWs via Interpol, for instance, while Ireland and Latvia transmitted none via Interpol. Poland and Germany also made the most use of the Schengen Information System (SIS) as a means of transmission (3957 Polish, 2433 German). Almost none of the Member States has so far made use of the possibility to transfer an EAW via the secured line of the European Judicial Network. 1367 of the Polish and 777 of the German EAWs resulted in the effective surrender of the persons involved. The highest match of surrenders compared to the number of issued EAWs was achieved by Lithuania (56%) and Ireland (48%).

Looking at the execution of EAWs, the replies indicate that Spain (1629), France (967), and the Netherlands (683) were the three EU Member States whose judicial authorities received the most EAWs in 2009. Germany received 11,310 EAWs through SIS and 2142 through Interpol. Most persons were arrested under an EAW in Spain (1232) and Germany (1208), of which 982 were effectively surrendered in Germany and 990 in Spain. The correlation rate between receipt of an EAW and effective surrender was generally very high in 2009. In Cyprus and Latvia, 100% of the persons arrested were surrendered. In all Member States but the Netherlands and Sweden, of all persons arrested, more persons consented to their surrender than disagreed. Looking at the refusal to execute an EAW, Estonian and Cypriot judicial authorities did not refuse to execute a single EAW in 2009.

Generally, the number of refusals was quite low in the Member States (the indi-

The European Investigation Order in criminal matters – Towards the next level of obtaining evidence across internal borders in the EU

Brussels, 14-15 December 2010

In April 2010, seven EU Member States deemed the time ripe to make a clear step in European judicial cooperation in criminal matters and implement the Stockholm Programme in the field of evidence by launching an initiative for a so-called European Investigation Order (EIO).

The order can be seen as a reply to the fragmented and complicated mechanisms developed so far with regard to obtaining evidence abroad in the EU. Traditional mutual legal assistance is governed by multiple instruments adopted at different levels (Council of Europe, Schengen, EU). Moreover, both of the two main EU instruments in this area, the Framework Decision on the execution of orders freezing property or evidence (2003/577/JHA) as well as the European Evidence Warrant (EEW), could not convince. While the freezing order's scope is limited as to which transfer of evidence is still subject to mutual legal assistance results in many practitioners not seeing added value in its use. The foreseeable redundancy and possible negative impacts of the EEW due to its scope being limited to existing evidence have caused legislators to rate the EEW's implementation low on their agendas.

Hence, the EIO aims to introduce a comprehensive system based on the principle of mutual recognition, covering all types of evidence and most investigative measures. In this regard, the EIO constitutes a radical change in the current approach and aims to preserve the flexibility and efficiency of the existing cooperation of EU Member States in the framework of mutual legal assistance.

But what can be the level of ambition for such a comprehensive system? How to preserve its flexibility whilst covering investigative measures of very different natures? How to conciliate the different legal systems of the Member States? How to combine efficient judicial cooperation and a high level of procedural safeguards?

In cooperation with the Belgian Presidency, and together with representatives of the EU Member States, EU institutions, practitioners with long-standing experience in European cross-border cooperation as well as leading academics, this conference will present and discuss the pros and cons of such an approach, its added value for the practitioners, possible drawbacks, and its overall impact on European judicial cooperation.

This conference is organised in cooperation with the Belgian EU presidency. The conference will be held in English and French. Simultaneous interpretation will be provided.

For further information, please contact Mrs. Cornelia Riehle, Deputy Head of Section – Public and Criminal Law, ERA, E-mail: criehle@era.int .

vidual grounds for refusal by the Member States that replied to the questionnaire are listed in the second part of the analysis). The average surrender procedure for a person that agreed to the surrender varied between 1-5 days in Lithuania and 40 days in the Czech Republic. If the person did not agree, the average surrender procedure varied between 12 days in Estonia and 4,5 months in Ireland. Judicial authorities of most Member States were always able to observe the 90-day time limit for the decision on the execution of the EAW (Art. 17 (4)) as well as respect the 10-day time limit for surrender (Art. 23(2)). In case the 90-day time limit could not be met, Eurojust was, however, only very rarely informed. In almost no Member State was a person to be released due to the expiry of the time limit (Art. 23(5)), however, 13 cases were reported by Poland.

EAWs with regard to nationals or residents of the Member States were executed in all Member States that replied to the questionnaire except Lithuania. Most of the States never asked for an additional guarantee to have the person returned after the hearing to serve his/her sentence (Art. 5(3)). According to the responses, Member States also hardly made use of the other guarantees under Art. 5(1) and 5(2). (CR)

➤eucrim ID=1003040

European Investigation Order

UK Opt-In

Using its right under Art. 3(1) of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, on 27 July 2010, the UK gave formal notification of its intention to take part in the adoption of the initiative regarding the so-called European Investigation Order or EIO (see also eucrim 2/2010, p. 54). (CR)

➤eucrim ID=1003041

Discussions with Working Party on Cooperation in Criminal Matters

The Belgian Presidency has published the outcome of its meeting with the Working Party on Cooperation in Criminal Matters of 27-28 July 2010 where it discussed the European Investigation Order (EIO) initiative. In general, the meeting showed that all delegations were still in process of internal consultation and that a number of delegations had maintained a general scrutiny reservation on the initiative. Furthermore, the meeting revealed the need to ask the Council Legal Service for its opinion on whether the EIO is a development of the "Schengen Acquis" and what the consequences could be of replacement of the current legal framework on cooperation with non-participating Member States.

Specific issues that were discussed concerned:

- The scope of the EIO;
- The definition of the authorities competent to execute an EIO;
- The participation of competent authorities of the issuing State during the execution of an EIO in an executing State;
- Grounds for refusal;
- Time limits;
- Legal remedies.

Discussions regarding the actual scope of the EIO concerned:

- The possible inclusion of Joint Investigation Teams;
- Special forms of interception of telecommunications;

- Controlled deliveries;
- Other forms of mutual legal assistance, such as the serving of procedural documents in another Member State.

With regard to grounds for refusal, delegations discussed whether the following should be included:

- The submission of incomplete forms;
- The lack of proportionality;
- A breach of fundamental rights;
- Double criminality;
- Ne bis in idem;
- An age limit to criminal liability;
- The need to ensure the effectiveness of ongoing proceedings in the executing State;
- Excessive costs of the requested measure.

Finally, the Presidency also agreed to consider requesting the advice of the EU Agency for Fundamental Rights on the initiative for the EIO Directive. (CR)
➤eucrim ID=1003042

Types of Procedures for Issuing an EIO

In July 2010, the Belgian Presidency distributed a questionnaire to the Member States with a focus on certain types of procedures for which an EIO could be issued. Questions concerned the types of proceedings under Art. 4(b) and (c) of the initiative, namely proceedings brought by administrative authorities (Art. 4(b)) and judicial authorities (Art. 4(c)).

In its questionnaire, the Presidency asked Member States whether, in accordance with their national law, investigative measures could be ordered for these types of proceedings, and if yes, asked for additional information concerning the type of investigative measure(s) concerned, the kind of authority concerned, the types of punishable acts concerned, etc. Furthermore, if such measures were possible in the Member State, Member States were asked whether they would also be willing to make use of the EIO in those kinds of proceedings.

On 31 August 2010, the replies to the questionnaire were published. Responses were received from 20 Member States, of which 12 replied that they could not order investigative measures in proceedings under Art. 4(b) brought by administrative authorities. 13 Member States stated that they could not order such measures in proceedings under Art. 4(c) brought by judicial authorities. In their replies to the last question, regarding their willingness to use the EIO in such proceedings, two Member States stated that they would not be willing to use an EIO in contexts other than criminal proceedings. While the other States saw leeway for such a possibility, however, most of them would base their reply on the final content of the Directive. (CR)
➤eucrim ID=1003043

Questionnaire on Interception of Telecommunications

On 19 August 2010, the Belgian Presidency distributed a questionnaire investigating the scope of the proposed Directive on the so-called European Investigation Order with regard to the question of telecommunications. While the current proposal only includes ordinary interceptions of telecommunications, the questionnaire shall assess the relevance of four specific types of interception of telecommunication:

- Ordinary interception of telecommunications without immediate transmission;
- Ordinary interception of telecommunications with immediate transmission;
- Interception of satellite telecommunications (relationship between the requesting State and the State hosting the terrestrial station);
- Interception of telecommunications in cases where the requesting State does not need the technical assistance of the Member State where the target is located.

Of the four, only the first situation is covered by the current proposal. Amongst others, Member States are asked how many such cases they dealt with in the last five years, whether interception of satellite telecommunications is technically possible, and whether they host a terrestrial station. The deadline for submission of the questionnaire was 30 September 2010. (CR)
➤eucrim ID=1003044

Law Enforcement Cooperation

Change of Name for Police Cooperation Working Party

Since 1 July 2010, the Council's Police Cooperation Working Party changed its name to Law Enforcement Working Party (LEWP). The responsibilities of the LEWP now combine the activities of the former Police Cooperation Working Party with those of the Europol Working Party:

- Police cooperation issues, such as public order and safety;
- Telecommunications;
- Common education and training;
- Investigative techniques and forensic science;
- Exchange of police intelligence within the framework of Schengen cooperation.

It also includes issues regarding the Europol Council Decision and other legal instruments that govern the cooperation of Member States within the Europol framework. (CR)
➤eucrim ID=1003045

Use of Signs in the Field of Security

One of the issues that the Belgian Presidency has set on its agenda concerns the degree of uniformity of security signs (signs used by public and private security companies to indicate themselves and/or the security measure applied) in the EU and whether they are sufficiently recognisable by European citizens moving around the EU.

To assess this question, the Belgian Presidency distributed a questionnaire to the Law Enforcement Working Party asking for the existing national rules regarding security signs (as opposed to "safety" signs, e.g., signs used in buildings for fire prevention). 23 Member States responded to the questionnaire. The analysis of these replies was pre-

sented by the Presidency on 1 September 2010.

With regard to video surveillance, the replies showed that, while most of the Member States that allow for video surveillance ask for clear indication that such surveillance is in operation, the rules governing the method of signalling differ considerably from one Member State to the other.

Concerning private security, the survey indicated that Member States' regulations for specific emblems or logos on the work clothes of private guards also vary considerably, from regulated distinctive uniform emblems to authorised emblems and even to the simple requirement to use emblems or inscriptions that indicate the type of function carried out.

The replies revealed that most Member States do not have rules on displaying that a vehicle and/or container are/is used for the secure transport of valuables. The same is true for regulations regarding other pictograms, signs, emblems, or markings indicating private security.

With a view to security in general, half of the Member States replied that their regulations do not provide for other signs while the other half referred mainly to signs like pictograms indicating the presence of a police station, police checks, police officers, emblems worn by specific types of guards, police signs in general, and signs informing the public of specific security measures displayed on armoured vehicles, casinos, cash dispensers, etc.

In a second step, the Presidency assessed the question of whether it was useful and appropriate to take measures to standardise security signs in the EU. Of the 23 Member States that replied, 15 were in favour of such standardisation, five deemed it inappropriate, and two were partly in favour. Arguments favouring such standardisation underline the enhanced demand for security by European citizens moving around in the EU. Furthermore, the increased responsibilities of private security companies and their increased cross-border and international activities warrant the use of standard pictograms, signals, and symbols. Standardised pictograms in the field of public security would also increase legal certainty in the EU.

Arguments against standardisation mainly underline the fact that existing signs are already sufficiently clear and that standardisation would not improve security, especially in cases where private companies do not operate internationally. Furthermore, identical pictograms could be interpreted in different ways in different Member States. Other problems that were anticipated include the lack of effective cooperation between the different bodies in charge of security, the potential lack of interest on the part of the Member States, the subsidiarity principle, linguistic diversity, etc.

Summing up the replies, the Belgian Presidency arrived at the conclusion that it would be appropriate to move towards adopting Council conclusions that aim at encouraging Member States and European institutions wishing to prescribe a particular pictogram or graphic symbol in their legislation to take into account the signs that already exist in other Member States. In this way, the Presidency hopes to help produce easily recognisable signs in the EU. (CR)

➤eucrim ID=1003046

E-Justice

European E-Justice Internet Portal Opened

On 16 July 2010, the EU launched its so-called "European e-Justice portal." The website offers an electronic "one-stop-shop" for access to justice throughout the EU. The portal includes information for citizens, businesses, legal practitioners, and the judiciary.

Information provided to citizens includes advice on how to go to court and how to find a lawyer, notary, translator, interpreter, or mediator in the EU. Information is also available on family matters, legal aid, costs of proceedings, monetary claims, and mediation.

Information for businesses includes support on how to find the European Business Register (EBR) and national business registers, national insolvency registers, and "land registers" at the EU and national levels. Furthermore, it offers guidelines and information on cross-border legal proceedings, monetary claims, explanations of the different legal professions in the EU, and the possibilities for solving a dispute via alternative dispute resolution techniques, such as mediation.

For legal practitioners, the portal offers information on international, EU, and national law. It also provides information on EU and national jurisprudence, the types of and organisations for legal professions at the EU and national levels as well as the various justice networks, e.g., the European Judicial Network in civil and commercial matters or the European Judicial Network in criminal matters. Furthermore, it outlines the roles, tasks and activities of the so-called Justice Forum, a platform launched by the European Commission for consulting stakeholders on EU justice policies. Another chapter gives information on the organization of justice at the EU and national levels. Information on business, land, and insolvency registers at the EU and national levels can also be found here. Finally, there is a general introduction and advice on videoconferencing in cross-border cases.

The last chapter addressing the judiciary offers additional information on tools and facilities designed to facilitate the work of courts and justice practitioners at the EU and national levels, e.g., explanations on judicial cooperation in civil or criminal matters, judicial training opportunities, funding possibilities through Commission tenders and calls for proposals, and access to the European Judicial Atlas in civil matters.

The portal is available in all official languages of the EU. (CR)

➤eucrim ID=1003047

Council of Europe*

Reported by Dr. András Csúri

Foundations

Human Rights

Human Rights Commissioner Calls on Cyprus to "eradicate trafficking in human beings"

On 26 July 2010, following his on-site visit to Cyprus on 10 June 2010, Thomas Hammarberg, CoE Commissioner for Human Rights (hereinafter: the Commissioner), sent a letter to the Minister of Interior of the country. The letter underlined that progressive measures have been taken in Cyprus to fight trafficking in human beings and suggested that the country step up efforts to eradicate this "scourge" totally. The letter further focused on the human rights of asylum seekers and refugees. The Commissioner welcomed the abolition of the much criticised "cabaret artist visa" (linked to cases of forced prostitution of women in cabarets). However, he expressed his concern that other types of work permits, such as the one for barmaids, might be used to circumvent the law. Therefore, in his letter, the Commissioner stressed that the authorities should ensure that no type of visa or working permit be able to be abused for trafficking in human beings. The Commissioner further underlined that "ongoing awareness-raising efforts should be complemented with measures aimed at eliminating the nexus of sexual demand with trafficking". The Commissioner further stressed that budgetary cuts planned to face the economic crisis should not undermine adequate assistance to these victims. Regarding the human rights of asylum seekers and refugees, the Commissioner welcomed the improvement of access to health care, the labour market, and legal aid, but called for the removal of remaining administrative obstacles that may hamper the full enjoyment of these rights. Nevertheless, the Commissioner remained concerned about the long periods of detention that some asylum seekers are faced with. The letter urged the authorities to ensure an individual examination of each case in order to assess the purpose and proportionality of all asylum seekers' detentions.

➤eucrim ID=1003048

Specific Areas of Crime

Corruption

San Marino Joins GRECO

On 13 August 2010, the Republic of San Marino joined the Council of Europe Group of States against Corruption (GRECO) as its 48th Member State. By doing so, San Marino has actively committed itself to fighting corruption. The accession further strengthens GRECO's role as the reference for anti-corruption monitoring in Europe. Its membership extends to the entire continent, including all 47 Member States of the Council of Europe and other states such as the United States of America.

An on-site visit will be soon carried out in San Marino to study the capability of national institutions to deal with corruption cases, immunities as a possible obstacle to prosecution, the deprivation of proceeds of corruption, integrity in public administration, as well as the responsibility of legal persons. Next year, GRECO will produce a report on San Marino summing up the findings and containing possible recommendations for improvement. A further evaluation visit with a focus on the criminalisation of bribery and trading in influence, as well as the transparency of party funding, will follow later.

➤eucrim ID=1003049

GRECO: Third Round Evaluation Report on "the former Yugoslav Republic of Macedonia"

GRECO published its Third Round Evaluation Report on the former Yugoslav Republic of Macedonia (FYROM) on 30 August 2010. As always, the report focused on two distinct matters: criminalisation of corruption and transparency of party funding. A total of 13 recommendations were made. The findings stressed the need for legal improvements in the criminalisation of corruption and identified shortcomings in the effective implementation of the rules on party financing.

Regarding the criminalisation of corruption, GRECO found that, due to the legal reform of the Criminal Code, the law largely complies with the relevant provisions of the CoE's Criminal Law Convention on Corruption (hereinafter: the Convention). There are though loopholes though, such as the narrow range of possible perpetrators of private sector bribery. Or the requirement of dual criminality with respect to corruption offences committed abroad and also as regards the trading-in-influence offence, which all fall short of the standards of the Convention. The report also underlined the potential to misuse the line of

* If not stated otherwise, the news reported in the following sections cover the period July–September 2010.

defence of "effective regret," which can be invoked when an offender reports a crime after its commission. Concerning transparency of party funding, GRECO found that the relevant legal framework of FYROM is well developed and contains a number of strong features. Nevertheless, in practice, there is a lack of effective implementation of the rules on political financing. GRECO stressed that this problem may be attributed to the extremely sporadic and overall inefficient system of external supervision. The result is that possible infringements of political financing rules are not being prosecuted and sanctioned. The report stated that it is crucial for the credibility of the system that, in practice, the limits of election expenditure are respected, particularly as follows:

- By establishing an adequate financial reference period during election campaigns;
- By ensuring that goods and services granted at discount prices are properly identified and accounted for.

➤eucrim ID=1003050

GRECO: Third Round Evaluation Report on Hungary

On 29 July 2010 GRECO, published its Third Round Evaluation Report on the Republic of Hungary. On the whole, the report addressed 15 recommendations that GRECO had made earlier to the country. Regarding the criminalisation of corruption, the report found that legislation is, to a large extent, in conformity with the requirements of the Convention. It highlighted shortcomings, however, regarding foreign passive bribery in the private sector and the scope of the offence of trading in influence, which appears to be more limited than required by the Convention.

GRECO called for Hungary to urgently ratify the Additional Protocol to the Convention and to clarify the criminalisation of "domestic arbitrators". The report required further procedural adjustments regarding the extension of the limitation period for the prosecution of certain forms of bribery and trading-in-influence offences, as well as a review of the special line of defence of "effective regret" in order to minimise risks of misuse.

Concerning the transparency of party funding, the report noted the gap between the relatively good standards of Hungarian legislation on paper and its less effective application in practice. This has led to strong mistrust in the system of political financing. The absence of transparency in the financing of election campaigns is an area of particular concern, as a great majority of such funding is possibly not accounted for or reported at all in Hungary. In order to enhance the credibility of the system, GRECO stressed that the control on the part of the State Audit over political financing must be considerably sharpened through more frequent and swift audits, as well as by adopting a genuinely proactive approach. The financial discipline of political parties must also be strengthened, in particular by establishing clear rules obliging political parties to keep proper books and accounts and by subjecting them to an independent audit. Lastly, GRECO called for appropriate sanctions against the violation of funding rules.

➤eucrim ID=1003051

GRECO: Third Round Evaluation Report on Greece

On 7 July 2010, GRECO published its Third Round Evaluation Report on Greece. The report addressed a total of 27 recommendations made by GRECO, criticising primarily the country's excessively complex criminal legislation. It also suggested improvements in the transparency of the funding of political parties and election campaigns.

Regarding the criminalisation of corruption, GRECO concluded that Greek criminal legislation covers all offences of corruption and trading in influence criminalised by the Convention and its Additional Protocol. However, the effectiveness of their application is affected by the complexity of the legal framework. There are a number of shortcomings in the provisions on bribery of domestic, foreign, and international judges, arbitrators, jurors and members of public assemblies, and there are procedural obstacles to an effective fight against corruption. GRECO recommended abolishing the special shorter limitation period for the prosecution of corruption offences committed by members and former members of government. Furthermore, the report suggested removing the possibility to postpone or suspend prosecution of "political acts" and "offences through which international relations of the State may be disturbed."

As regards the transparency of party funding, GRECO acknowledged that there is a fairly comprehensive framework on the funding of political parties. However, it concluded that more trans-

Ratifications and Signatures

Council of Europe Treaty	State	Date of ratification (r), signature (s) or acceptation (a) of the provisional application
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)	Azerbaijan	3 May 2010 (r)
Criminal Law Convention on Corruption (ETS No. 173)	Spain	28 April 2010 (r)
Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 177)	Slovenia	7 July 2010 (r)

Council of Europe Treaty	State	Date of ratification (r), signature (s) or acceptation (a) of the provisional application
Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181)	Liechtenstein Montenegro Moldova Spain Bulgaria	28 January 2010 (r) 3 March 2010 (r) 29 April 2010 (s) 3 June 2010 (r) 8 July 2010 (r)
Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182)	UK	30 June 2010 (r)
Convention on Cybercrime (ETS No. 185)	Montenegro Azerbaijan Portugal Spain	3 March 2010 (r) 15 March 2010 (r) 24 March 2010 (r) 3 June 2010 (r)
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)	Montenegro Portugal Netherlands	3 March 2010 (r) 24 March 2010 (r) 22 July 2010 (a)
Protocol amending the European Convention on the Suppression of Terrorism (ETS No. 190)	Montenegro	28 April 2010 (r)
Protocol No. 14 to the Convention for the Protection of Human Rights and Fundamental Freedoms, amending the control system of the Convention (CETS No. 194)	Russia	18 February 2010 (r)
Convention on the Prevention of Terrorism (CETS No. 196)	Norway FYROM Netherlands Sweden	1 February 2010 (r) 23 March 2010 (r) 22 July 2010 (a) 30 August 2010 (r)
Convention on Action against Trafficking in Human Beings (CETS No. 197)	Estonia Netherlands Sweden Azerbaijan Ireland	3 February 2010 (s) 22 April 2010 (a) 31 May 2010 (r) 23 June 2010 (r) 13 July 2010 (r)
Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198)	Latvia Spain Portugal Slovenia San Marino	25 February 2010 (r) 26 March 2010 (r) 22 April 2010 (r) 26 April 2010 (r) 27 July 2010 (r)
Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201)	Netherlands San Marino Switzerland Serbia Spain Malta France	1 March 2010 (a) 22 March 2010 (r) 16 June 2010 (s) 29 July 2010 (r) 5 August 2010 (r) 6 September 2010 (r) 27 September 2010 (r)
Protocol No. 14bis to the Convention for the Protection of Human Rights and Fundamental Freedoms (CETS No. 204)	Lithuania FYROM Luxembourg Slovakia	5 February 2010 (s) 27 April 2010 (r) 14 April 2010 (r) 5 May 2010 (r)

➤eucrim ID=1003052

parency is needed, especially a more accurate recording of financial activities during election campaigns. The possibility of using anonymous coupons for donations should be abolished. All donations above a certain value should be made by bank transfer, and information on the financing of political parties and election campaigns should be published in a timely manner. The report most notably criticised the inefficient and obscure supervision of the funding of political parties and election campaigns, which may have contributed to the general mistrust in the system of political financing. GRECO therefore recommends strengthening the independence of the Control Committee responsible for this task, ensuring more substantial and ongoing monitoring, and reinforcing control over the financing of local and regional elections.

➤eucrim ID=1003053

Legislation

GRETA: Pan-European Campaign on Compensation for Trafficked Persons

The CoE Convention on Action against Trafficking in Human Beings (hereinafter: the Convention) has the first and still only international binding provision on the right of victims of trafficking in human beings to be compensated for the damage suffered, as well as the obligation for States to guarantee this compensation in their national law. The CoE granted institutional support on the basis of Art. 15 of the Convention to the COMP.ACT Project ("European Action for Compensation for Trafficked Persons") and the Pan-European Campaign on Compensation for Trafficked Persons. These projects are being undertaken by Anti-Slavery International and La Strada International, together with partners in 14 countries, and were launched in Prague on 2 July 2010.

➤eucrim ID=1003054

Der Europäische Auswärtige Dienst und seine Potentiale in Bezug auf die Gemeinsame Innen- und Justizpolitik

Elmar Brok/Christiane Ahumada Contreras

After the establishment of the post of the High Representative of the Common Foreign Affairs and Security Policy/Vice President of the European Commission (HR/VP) and an External Action Service (EEAS), the EU's external relations should become more coherent, more efficient, and more democratic. This article is dedicated to the question of how the HR/VP and the EEAS can be used as instruments for the realisation of an "area of freedom, security and justice." The article shows the linkage between Foreign Affairs on the one hand and Justice and Home Policy on the other, and it explores different possibilities and options as to how the HR/VP and the EEAS could benefit Justice and Home Policy. The aim is to address all relevant actors in order to pursue a clearer policy on all levels, using and combining all instruments of the EU to broadcast European interests and values throughout the world and thereby enhance security and welfare for all EU citizens.

I. Einleitung

Zu Beginn des 21. Jahrhunderts steht Europa innen- und außenpolitisch vor großen Herausforderungen – die Finanz- und Wirtschaftskrise, organisierte Kriminalität, illegale Migration, Terrorismus und der Klimawandel sind nur einige Beispiele, die unsere innere Sicherheit, unseren Frieden und unseren Wohlstand in Europa bedrohen. Erstmals wurden die Unmittelbarkeit und die Brutalität dieser Gefahren durch die Ereignisse des 11. September 2001 sowie die nachfolgenden Terroranschläge in Madrid und London deutlich. Konzeptionell zogen die europäischen Mitgliedstaaten bereits 2003 die Konsequenz und verabschiedeten die Europäische Sicherheitsstrategie (ESS),[1] in der sie die Hauptbedrohungen für Europa identifizierten und einen sogenannten „erweiterten Sicherheitsbegriff" definierten: Aufgrund der neuen Natur der Bedrohungen und der Verknüpfung von innerer Sicherheit mit äußeren Gegebenheiten müssen die europäischen Mitgliedstaaten gemeinsam diesen Bedrohungen in enger Zusammenarbeit mit ihren Partnern und unter Nutzung aller der EU zur Verfügung stehenden zivilen, militärischen und wirtschaftlichen Mittel entgegnen. Mit der Verabschiedung des Lissabonner Vertrags am 1. Dezember 2009 wurden nun, sechs Jahre später, auch die institutionellen Konsequenzen gezogen und die europäischen Institutionen grundlegend reformiert. Das Ziel: Europa transparenter, kohärenter, handlungsfähiger und vor allem auch demokratischer[2] zu machen. Dem in der ESS beschriebenen umfassenden Sicherheitsbegriff soll nun auch auf praktischer Ebene Rechnung getragen werden. In diesem Zusammenhang sind drei Neuerungen des Lissabonner Vertrags von besonderer Bedeutung: Erstens hat man den Posten eines Hohen Vertreters (HV), der zugleich Vizepräsident (VP) der Kommission ist und einen diesen unterstützenden Europäischen Auswärtigen Dienst (EAD) eingeführt. Zweitens wurde der bisher intergouvernementale Bereich der Polizeilichen und Justiziellen Zusammenarbeit (PJZ) vergemeinschaftet.[3] Drittens wurde die Säulenstruktur aufgelöst und der EU der Status eines Völkerrechtssubjekts übertragen, womit das Recht einhergeht, völkerrechtliche Verträge mit Drittstaaten abzuschließen.

Fast zeitgleich mit der Verabschiedung des Lissabonner Vertrags haben sich die Staats- und Regierungschefs mit dem am 2. Dezember 2009 verabschiedeten Stockholmer Programm,[4] das die innenpolitischen Leitlinien der nächsten Jahre festlegt, ein ehrgeiziges Ziel gesetzt: Einen Raum der Freiheit, der Sicherheit und des Rechts (RFSR) in Europa zu schaffen. Sowohl der Lissabonner Vertrag als auch das Stockholmer Programm gehen auf eine gemeinsame Erkenntnis der Mitgliedstaaten zurück: Angesichts der aktuellen Herausforderungen müssen sie enger und koordinierter denn je zusammenarbeiten. Sicherheit, Freiheit und Frieden in Europa können nur dann garantiert werden, wenn die Mitgliedstaaten gemeinsam vorgehen. Im Folgenden soll näher betrachtet werden, wie der Bereich der europäischen Außenpolitik, der durch den Lissabonner Vertrag grundlegend reformiert wurde, zur Realisierung des im Stockholmer Programm aufgezeigten RFSR beitragen kann. Was bedeutet die Einführung des HV/VP und des EAD für dessen Verwirklichung? Welche Möglichkeiten und Potentiale ergeben sich aus dem Bereich der Außenbeziehungen

der EU für die Gestaltung der Zusammenarbeit in der Justiz- und Innenpolitik (ZJIP)? Was kann der Beitrag des EAD im Kampf gegen das internationale Verbrechen sein? Wie kann die Verbindung zwischen dem EAD und der Schaffung von innerer Sicherheit aussehen? Was ist vorgesehen, was wäre wünschenswert und worauf sollten die handelnden Akteure achten?

Es geht darum, eine Verbindung herzustellen zwischen der durch den Lissabonner Vertrag gestärkten Außenpolitik der EU und der Schaffung des RFSR. Dieser Artikel soll ein Appell für eine insgesamt kohärentere EU-Politik auf allen Ebenen sein. Der Lissabonner Vertrag kann zwar den theoretischen, institutionellen Unterbau liefern – umgesetzt und genutzt werden müssen die neuen Mechanismen hingegen von den Akteuren.

II. Zum Verhältnis von Innen- und Außenpolitik

„Foreign Policy Begins at Home" – dieses geflügelte Wort hat heute weiterhin Gültigkeit. Jede Außenpolitik muss von innen heraus gestützt sein und es sind die innenpolitischen Verhältnisse und Bedürfnisse, die die Ziele und Strategien der Außenpolitik bestimmen. Aber es muss auch in die umgekehrte Richtung gedacht werden: Die Innenpolitik wird heute auch von der Außenpolitik gestützt. Wesentliche innenpolitische Ziele wie die Herstellung und Aufrechterhaltung von Sicherheit sind heute nicht mehr ohne eine effiziente und schlagkräftige Außenpolitik zu garantieren. Außen- und Innenpolitik stehen in einem Wechselverhältnis, bestimmen und definieren sich gegenseitig. So bemerkte der spanische Philosoph Ortega y Gasset bereits zu Anfang des 20. Jahrhunderts:

> Die großen Nationen sind nicht von innen gemacht, sondern nach außen; nur eine geschickte Außenpolitik (...) ermöglicht eine fruchtbare Innenpolitik (...).[5]

Aber man muss auch bedenken, dass Außenpolitik nicht allein von innenpolitischen Interessen geleitet ist. Es geht nicht nur um die Durchsetzung der internen Ziele wie Sicherheit und Frieden für das jeweilige Land, sondern auch um die Durchsetzung von Werten und Standards in der Welt. Die Grundpfeiler unseres europäischen Systems wie Demokratie, Rechtsstaatlichkeit und die Achtung der Menschenrechte werden über unsere außenpolitischen Instrumente in der Welt verbreitet und tragen somit über die europäischen Grenzen hinweg zu Frieden, Stabilität und Wohlstand bei. Die „Grundsätze und Ziele des auswärtigen Handelns" sind in Art. 21 EUV festgelegt. Es heißt hier:

> Die Union lässt sich bei ihrem Handeln auf internationaler Ebene von den Grundsätzen leiten, die für ihre eigene Entstehung, Entwicklung und Erweiterung maßgebend waren und denen sie auch weltweit zu stärkerer Geltung verhelfen will: Demokratie, Rechtsstaatlichkeit, die universelle Gültigkeit und Unteilbarkeit der Menschenrechte und Grundfreiheiten, die Achtung der Menschenwürde, der Grundsatz der Gleichheit und der Grundsatz der Solidarität sowie die Achtung der Grundsätze der Charta der Vereinten Nationen und des Völkerrechts.

Konzeptionell wurde die Wichtigkeit der Verbindung von Innen- und Außenpolitik in der ESS aufgegriffen. Die sich intern auswirkenden, aber oftmals extern entstehenden Bedrohungen sind nicht voneinander zu trennen. Die ESS erkennt, dass „bei den neuen Bedrohungen (…) die erste Verteidigungslinie oftmals im Ausland liegen (wird)"[6] und mahnt eine präventive Politik an. Auch das Stockholmer Programm hat diese Wechselbeziehung richtig erkannt. An zentraler Stelle heißt es:

> Die externe Dimension ist von entscheidender Bedeutung, um den zentralen Herausforderungen zu begegnen (...) Die externe Dimension der Politik in den Bereichen Freiheit, Sicherheit und Recht ist von entscheidender Bedeutung (...) und sollte insbesondere alle anderen Aspekte der EU-Außenpolitik berücksichtigen und mit diesen voll im Einklang stehen.[7]

Hier wird zum einem die Wichtigkeit einer externen Dimension von Justiz- und Innenpolitik angesprochen, und zwar dass eine Kooperation im Bereich der Justiz und Strafverfolgung innerhalb der Mitgliedstaaten, aber auch mit Drittstaaten, regionalen Partnern und internationalen Organisationen erfolgen muss. Kriminalitätsbereiche wie Terrorismus, organisierte Kriminalität, Korruption, Drogen und Migration haben eine klare internationale Dimension und müssen auf einer internationalen Ebene angesprochen werden. Die externe Justizpolitik trägt somit zu einem inneren Raum von Freiheit, Sicherheit und Justiz bei. Zugleich geht sie mit den Zielen der EU-Außenpolitik einher, indem sie Rechtsstaatlichkeit, Demokratie, Menschenrechte und gute Regierungsführung in anderen Staaten fördert. Externe Innen- und Justizpolitik und Außenpolitik haben daher ein großes Überschneidungsfeld – sie richten sich an die gleichen Partner und noch wichtiger: Sie verfolgen die *gleichen* Ziele. Letztlich liegt die Verflechtung von Außen- und Innenpolitik in der Parallelität der Ziele begründet. Sowohl die ESS als auch der Lissabonner Vertrag und das Stockholmer Programm gehen auf das gemeinsame Streben nach Frieden, Sicherheit und Wohlstand zurück. Der Aktionsplan der Kommission zur Umsetzung des Stockholmer Programms fordert deswegen konkret Rückkoppelungsmechanismen der beiden Politikbereiche:

> Continuity and consistency between internal and external policies are essential to produce results, as is coherence and complementarity between the Union and Member States' action.[8]

Worin liegen genau die Chancen einer engeren Koordinierung von Innen- und Außenpolitik? Im Allgemeinen zunächst in den unterschiedlichen Instrumentarien, die der Innen- und der Außenpolitik zur Verfügung stehen. Hat die Innenpolitik

eher ein reaktives, sanktionierendes Instrumentarium, so steht der Außenpolitik ein aktives, präventives Instrumentarium zur Verfügung. Der Bereich der Innen- und Justizpolitik der EU *reagiert* zum Beispiel mit Maßnahmen zur Drogenbekämpfung, Nachrichtenauswertung, Grenzkontrolle, grenzüberschreitender strafrechtlicher Zusammenarbeit, Auslieferung und Strafverfolgung. Diese Instrumente sind sinnvoll und müssen in Zukunft gestärkt werden. Allerdings braucht man einen breiteren Ansatz, der auch aktivere, präventive Mechanismen mit einbezieht. Die Instrumente der EU-Außenpolitik, die sowohl Entwicklungszusammenarbeit, diplomatische Beziehungen, Handelspolitik, die intensive Kooperation mit Drittstaaten über Verträge und Abkommen, gemeinsame Erklärungen und Aktionspläne, Experten- und Ministertreffen, die Überwachung und Evaluation von Programmen, sowie die Implementierung von Hilfsprogrammen und zivile und militärische Kriseneinsätze in aller Welt umfassen, müssen zur Konfliktprävention eingesetzt werden – Terrorismus, Kriege und Konflikte entstehen nicht gänzlich unvorhergesehen. Diese präventiven außenpolitischen Instrumentarien, die durchaus auch sanktionierende Wirkung haben können und Wirtschaftssanktionen einschließen, müssen mit den Möglichkeiten der innen- und justizpolitischen Maßnahmen kombiniert werden.

Deswegen forderte schon 2005 der Europäische Rat in der Strategie zur externen Dimension der Justiz und Innenpolitik: "The EU should (...) make JHA a central priority in its external relations."[9] Im Aktionsplan der Kommission zur Umsetzung des Stockholmer Programms werden sogar explizit die HV/VP und der EAD als Chancen erwähnt, die gewünschte Kohärenz von Innen-/Justizpolitik und Außenbeziehungen zu realisieren[10], ohne allerdings auszuführen, worin diese Chancen bestehen könnten. Und auch die Ratsentscheidung über den Aufbau des EAD bekräftigt: "The Union will ensure consistency between the different areas of its external action and between those areas and its other policies,"[11] ohne dabei konkret zu werden.

Wie können also konkret die HV/VP und der EAD zu der geforderten besseren Verknüpfung der innen- und außenpolitischen Instrumente beitragen? Um dies zu beurteilen, muss zuvor ein Blick auf die Befugnisse der HV/VP und die Struktur des EAD geworfen werden.

III. Struktur und Befugnisse von HV/VP und EAD

Die Schaffung des EAD ist auf administrativer Ebene die Konsequenz dreier vom Vertrag von Lissabon eingeführter Neuerungen: Erstens der Wahl des ständigen Präsidenten des Europäischen Rates, der auf der Ebene der Staats- und Regierungschefs die Außenvertretung der Union wahrnimmt, zweitens der Ernennung des Hohen Vertreters für Außen- und Sicherheitspolitik der Union, der zugleich Vizepräsident der Kommission ist und drittens der ausdrücklichen Zuerkennung der eigenen Rechtspersönlichkeit, die die Union auf internationaler Ebene in vollem Umfang handlungsfähig macht. Der EAD ist allerdings keine entscheidungsbefugte Institution, sondern lediglich ein Dienst, der nach Art. 23III EUV die HV/VP bei der „Erfüllung" ihrer Aufgaben unterstützen soll. Deswegen muss der Posten der HV/VP näher betrachtet werden.

Bisher gab es die Außenkommissarin, der die finanziellen Mittel und ein großer Apparat zur Verfügung standen. Zudem gab es den Hohen Beauftragten, der ein Verhandlungsmandat, aber weder Geld, noch einen Verwaltungsapparat zur Verfügung hatte. Und es gab die Ratspräsidentschaft, die den Vorsitz des Außenministerrates leitete, aber alle sechs Monate wechselte. Nun wurden diese Posten in der Person der HV/VP vereinigt. Diese hat einen „Doppelhut" auf und ist als HV für die Planung und Durchführung der im Rat angesiedelten intergouvermentalen Gemeinsame Außen- und Sicherheitspolitik/Europäische Sicherheits- und Verteidigungspolitik (GASP/ESVP) zuständig. Als VP koordiniert sie die verschiedenen gemeinschaftlichen Außenpolitiken der Kommission wie die Entwicklungs- und Handelspolitik sowie die humanitäre Hilfe und Krisenreaktion. Als Vorsitzende des EU-Außenministerrates wiederum bestimmt sie die Agenda und bereitet Beschlussvorlagen vor.

Mit dem EAD kann die HV/VP nun nicht mehr nur auf dem kleinsten gemeinsamen Nenner nationaler Politik, sondern auf hohem Niveau gemeinsame Außenpolitik betreiben. Der EAD reflektiert den Doppelhut der HV/VP und ist ein „hybrider Dienst", indem er die gemeinschaftlichen und intergouvernementalen Komponenten der EU-Außenbeziehungen vereint und dadurch zu mehr Kohärenz auf horizontaler Ebene zwischen Rat und Kommission beiträgt. Dadurch kann die GASP mit den sonst gemeinschaftlich verfassten auswärtigen Instrumenten koordiniert werden, ohne diese Bereiche zu intergouvermentalisieren. Zu diesem Zweck werden insbesondere die Dienststellen von Kommission und Rat, die mit Außenbeziehungen betraut sind, sowie die Delegationen der Kommission[12] in Drittländern unter dem Dach des EAD vereint.

Man erreicht hier Verbesserung in zweierlei Hinsicht: Die europäische Außenpolitik wird kohärenter und transparenter für den Rest der Welt. Und sie vereint zudem auf vertikaler Ebene die nationalen und europäischen Ebenen der Diplomatie. Durch die Einführung der HV/VP und des EAD bietet sich die Chance, eine kohärentere Außenpolitik zu führen. Welche Potentiale bieten sich hier wiederum für die Umsetzung des Stockholmer Programms und die Herstellung eines RFSR?

IV. Der Beitrag des EAD zur Umsetzung des Raumes der Freiheit, der Sicherheit und des Rechts

Erstens wird dadurch, dass der Bereich der EU-Außenbeziehungen in sich kohärenter gestaltet wird, eine Zusammenarbeit mit den Bereichen der Innen- und der Justizpolitik einfacher. Die Kommissarinnen Reding und Malmström haben jetzt *einen* übergreifenden Ansprechpartner für den Bereich der Außenbeziehungen: Die HV, die als Vizepräsidentin der Kommission gemeinsam mit ihnen im Kollegium sitzt, so dass Details wiederum mit dem Entwicklungskommissar oder Handelskommissar abgestimmt werden können und sich so das Ganze zusammenfügt. Dadurch sollte auch eine bessere Koordinierung mit den Maßnahmen im Rahmen der Zusammenarbeit in der Innen- und Rechtspolitik (ZIJP) zu erzielen sein. Eine hochrangige Zukunftsgruppe Innenpolitik der Mitgliedstaaten,[13] die im Juni 2008 ihre Empfehlungen veröffentlichte, forderte, dass noch in der Planungsphase die verschiedenen Komponenten eingebunden und alle zivilen, militärischen und justiziellen Einheiten eines Einsatzes von Anfang an zusammengeführt werden sollten.

Der EAD bietet dafür insofern die Voraussetzung, als dass die geografischen Prioritäten der externen Dimension von Justiz, Freiheit und Sicherheit[14] in den EAD als geografische und thematische „Desks“ integriert sind. Denn sowohl die ehemalige Generaldirektion Außenbeziehungen (Relex) der Kommission mit allen ihren geografischen und thematischen Abteilungen als auch die kompletten ESVP und Krisenmanagementstrukturen des Rates wurden in den EAD überführt. Ob Beziehungen zu den USA, Russland, China, oder die Task Force für die Östliche Partnerschaft und Menschenrechte, dies alles wird unter dem Dach des EAD direkt mit den Ratsstrukturen der GASP/ESVP koordiniert. Indem er alle Instrumente der europäischen Außenbeziehungen zusammenführt, kann er auf breiterer Basis die Entwicklung von Rechtstaatlichkeit und die Achtung von Menschen- und Grundrechten fördern.

Damit dieses nicht nur Theorie bleibt, wurden zum Beispiel bezüglich der Rolle, die die Förderung von Menschenrechten sowie das Krisenmanagement und friedensschaffende Maßnahmen in der Struktur des EAD spielen, auf Druck des Europäischen Parlaments Garantien gegeben. Während Menschrechte im ersten legislativen Entwurf der HV/VP Ashton nicht erwähnt wurden, hat sie sich nunmehr in einer Erklärung vor dem Plenum zu folgendem verpflichtet:

> The HR will give high priority to the promotion of Human Rights and good governance around the globe and promote its mainstreaming into external policies, throughout the EEAS. There will be human rights and democracy structure at headquarters level as well as focal points in all relevant Union delegations with the task of monitoring the human rights situation and promoting an effective realisation of EU human rights policy goals.[15]

Zudem ist alles Handeln der HV/VP an die durch den Lissabonner Vertrag rechtlich verbindliche Grundrechtecharta gebunden.

Durch die Zusammenführung der Rats- und Kommissionsstrukturen der europäischen Außenpolitik im EAD wird auch eine bessere Terrorismusbekämpfung möglich. Es handelt sich hierbei um eine Querschnittsaufgabe, die über alle Politikbereiche der EU hinweg gemeinsam behandelt werden sollte. Im Rahmen der vergemeinschafteten Außenpolitiken kann Unterstützung für Drittländer bei der Terrorismusbekämpfung geboten werden, im Rahmen der GASP/ESVP können z.B. mit Drittstaaten Deklarationen für Aktivitäten gegen terroristische Organisationen verabschiedet werden und im Bereich der ZJIP hat es mehrere Maßnahmen zur Stärkung der Zusammenarbeit zwischen den Sicherheitsbehörden der EU-Mitgliedstaaten gegeben. Bisher gibt es zwar einen gemeinsamen Ansatz auf EU-Ebene,[16] jedoch (noch) keine gemeinsame Vorgehensweise. In Koordinierung mit und über den EAD sollten gemeinsame Verfahrensweisen gefunden werden. Die Aufgabe des EAD sollte es also sein, Unterstützung für Drittländer zu gewähren und Ansätze für gemeinsame Maßnahmen zu entwickeln sowie diese zusammenzuführen. An den Polizeimissionen, die über die GASP/ESVP in aller Welt tätig sind, wird die Überlappung von Innen- und Außenpolitik besonders deutlich.[17]

Zweitens erhält die EU durch die Umwandlung der Kommissionsdelegationen in EU-Delegationen ein höheres außenpolitisches Gewicht gegenüber Drittstaaten. Hier eröffnen sich neue Verhandlungsmöglichkeiten, die die Justiz- und Innenkommissarinnen nutzen sollten. Auch sie sollten über die EU-Delegationen als Vertreter der EU mit den Drittstaaten kooperieren und darüber ihre Prioritäten einbringen. Durch den EAD sollte eine in politischer und operationeller Hinsicht engere Koordination mit Drittstaaten erreicht werden. Wichtig sind vor allem die Kooperation mit dem Partner USA, aber auch mit strategischen Partnern wie China und Russland – und nicht zuletzt mit den sogenannten „failed states“. Im Rahmen der Außenbeziehungen der EU gibt es vielfältige Initiativen und Abkommen in der unmittelbaren Nachbarschaft der EU – Die Östliche Partnerschaft, die Mittelmeer-Union und die Schwarzmeerkooperation sind gute Beispiele. Hier muss die HV/VP darauf achten, dass beispielsweise in den Partnerländern der Östlichen Partnerschaft auch justiz- und innenpolitische Bereiche umgesetzt werden, zum Beispiel bezüglich Migration und Grenzschutz und mit Blick auf eine graduelle Annäherung an eine Visaliberalisierung. Auch im Rahmen der Mittelmeerunion müssen Themen wie Migration, Drogenschmuggel, Stärkung der Zivilgesellschaft und eine verstärkte Zusammenarbeit in Strafsachen gefördert werden. Ebenso ist die Kooperation mit unserem wichtigsten Partner, den USA, sehr wichtig. Die EU-US Zusammenarbeit muss z.B. im

Bereich der Internetkriminalität gestärkt werden. Und natürlich muss bei der Bekämpfung des Terrorismus zusammengearbeitet werden, wie der missglückte Anschlag auf den Flug von Amsterdam nach Detroit zeigt. Hier sollten die Netzwerke der EU-Delegationen und des EAD genutzt werden.

Drittens ist insbesondere das in Art. 216 AEUV festgelegte Recht der EU, Verträge entsprechend dem in Art. 218 AEUV beschriebenen Verfahren abzuschließen, entscheidend. Praktisch wird es so aussehen, dass der Ministerrat einen Verhandlungsführer ernennen wird. In GASP Angelegenheiten wird das die HV/VP sein und in Angelegenheiten, die unter den vergemeinschafteten Bereich fallen, der jeweils zuständige Kommissar. Bei sogenannten „Cross-Pillar-Mixity" Abkommen, die sowohl die intergouvermentalen als auch die vergemeinschafteten Politikbereiche der EU betreffen, muss laut Art. 218 AEUV der Ministerrat entscheiden, wer die Verhandlungsführung übernimmt. Es bietet sich die Chance, dass die Innen- und Justizpolitik ihre Ziele über die HV/VP und den EAD auch in Abkommen einfließen lassen, die nicht primär die polizeiliche und justizielle Zusammenarbeit mit Drittstaaten zum Gegenstand haben. So könnten etwa in Partnerschaftsabkommen neben Umwelt- und Sozialklauseln auch gemeinsame Maßnahmen im Bereich der Terrorismusbekämpfung, Menschenhandel, Drogenhandel sowie Menschenrechtsstandards und Regeln für eine gemeinsame Strafverfolgung und Auslieferungen vereinbart werden. Die HV/VP und der EAD können Rechtsstaatlichkeit und Justiz wie auch die Prävention von illegalen Aktivitäten im Rahmen von Partnerschafts- und Kooperationsabkommen unterstützen, Demokratie fördern und europäische Interessen, Werte und Standards durchsetzen.

Dieser neue „Mix" wird in internationalen Verträgen schrittweise Bedeutung erlangen. Es geht dann darum, wie man über die Außen- und Sicherheitspolitik hinaus auf breiter Linie Politik beeinflussen kann – z.B. im Hinblick auf Menschenrechtsfragen, Fragen, die mit Umweltschutzstandards zu tun haben oder Fragen, die mit sozialen Rechten zu tun haben. Die HV/VP und vor allem auch das Europäische Parlament über seinen Ausschuss für Menschenrechte müssen sich dafür einsetzen, dass dementsprechende Klauseln, die in Assoziierungsverträgen oder auch Handelsabkommen integriert sind, umgesetzt werden. Das EP muss also darauf achten, dass diese nicht nur „auf dem Papier stehen", sondern auch angewandt werden. Dieses darf aber keineswegs protektionistischen Zielen dienen, sondern muss in einer ausbalancierten Art und Weise geschehen. Es sollten also nicht einzelne, sondern umfassende Abkommen mit Drittstaaten abgeschlossen werden. Wenn man im Paket verhandelt, hat man mehr Durchsetzungskraft und mehr Verhandlungsspielraum, da Kompromissmöglichkeiten gegeben sind. Kritisch ist z.B. die Erklärung der EU und Russlands zum Abschluss der „Partnership for Modernization" (PFM),[18] welche unabhängig vom Partnerschafts- und Kooperationsabkommen (PCA), welches zurzeit noch verhandelt wird, abgegeben wurde. Hat man damit nicht Verhandlungsspielraum aus der Hand gegeben, den man hätte nutzen sollen?[19]

Viertens kann die HV/VP über die EU-Delegationen Informationen erhalten, auf deren Basis im EAD Zentrum in Brüssel Entscheidungen langfristig und gezielt vorbereitet werden. Die bisherigen Kommissions-Delegationen mussten sich häufig mühselig Informationen aus den nationalen Botschaften beschaffen. Da die Kommissionsbeamten aber oft nicht die notwendigen Kontakte hatten, war der Informationsfluss zäh und unvollständig. Der EAD verbindet hingegen auch in personeller Hinsicht nicht nur auf horizontaler, sondern auch auf vertikaler Ebene. Diplomaten werden nicht nur aus Kommission und Rat, sondern direkt aus den Mitgliedstaaten abbestellt: Da Ratsbeamte und mitgliedstaatliche Beamte oft besser an die Mitgliedstaaten angebunden sind, ihre Kontakte und Netzwerke haben, ist ein besserer Informationsfluss zu erwarten, der wiederum für eine bessere und effizientere Strafverfolgung von großem Nutzen sein kann.

Die Integration des Gemeinsamen Lagezentrums SitCen in den EAD[20] bietet hierfür ebenfalls Potential. Schon in seinem Bericht über den EAD von Oktober 2009 forderte das EP, dass, „um den Vizepräsidenten und Hohen Vertreter bei der Erfüllung seines Auftrags einer einheitlichen, kohärenten und effizienten Außenpolitik der Union zu unterstützen, (...) eine gemeinsame nachrichtendienstliche Auswertung durch die Akteure innerhalb des EAD von grundlegender Bedeutung" sei. Ist in nationalen Botschaften vor Ort in Drittstaaten nicht selten ein Kontaktmann des BND vertreten, so müssen wir Ähnliches für die EU-Botschaften erreichen. Um einen gesammelten Informationsfluss zu garantieren, ist wichtig, dass alle Informationen wie auch Anweisungen über die HV/VP laufen. Informationen und Analysen von SitCen müssen eng mit Europol und Eurojust ausgetauscht werden und gemeinsame Parameter für die Erstellung von Analysen und Bewertung von Informationen erstellt werden. Insgesamt muss ein besserer Informationsfluss zwischen den Strafverfolgungsbehörden der Mitgliedstaaten, Eurojust und Europol erreicht werden.

Wichtig ist auch, dass alle Anweisungen an die Delegationen über die HV/VP laufen. Der Delegationsleiter erhält die Anweisungen direkt von der HV/VP und ist für die Umsetzung verantwortlich. Allerdings kann auch die Kommission, wenn es in ihren Bereich fällt, direkt Anweisungen an die Delegationsleiter geben. Hier liegt es in der Verantwortung der Akteure, eine enge Absprache zu handhaben. Vor allem die Delegationsleiter, die direkt der HV/VP Bericht erstatten müssen, nehmen diesbezüglich eine zentrale Rolle ein.

V. Abschließende Überlegungen

Die Möglichkeiten des EAD mit Blick auf die Umsetzung des Stockholmer Programms und die Herstellung eines RFSR liegen zusammengefasst darin, dass er eine Nahtstelle für alle auswärtige Politik, also auch für die externe Dimension der ZIJP, bilden und mit den anderen Außenpolitiken der EU koordiniert werden kann. Ob dies gelingt, liegt vor allem in den Händen der HV/VP. Diese kann als VP der Kommission Rücksprache mit dem Justiz- und Innenkommissar halten, als HV und Vorsitzende des Außenministerrates kann sie Politik mit Nationalstaaten koordinieren und Entscheidungen vorbereiten. Dadurch können gemeinsame Definitionen, Perzeptionen, Strategien und Handlungsansätze entwickelt werden. Außerdem ist ein wesentlich besserer, detaillierterer und effizienterer Informationsfluss zu erwarten. Zweitens kann über die HV/VP und den EAD ein gemeinsames Auftreten gegenüber Drittstaaten gewährleistet werden und dadurch die Durchsetzung europäischer Werte, Standards und Interessen sowie die Kooperation mit Drittstaaten bezüglich Terrorismusbekämpfung, Achtung der Menschenrechte etc. verbessert werden. Drittens können mit Hilfe der HV/VP und des EAD gemischte Verträge ausgehandelt werden, die über den konkreten Vertragsgegenstand hinaus auch Abkommen im Bereich der Strafverfolgung, der Menschenrechtsstandards und der Terrorismusbekämpfung einbringen.

Allerdings muss beachtet werden, dass der Kommissionspräsident zu Recht auf Artikel 17 des Vertrages hingewiesen hat, nach dem für alle auswärtigen Beziehungen mit Ausnahme der GASP/ESVP die Kommission zuständig ist. Artikel 21 sagt auch, dass die Kommission die Vorschläge in allen Fragen der auswärtigen Beziehungen macht, erneut und eben nur mit Ausnahme der GASP/ESVP. Dies bedeutet, dass z.B. die Handelspolitik ebenso wie die ehemaligen Gemeinschaftszuständigkeiten nicht intergouvernemental be- und verhandelt werden können. Was nicht in die Zuständigkeiten des künftigen Europäischen Auswärtigen Dienstes (EAD) zu fallen hat, sondern in den bisherigen Zuständigkeiten der Kommission verbleibt, bedarf einer engen, dem Integrationsprinzip folgenden Verbindung durch eine gemeinsame außenpolitische Strategie sowohl auf der exekutiven Ebene als auch auf legislativer Ebene im Hinblick auf die Zusammenarbeit zwischen dem Handelsausschuss des EP und dem Auswärtigen Ausschuss des EP.

Insgesamt müssen wir es schaffen, unsere außen- und innenpolitischen Instrumentarien miteinander so in Einklang zu bringen, dass die Summe die EU als Ganzes stärkt. Innerhalb der EU-Institutionen gilt es daher auch zu überlegen, wie die Hauptakteure der Außenbeziehungen und der Innen- und Justizpolitik effiziente Methoden der Kooperation des Meinungsaustauschs entwickeln können, damit die relative Stärke der EU für zentrale politische Ziele genutzt werden können. Wünschenswert ist, dass der EAD ähnlich einem nationalen Außenministerium eine koordinierende Rolle bei allen Aspekten auswärtigen Handelns einnimmt. In Deutschland zum Beispiel trifft sich unter dem Vorsitz des Auswärtigen Amtes alle zwei bis drei Monate der sogenannten „Staatssekretärausschuss für Europaangelegenheiten“, an dem neben den Europa-Staatssekretären auch der ständige Vertreter bei der EU teilnimmt. Ziel dieser Treffen ist es, Entscheidungen und Positionen vorzubereiten und Konflikte zwischen den Ressorts zu lösen. Zudem treffen sich jeden Dienstag im sogenannten Dienstagsausschuss die Ressortleiter aus den einzelnen Ministerien, die sich mit EU-Fragen beschäftigen.[21] Ähnliche Mechanismen müssen auch auf europäischer Ebene gefunden werden. In jeder Generaldirektion der Kommission sollte es zuständige Beamte geben, die als Verbindungsstellen zwischen ihrem Ressort und dem EAD dienen sollten. Unter dem Dach des EAD sollten diese sich regelmäßig treffen. Zudem sollten auf einem High-Level Niveau regelmäßig alle mit Außenbeziehungen befassten Kommissare sowie die Kommissare für Inneres und Justiz unter der Leitung der HV/VP zusammenkommen. Dabei wäre auch sinnvoll, dass regelmäßig Delegationsleiter aus strategisch entscheidenden Drittstaaten zur Berichterstattung und Abstimmung der Maßnahmen eingeladen werden.

Noch einmal der vergleichende Blick nach Deutschland: Auf Bundesebene muss das jeweils zuständige Ministerium bei einem neuen Richtlinienvorschlag der Kommission die anderen betroffenen Ministerien informieren und um eine Stellungnahme bitten. Aus den verschiedenen Stellungnahmen heraus wird dann eine Verhandlungsposition erarbeitet. Zu einer solchen Koordinierung müssen wir auch auf europäischer Ebene kommen. Justiz-/Innenpolitik und Außenpolitik sollten nicht getrennt geplant werden. Auch hier gilt es, engere Abstimmungsmechanismen zu finden. Beachtet werden sollte auch, dass bei dem Abschluss von internationalen Abkommen das EP zustimmen muss. Deswegen muss eine frühzeitige Information und Koordinierung gegeben sein.

Gibt es im Auswärtigen Amt der Bundesrepublik eine sogenannte EU-Koordinierungsgruppe, die laufend die Meinungsbildungsprozesse der EU-Institutionen analysiert, um so zu sehen, wo Konflikte liegen und wo verhandelt werden muss, sollte es Ähnliches im EAD geben, um so die Rückkoppelung an die DG Justiz und DG Inneres sowie die Mitgliedstaaten zu garantieren. Eine solche Koordinierungsgruppe sollte auch eng an die Delegationsleiter der EU-Botschaften angeschlossen sein, um diesen die Informationen für ihre Arbeit vor Ort zu liefern. Wichtig sind die enge Koordinierung und der Informationsaustausch zwischen Mitgliedstaaten und EU-Agenturen und Institutionen wie FRONTEX, Europol, Eurojust, OLAF mit dem EAD.

Es wird von den politischen Akteuren abhängen, ob der EAD ein effizienter, durchsetzungsfähiger Dienst sein wird. Insbesondere die Mitgliedstaaten müssen bereit sein, nationale Eitelkeiten zu überwinden und gemeinsam auf internationaler Bühne aufzutreten. Ein Beispiel, wie problematisch das sein kann, zeigt die Tatsache, dass einzelne Mitgliedstaaten immer noch Waffen an Drittstaaten liefern, ohne dies mit ihren europäischen Partnern abzustimmen. An diesem hochbrisanten Beispiel, das derzeit auch im EP diskutiert wird, wird deutlich, dass die Koordinierung hier noch nicht funktioniert. Und die Frage ist sowohl für die Außenpolitik als auch die Herstellung des RFSR hochbedeutsam. Denn die Waffenlieferung an Drittstaaten hat sicherheitspolitische Brisanz – die Waffen können in die Hände von terroristischen Gruppen geraten und unsere Sicherheit in Europa gefährden. Zudem kann eine solche einzeln vorgenommene, nicht mit den europäischen Partnern abgestimmte Waffenlieferung die europäische Außenpolitik konterkarieren. Wie kann man ein Land für seine Menschenrechtspolitik kritisieren, wenn ihm zugleich aus den eigenen Reihen die Waffen geliefert werden, mit denen es seine repressive Politik ausführen kann? Dieses Beispiel macht nochmals die Wichtigkeit eines kohärenten Vorgehens auf europäischer Ebene deutlich.

Doch sowohl die gemeinsamen innen- als auch außenpolitischen Ziele können nicht verwirklicht werden, wenn die politischen Akteure diese Solidarität und gemeinsame Identität nicht leben. Um eben diese Unterschiede und Diskrepanzen zu überwinden, sieht Art. 34 EU in Bezug auf Art. 19 EU eine Treu-, Förderungs- und Unterrichtungspflicht der Mitgliedstaaten vor. Die Mitgliedstaaten sollen die GASP aktiv und vorbehaltlos im Geiste der Loyalität und gegenseitigen Solidarität unterstützen, das Handeln der EU in diesem Bereich achten und sich jeder Handlung enthalten, die den Interessen der Union zuwiderläuft oder ihrer Wirksamkeit schaden könnte. Bleibt – in unser aller Interesse – zu hoffen, dass dies nicht nur ein Bekenntnis auf dem Papier bleibt, sondern der notwendige politische Wille da ist, die beschriebenen Potentiale im Bereich der Außenpolitik für die Verwirklichung eines Raumes der Freiheit, der Sicherheit und des Rechts zu nutzen.

Elmar Brok
Mitglied des Europäischen Parlaments,
Außenpolitischer Sprecher EVP-Fraktion

Christiane Ahumada Contreras
Wissenschaftliche Referentin, Europäisches Parlament

1 Ein sicheres Europa in einer besseren Welt, Europäische Sicherheitsstrategie, Brüssel den 12. Dezember 2003, zu finden unter http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIDE.pdf.

2 Vor allem die Rechte des Europäischen Parlaments (EP) wurden gestärkt. So ist das EP nun gleichberechtigter Co-Gesetzgeber neben dem Rat. Zudem wurden die Budgetrechte des EP ausgeweitet und verstärkte Kontrollrechte gegenüber der Exekutive eingeführt. Für ausführlichere Informationen zu den neuen Rechten des EP nach dem Vertrag von Lissabon vgl. Elmar Brok, Neue Basis oder neue Konflikte? Die Machtbalance der europäischen Institutionen nach Lissabon, in: Kurt J. Lauk, Europa von innen gesehen: Europa jenseits der Bürger, Stuttgart, Leipzig 2009, S. 68-87.

3 Für eine ausführliche Darstellung der Justiz- und Innenpolitik nach dem Vertrag von Lissabon siehe Daniela Kietz/Roderick Parkes, Justiz- und Innenpolitik nach dem Lissabonner Vertrag, Diskussionspapier Stiftung Wissenschaft und Politik, 13. Mai 2008, Berlin, zu finden unter http://www.swp-berlin.org/common/get_document.php?asset_id=5000.

4 Rat der Europäischen Union, Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, Brüssel 2. Dezember 2009, zu finden unter http://register.consilium.europa.eu/pdf/de/09/st17/st17024.de09.pdf.

5 Ortega y Gasset, José, Aufbau und Zerfall Spaniens (Originaltitel: España invertebrada: Bosquejo de algunos pensamientos históricos), Madrid 1957, S. 157.

6 ESS, S. 7.

7 Stockholmer Programm, S. 5.

8 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, Delivering an area of freedom, security and justice for Europe's citizens. Action Plan implementing the Stockholm Programme, Brüssel 20.4.2010, zu finden unter http://ec.europa.eu/commission_2010-2014/malmstrom/archive/COM%202010%20171%20EN.pdf .

9 Council of the European Union, A Strategy for the External Dimension of JHA: Global Freedom, Security and Justice, Brüssel, 30. November 2005, S. 2, zu finden unter http://register.consilium.europa.eu/pdf/en/05/st14/st14366-re03.en05.pdf .

10 Communication, Implementing the Stockholm Programme, S. 8, zu finden unter http://ec.europa.eu/commission_2010-2014/malmstrom/archive/COM%202010%20171%20EN.pdf.

11 Council Decision establishing the organisation and functioning of the European External Action Service, Brüssel 20. Juli 2010, zu finden unter http://register.consilium.europa.eu/pdf/en/10/st11/st11665-re01.en10.pdf.

12 Handelte es sich hierbei bisher um Delegationen der Kommission, sind diese seit Inkrafttreten des Lissabonner Vertrags EU-Delegationen, es handelt sich hier also nicht mehr um Vertretungen, die allein die Kommission repräsentieren und dieser zuarbeiten, sondern die gesamte EU wird nun durch sie vertreten.

13 Die Ergebnisse des Abschlussberichts "Freiheit, Sicherheit, Privat – Europäische Innenpolitik in einer offenen Welt" finden sich unter http://www.bmi.bund.de/cae/servlet/contentblob/128602/publicationFile/15773/European_home_affairs_executive_final_report_de.pdf, zuletzt angerufen am 6.9.2010.
Den Vorsitz der Zukunftsgruppe hatten der Vize-Präsident der Europäischen Kommission und der Innenminister der jeweils amtierenden Präsidentschaft inne. In ihr kamen ad personam die Innenminister der beiden aktuellen Triopräsident-

schaften (Deutschland, Portugal, Slowenien; Frankreich, Tschechische Republik, Schweden) sowie ein Vertreter des zukünftigen Präsidentschaftstrios, d.h. Spanien, Belgien und Ungarn, zusammen. Weitere Teilnehmer waren ein Beobachter für die Staaten mit Gewohnheitsrecht (Vereinigtes Königreich), der Vorsitzende des LIBE-Ausschusses des Europäischen Parlaments und ein Vertreter des Generalsekretariats des Rates.

14 Erweiterung und westlicher Balkan, Unterstützung der Kandidatenländer, Stabilisierung der Region, Europäische Nachbarschaftspolitik, Aktionspläne, Einbeziehung von Freiheit, Sicherheits- und Justizkomponenten, Strategische Partnerschaften: USA, Kanada, Russland, Brasilien, transatlantischer Dialog, vor allem auch Beziehungen mit Russland.

15 Dieses Statement hat die HV/VP vor dem Plenum am 7. Juli 2010 verlesen. Es ist zu finden unter http://www.europa-eu-un.org/articles/en/article_9910_en.htm, zuletzt abgerufen am 6.9.2010.

16 Im Dezember 2005 verabschiedete der Europäische Rat eine EU-Strategie zur Terrorismusbekämpfung sowie eine Strategie zur Bekämpfung von Radikalisierung und Rekrutierung. Abzurufen unter http://www.consilium.europa.eu/showPage.aspx?id=1195&lang=de.

17 Siehe zum Zusammenhang von ESVP-Missionen und dem RFSR auch Stockholmer Programm, S. 75.

18 Council of the European Union, Joint Statement on the Partnership for Modernisation EU-Russia Summit, 31 May-1 June 2010, Rostov-on-Don, 1 June 2010, zu finden unter http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/er/114747.pdf.

19 In der Erklärung wird vor allem die wirtschaftliche und technische Zusammenarbeit zwischen EU und Russland vereinbart. Zwar wird erwähnt, dass die Grundsätze der Rechtsstaatlichkeit beachtet werden sowie der Demokratiegrundsatz, aber Standards im Bereich Menschenrechte oder gemeinsame Mechanismen zur Bekämpfung Organisierter Kriminalität bleiben außen vor. Russlands großes Interesse an dem Abkommen hätte man nutzen können, um im Partnerschaftsabkommen eben solche Bereiche wie Menschenrechte und Förderung von Demokratie etc. aus einer besseren Verhandlungsposition heraus verhandeln zu können. Das PfM deckt einen Großteil der wirtschaftlichen Aspekte des PCA ab und lässt die übrigen Aspekte des PCA außen vor. Darüber soll sich dann im PCA geeinigt werden. Da es Russland aber auch beim PCA vor allem um den wirtschaftlichen Teil geht und dieser nur mit dem PfM gedeckt ist, kann es sein, dass eine Einigung über das PCA damit erstmal aufgeschoben ist.

20 Das SitCen (Joint Situation Center) wurde von Javier Solana als Zelle innerhalb der Policy Unit im Rat gegründet. Angestellte nationaler Nachrichtendienste und des EU-Militärstabes sammeln hier Informationen, die die Grundlage für die Erarbeitung politischer Analysen und Strategien der Policy Unit geben. Innerhalb des SitCens wurde 2002 eine nachrichtendienstliche Zelle eingerichtet, die sich aus Vertretern der Nachrichtendienste Deutschlands, Finnlands, Frankreichs, Großbritanniens, Italiens, der Niederlande, Polens, Sloweniens, Spaniens und Ungarns besteht. Das SitCen beschäftigt sich seit den Anschlägen von Madrid auch mit Terrorismusgefahr.

21 Vgl. Martin Grosse Hüttemann, Die Koordination der deutschen Europapolitik, in: APuZ 10/2007, S. 39-45, S. 42.

Transatlantic Counter-Terrorism Cooperation after Lisbon

Prof. Dr. Valsamis Mitsilegas

I. Introduction

EU-US counter-terrorism cooperation has been an area of EU external relations with substantial growth in the recent past. The political momentum for such cooperation was boosted post-9/11 and resulted in the conclusion of a number of international agreements between the European Union and the United States. Concluded primarily under the third pillar, these agreements have been subject to considerable criticism in Europe, both in terms of democracy and legitimacy and in terms of substance and the compatibility of their content with fundamental rights. These issues are now due to be reviewed following the entry into force of the Lisbon Treaty, which brings about a number of significant constitutional changes to the way the Union operates both internally and externally. This article is a contribution to the current discussion on the direction and content of future transatlantic counter-terrorism cooperation arrangements in the light of the entry into force of the Lisbon Treaty. I will begin by highlighting the key legal, constitutional, and political issues surrounding the existing EU-US counter-terrorism agreements; I will then outline the main changes brought about by the Lisbon Treaty that have the potential to influence transatlantic relations in the field of counter-terrorism and criminal matters more generally; and I will finish by putting forward a series of recommendations highlighting key issues to be taken into account in the future development of transatlantic cooperation against terrorism.

II. Transatlantic Counter-Terrorism Cooperation before Lisbon: The Legacy of 9/11 and the Third Pillar

Transatlantic counter-terrorism cooperation before Lisbon was exemplified by the conclusion of a series of agreements be-

tween the European Union and the United States covering a wide range of issues and triggered primarily by the events of 9/11. The first major step in this context was the conclusion of the EU-US agreements on extradition and mutual legal assistance.[1] Their signature marked an important constitutional precedent for the European Union, with the agreements being the first major international agreements concluded under the third pillar.[2] The agreements were the outcome of the political momentum generated post-9/11 at the EU level. This momentum resulted both in furthering European integration internally, via the adoption of a raft of EU legislation (the Framework Decisions on terrorism and the European Arrest Warrant being prime examples in this context), and in boosting the EU's position as a global actor in the field.[3] While these agreements reflected the Parties' political will to cooperate post-9/11, subsequent agreements were generated from the need to comply with US measures taken after the attacks. The first example concerns the agreements relating to the transfer, from airlines to the US Department of Homeland Security, of Passenger Name Records (PNR) of passengers flying from the EU to the US, which were necessitated in order to ensure that compliance of airlines with US law requiring such transfers did not breach EU law. Following the acceptance by the Commission of the adequacy of US data protection standards, transatlantic cooperation in this context began as a first pillar international agreement (between the Community and the US).[4] Following an ECJ ruling against the legality of the first pillar legal basis used,[5] the EC-US agreement was replaced by third pillar agreements between the EU and the US.[6] Last but not least, the publicity regarding the transfer to the US authorities of personal data contained in transactions processed by SWIFT[7] generated political pressure resulting in another third pillar agreement enabling the transfer of such data to the US authorities, signed one day before the entry into force of the Lisbon Treaty.[8] The signature of these agreements by the European Union has been met by strong objections and concerns on political, democratic, and human rights/rule-of-law grounds.

1. Political concerns

Increased cooperation with the US could be seen as welcome as a sign of the emergence of the EU as a global actor in criminal matters. From this perspective, the signature of agreements in criminal matters with the US was of great constitutional significance, as the agreements constituted precedents for external action under the third pillar and, at least for some, rendered academic the then contested issue of whether the Union had a legal personality.[9] However, the agenda of furthering European integration in the field of criminal matters has had to be promoted against the background of growing political concerns with regard to the extent and nature of transatlantic cooperation post-9/11. These concerns − which are of course inextricably linked with the content of transatlantic counter-terrorism cooperation − centered on the nature of the US response post-9/11 and the perceived willingness of the EU to uncritically adopt the US "war on terror" approach. In this context, it should be remembered that two of the major elements of transatlantic cooperation in the field of criminal matters, the PNR and the Terrorist Finance Tracking Programme (TFTP) Agreements, consist of an EU response to US unilateral post-9/11 demands and entail to a large extent the acceptance of the legality of US measures under EU law. In its willingness to emerge as a global actor in the field of counter-terrorism and criminal law in general, the European Union has demonstrated a willingness to accommodate to a great extent emergency measures developed outside the Union. As will be seen below, the compatibility of some of these heavily securitised measures with EU law (in particular privacy and data protection standards) has been contested. External action in the field of cooperation in criminal matters came at a juncture, where security was also being prioritised at the level of internal EU action, reflected in policy terms particularly in the Hague Programme, which focused to a great extent on the collection and exchange of a wide range of personal data for security purposes.[10]

2. Democratic concerns

Concerns with regard to the uncritical adoption of US standards by the EU have been compounded by the marked lack of democratic scrutiny and transparency in the negotiation and conclusion of the agreements. From a constitutional point of view, the fact that the agreements were ultimately negotiated under the third pillar meant that negotiations were formally led by the Presidency of the European Union and that the European Parliament did not have any role in the process of negotiation and signature**.** These constitutional constraints were combined with the negotiating practice of Member States (and at times the Commission), which effectively shielded the agreements from any kind of meaningful debate and scrutiny. The EU-US agreements remained classified until the very last weeks before signature, notwithstanding repeated requests for their publication for the purpose of scrutiny.[11] The Europol-US Agreement was not even published in the Official Journal.[12] The first version of the PNR Agreement (between the Community and the US) was transmitted to the European Parliament for examination under deadlines which, according to Parliament, did not enable it to conduct meaningful scrutiny − with the handling of scrutiny leading to Parliament challenging the agreement in the ECJ.[13] The TFTP Agreement was, as seen above, signed a day before the entry into force of the Lisbon Treaty − in an attempt to conclude it under the intergovern-

mental process of the "old" third pillar, thus pre-empting the Community elements brought about by Lisbon and effectively sidelining the European Parliament. Unsurprisingly, this handling led to the eventual rejection of the agreement by the Parliament after Lisbon.[14] The conclusion of these agreements, negotiated with minimal transparency in the face of sustained and growing fundamental rights concerns expressed by parliaments, EU expert bodies, and civil society,[15] was presented as a *fait accompli*, with signature dates set out in advance and limited time for debate and scrutiny.[16]

3. Substantive concerns – fundamental rights and the rule of law

A key fundamental rights concern in transatlantic counter-terrorism cooperation involves privacy.[17] The agreements on mutual legal assistance, PNR and TFTP, all provide for the transfer of a wide range of everyday personal data to a wide range of US authorities. The adverse consequences of such extensive information sharing for the right to privacy and data protection have been documented repeatedly and in detail. The conclusion of these agreements in such broad terms and with limited protection safeguards raises the question of whether, in its emergence as a global actor in criminal matters, the European Union has compromised its proclaimed internal standards and values. The human rights concerns stemming from the acceptance of a heavily securitised US agenda involving maximum collection of personal data are exacerbated in the light of the minimal rule-of-law safeguards secured by the EU in some of the agreements. The scope of information exchange agreements and the specification as to which US authorities will receive personal data have been drafted in such broad terms that the *foreseeability* and sure footing of the legislation leave much to be desired. Moreover, in particular in the PNR Agreement, safeguards secured by the EU side are not expressly legally binding but take the form of "letters" by the US executive.[18]

III. The Lisbon Treaty

The Lisbon Treaty introduces a number of changes with potentially far-reaching consequences for EU external action in general and transatlantic counter-terrorism cooperation in particular. They involve both changes in the internal constitutional architecture of the Union (such as, in principle, the abolition of the pillars), as well as changes in the provisions on the Union's external action. Underpinning these changes is the emphasis placed by the Lisbon Treaty on upholding the values of the Union and on protecting fundamental rights. As will be seen below, these changes can potentially address the shortcomings of the existing transatlantic cooperation analysed above.

1. Changes in the policy: European values in EU external relations

A key feature of the Lisbon Treaty is its emphasis on the values upon which the Union is deemed to be founded. These values are central not only to defining European identity internally but also to guiding the external action of the Union. Not surprisingly, respect for fundamental rights and the rule of law are expressly included in the list of EU values found in Art. 2 TEU. This enumeration of the values upon which the Union is founded is not merely declaratory. According to Art. 3(1) TEU, the promotion of these values is a key aim of the Union. The role of the Union in promoting its values is further highlighted with regard to EU external action, with Art. 3(5) TEU stating that "in its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens."

The centrality of the values of the Union, when the Union acts at the global level, is further confirmed by the specific Treaty provisions on external action. According to Art. 21(1) TEU, "the Union's action on the international scene shall be guided by the principles which have inspired its own creation, development and enlargement, and which it seeks to advance in the wider world," which include: democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms and respect for human dignity. According to Art. 21(2) TEU, the Union will define and pursue common policies and actions, and it will work towards a high degree of cooperation in all fields of international relations, in order to, *inter alia*, safeguard its values and consolidate and support democracy, the rule of law, human rights, and the principles of international law. Art. 205 TFEU reiterates that these provisions will guide the Union's action on the international scene. It is thus clear that the promotion of fundamental rights and the rule of law, forming key values of the Union, is a key element of EU external action after Lisbon.

2. Institutional changes – Addressing the democratic deficit?

The Lisbon Treaty introduces far-reaching institutional changes as regards the negotiation and conclusion of international agreements in criminal matters. These changes emanate from the abolition of the pillars in Lisbon and, in principle, the "communautarisation" of the third pillar. In this light, Art. 47 TEU expressly grants the Union legal personality. The negotiation and conclusion of international agreements in matters previously falling under the third pillar are now governed by the general provision of Art. 218 TFEU. A major development in this context is the enhanced role of the European Parlia-

ment. According to Art. 218(6)(v), the consent of the European Parliament in agreements covering fields to which the ordinary legislative procedure applies is required. This would cover the majority of areas falling under the TFEU Title on the Area of Freedom, Security and Justice (AFSJ). This change has the potential to address to a great extent the democratic concerns prevalent in the conclusion of the "previous" third pillar agreements, and the democratic debate and transparency in the development of EU external action in criminal matters will hopefully be enhanced. By its rejection of the third pillar TFTP Agreement, the European Parliament has shown that it intends to take its new powers seriously in practice. The rejection of this agreement − on institutional and human rights grounds − is a sign that the European Parliament will assume a central role in the negotiation and conclusion of international agreements in the field of counter-terrorism, with the Parliament being increasingly involved in the early stage of the negotiation of the mandate to these agreements.[19] This role is implied in Art. 218(10) TFEU, which states that the European Parliament must be informed immediately and fully at all stages of the procedure. It may also be regarded as a reflection of the duty of sincere mutual cooperation, which the Lisbon Treaty extends expressly to cover cooperation between the EU institutions.[20]

3. Substantive changes – Fundamental rights at the heart of the European project

The commitment to respect human rights lies at the heart of the Lisbon Treaty. Along with the central position of respect for fundamental rights in the list of the values of the Union, this commitment is clearly reflected in Art. 6 TEU. The sources of fundamental rights are manifold. The Union recognises the rights, freedoms, and principles set out in the Charter of Fundamental Rights, which will have the same legal value as the Lisbon Treaty.[21] Fundamental rights, as guaranteed by the European Court of Human Rights (ECHR) and as they result from the constitutional traditions common to the Member States, constitute general principles of the Union's law.[22]

The Treaty also calls for the Union's accession to the ECHR.[23] These provisions make respect for fundamental rights a key component of both EU internal and external action. The multiplicity of the sources of fundamental rights at the EU level (and, in particular, the express recognition of the legal value of the Charter) means that the content of these rights is both enhanced and expanded. This point is of particular relevance as regards fundamental rights that come into play in the context of transatlantic counter-terrorism cooperation, in particular the right to the protection of private life and the right to data protection, which is expressly recognised in the Charter.[24]

Another constitutional development which renders the protection of fundamental rights central to EU external action stems from the principle of consistency between EU external action and the other EU policies,[25] particularly when read in combination with the provisions on the EU as an Area of Freedom, Security and Justice. Respect for fundamental rights is a key element of the development of the Union into an "area of freedom, security and justice"[26] and the importance of fundamental rights in this context has also been emphasised in the Stockholm Programme.[27] The development of internal EU law in the field of cooperation in criminal matters must thus respect fundamental rights. The principle of consistency means that external action on AFSJ in general − and counter-terrorism in particular − must be consistent with internal standards in this field.

IV. Transatlantic Counter-Terrorism Cooperation after Lisbon

Where do the Lisbon changes leave us with regard to transatlantic counter-terrorism cooperation? A revised TFTP Agreement[28] has now obtained the consent of the European Parliament under the Lisbon framework.[29] However, this is not the end of the road with regard to the conclusion of international agreements in the field of cooperation in criminal matters. Along with negotiations on the conclusion of a new, post-Lisbon EU-US PNR Agreement,[30] the conclusion of the TFTP Agreement was accompanied by a commitment to negotiations on the conclusion of a horizontal EU-US Agreement on data protection in the field of criminal law.[31] In view of forthcoming negotiations on these agreements, and the possibility of transatlantic cooperation being extended to further areas in the future, Lisbon gives rise to a number of issues to be taken into account when shaping the principles and content of such cooperation from an EU perspective.

1. Political considerations – Upholding the values of the Union

As mentioned above, one of the key objections with regard to the conclusion of the third pillar EU-US agreements has been the perceived uncritical acquiescence of EU negotiators to heavily securitised US demands in the post-9/11 era. The time has come to rethink the acceptance of heavily securitised emergency measures in the EU legal order. The emergence of the European Union as a global actor with a strong voice under Lisbon requires the Union to uphold and promote its values, at the heart of which lie the respect for fundamental rights and the rule of law. The emphasis on the need to take fundamental rights and the rule of law seriously is already evident at the EU

level both internally (with the Stockholm Programme departing from the heavily securitised agenda of its Hague predecessor) and externally (with the ECJ ruling in *Kadi* linking the autonomy of the Union legal order with upholding fundamental rights and the rule of law[32]**).** Not compromising but rather upholding and promoting these values in the field of transatlantic counter-terrorism cooperation is a key task of EU negotiators in the post-Lisbon era. Promoting these values in this context is also crucial to projecting the identity of the Union in the world, as well as for enhancing the legitimacy of these agreements internally.

2. Institutional/democratic considerations

In the light of the potentially significant consequences of EU-US agreements in the field of counter-terrorism for fundamental rights, a clear case for their conclusion needs to be made to the European public. The democratic and legitimacy deficit underpinning the third pillar agreements needs to be addressed. As mentioned above, the Lisbon Treaty addresses the democratic deficit to some extent, by strengthening the role of the European Parliament in the negotiation and conclusion of agreements between the EU and the US. However, this does not appear to be the case with regard to agreements concluded between the US and EU bodies in the criminal justice field, such as Europol and Eurojust − the third pillar decisions delineating the rules applying to these bodies provide for specific rules on the conclusion of agreements with third countries with no real involvement of the European Parliament.[33] This deficit needs to be addressed after the entry into force of the Lisbon Treaty, in the amendment of the Europol and Eurojust decisions in line with the legal bases provided for in the Lisbon Treaty.[34] The strengthening of democratic controls over proposals for future transatlantic counter-terrorism agreements needs to be accompanied by an enhancement of transparency and the involvement of civil society. Transparency can take the form of consultation regarding the need for such agreements and − notwithstanding the limits with regard to divulging details on negotiations − information as regards their progress and general direction. Key players in enhancing both the democratic debate and transparency in this context are national parliaments, which have been granted an enhanced scrutiny role under the Lisbon Treaty.[35]

3. Substantive considerations

As argued throughout this article, after Lisbon, EU external action in general and in criminal matters in particular must be guided by the values the Union proclaims to uphold and promote, including respect for fundamental rights and the rule of law. In the negotiation of future agreements on transatlantic counter-terrorism cooperation, the protection and promotion of the rights to private and family life as well as data is of particular importance. In this context, and in the light of the precedents of transatlantic counter-terrorism cooperation that are highly invasive to private life, two separate – but interrelated − questions need to be thoroughly examined: what kind of, and how much, personal information is necessary to be collected and transferred to the US for the specific purposes of the agreements negotiated? And, at a second stage, once there is agreement on the types and volume of data to be collected and transferred, are the privacy safeguards offered by the US compatible with EU values and standards? The proposed EU-US horizontal agreement on data protection may serve as a good starting point in addressing both questions as regards the conclusion of future agreements on transatlantic counter-terrorism cooperation (including agreements concluded by Europol and Eurojust) but also as regards the functioning of looser structures of operational cooperation between the EU and the US (such as the exchange of liaison officers). As regards upholding the rule of law, the EU-US data protection agreement may contribute towards the establishment of clear, legally binding standards on privacy protection and remedies for the affected individuals.

Upholding the values of the Union in the context of the collection and analysis of personal data for counter-terrorism purposes should also be a guiding principle for the development of internal Union law in the field of cooperation in criminal matters. In a number of instances, the US approach – as seen above, heavily criticised in the context of EU-US cooperation − is in the process of being adopted by the EU legal order. The adoption of similar measures at the EU level has been justified on the grounds of facilitating transatlantic cooperation, on the one hand by adding EU safeguards and on the other by ensuring reciprocity. In this light, the recently signed TFTP Agreement states that, during its course, the Commission will carry out a study into the possible introduction of an equivalent EU system allowing for a more targeted transfer of data.[36] In the field of PNR, and notwithstanding the sustained concerns with regard to the compatibility of the EU-US PNR Agreements with EU privacy and data protection law, the Commission tabled a proposal in 2008 for a Framework Decision with a similar system of transmission of PNR data by carriers flying *into* the EU.[37] The Commission justified the proposal as a result of "policy learning" from the existing PNR Agreements with the US and Canada and a new, "lisbonised" proposal is expected to be tabled in the near future.[38] While these proposals may be of use in setting EU standards, which can form benchmarks for subsequent EU negotiations with the US and globally,[39] their necessity and compatibility with fundamental rights must be fully justified before they are adopted at the EU level. The

prospect of the EU importing heavily securitised law and policy with far-reaching privacy consequences is real.

V. Conclusion – Lisbon as an Opportunity for Change?

The legacy of the third pillar with regard to transatlantic counter-terrorism cooperation leaves much to be desired with regard to upholding fundamental rights and the rule of law in EU external action. The Lisbon Treaty has brought about a number of changes with a potentially profound impact on the EU as a global actor in the field of cooperation in criminal matters: it addresses the democratic deficits caused by the abolition of the third pillar and the greater involvement of the European Parliament in transatlantic counter-terrorism cooperation; it emphasises respect for fundamental rights as lying at the heart of the European project; and it focuses on the values of the Union and the duty to uphold and promote them in EU external action. In the light of these changes, Lisbon must be viewed as an opportunity to put the dialogue on transatlantic counter-terrorism cooperation in a different perspective. With the momentum for further agreements between the EU and the US in the field of cooperation in criminal matters growing, now is the time for the European Union to reframe a heavily securitised agenda and emerge as a strong global actor upholding fundamental rights and the rule of law.

Prof. Dr. Valsamis Mitsilegas
Professor of European Criminal Law,
School of Law, Queen Mary, University of London

1 Agreement on extradition between the European Union and the United States of America, O.J. L181, 19 July 2003, p. 27; Agreement on mutual legal assistance between the European Union and the United States of America, O.J. L 181, 19 July 2003, p. 34. See also the Council Decision, on the basis of Arts. 24 and 38 TEU, concerning the signature of these agreements: O.J. L 181, 19 July 2003, p. 25.
2 See *V. Mitsilegas*, The New EU-US Co-operation on Extradition, Mutual Legal Assistance and the Exchange of Police Data, in: 2003 *European Foreign Affairs Review* 8, pp. 515-536. See also the parallel negotiation and later signature of an agreement between Europol and the US on the exchange of personal data (doc. 13689/02 Europol 82, 4 November 2002) – for details, see Mitsilegas *op. cit.*
3 See *V. Mitsilegas*, *op. cit.* (fn. 2).
4 Commission Decision on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, O.J. L 235, 6 July 2004, p. 11 (including an Annex with the relevant US Undertakings); and Council Decision on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the US Department of Homeland Security, Bureau of Customs and Border Protection, O.J. L 183, 20 May 2004, p. 83 (the Agreement is annexed to the Decision).
5 Joined cases C-317/04 and C-318/04, *European Parliament v Council*, [2006] ECR I-4721.
6 An interim agreement to address the legal vacuum resulting from the Court's ruling in 2006 was followed by another agreement in 2007: Council Decision 2006/729/CFSP/JHA on the signing, on behalf of the European Union, of an Agreement between the European Union and the USA on the processing and transfer of PNR data by air carriers to the US Department of Homeland Security (L 298, 27 October 2006, p. 27 – the text of the Agreement is annexed to this Decision); and the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), O.J. L 204, 4 August 2007, p. 18. See also Council Decision approving the signing of the Agreement on the basis of Arts. 24 and 38 TEU, p. 16.
7 For further information, see *G. González Fuster/P. de Hert/S. Gutwirth*, SWIFT and the Vulnerability of Transatlantic Data Transfers, in: 2008 *International Review of Law, Computers and Technology* 22, pp. 191-202.
8 Council Decision 2010/16/CFSP/JHA of 30 November 2009 on the signing, on behalf of the European Union, of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, O.J. L 8, 13 January 2010, p. 9 (and p. 11 for the text of the Agreement).
9 For an overview of the debate with regard to the existence and extent of the EU legal personality in the context of the third pillar, see *J. Monar*, The EU as an International Actor in the Domain of Justice and Home Affairs, in: 2004 *European Foreign Affairs Review* 9, pp. 395-415.
10 O.J. C 53, 3 March 2005, p. 1.
11 See House of Lords European Union Committee, *EU-US Agreements on Extradition and Mutual Legal Assistance*, 38th Report, session 2002-03, HL Paper 135.
12 For an overview of the limited scrutiny of this agreement, see *Mitsilegas, op. cit.* (fn. 2).
13 *V. Mitsilegas,* Border Security in the European Union. Towards Centralised Controls and Maximum Surveillance, in: E. Guild/H. Toner/A. Baldaccini (eds.), *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, Hart Publishing, 2007, pp. 359-394. Of course, the Court's ruling resulted in the agreements being negotiated under the third pillar with the Parliament having a much more limited scrutiny role.
14 See *J. Monar*, The Rejection of the EU-US SWIFT Interim Agreement by the European Parliament: A Historic Vote and its Implications, in: 2010 *European Foreign Affairs Review* 15, pp. 143-151.
15 On the extradition/mutual legal assistance agreements and the Europol/US agreement, see *Mitsilegas*, *op. cit.* (fn. 2); on the PNR Agreements, see *V. Mitsilegas,* The External Dimension of EU Action in Criminal Matters, in: 2007 *European Foreign Affairs Review* 12, pp. 457-497; on SWIFT, see the Opinion of the European Data Protection Supervisor of 25 January 2010 and the Opinion of the Art. 29 Working Party of 22 January 2010.
16 A number of the Agreements envisaged an *ex post* scrutiny at the national level, with their conclusion being subject to Member States' internal constitutional procedures. While the EU-US agreements on extradition and mutual legal assistance were signed in 2003, their conclusion on behalf of the EU took place only on 2009 – see Council Decision 2009/820/CFSP, O.J. L 291, 7 November 2009, p. 40.
17 Another concern is the death penalty-extradition agreement – *Mitsilegas, op. cit.* (fn. 2).
18 The text of the PNR Agreement does not include details of the PNR data transfer per se. They are set out in a separate accompanying "US letter to the EU," signed by the former Homeland Security Secretary *Michael Chertoff.* The letter is, in turn, followed by an "EU letter to the US" confirming that, on the basis of the assurances provided in the US letter, the EU deems that the US ensure an adequate level of data protection and that, based on this finding, "the EU will take all the necessary steps to discourage international organisations or third countries from interfering with any transfers of EU PNR data to the United States" – p. 25.
19 On the potential role of the European Parliament in shaping policy in the negotiation of international agreements post-Lisbon, see *R. Passos*, Mixed Agreements from the Perspective of the European Parliament, in: *Ch. Hillion/P. Koutrakos* (eds.), *Mixed Agreements Revisited*, Hart, 2010, pp. 269-294.
20 Art. 13(2) TFEU.
21 Art. 6(1) TEU.
22 Art. 6(3) TEU.

23 Art. 6(2) TEU.
24 See Art. 7 of the Charter on the right to private and family life and Art. 8 on the right to data protection. See also Art. 47 for the right to an effective remedy. Moreover, Art. 16 TFEU affirms the special place of data protection in the Lisbon Treaty.
25 Art. 21(3) TEU, §2.
26 Art. 67(1) TFEU.
27 O.J. C 115, 4 May 2010, p. 1.
28 Council doc. 11222/1/10 REV 1, Brussels, 24 June 2010.
29 European Parliament legislative resolution of 8 July 2010 on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, P7_TA(2010)0279.
30 The Commission's Action Plan to Implement the Stockholm Programme (COM(2010) 171) envisages the tabling of proposals for authorising the negotiation of PNR agreements with relevant third countries (p. 21). For more recent developments, see European Voice, *Commission to seek new data sharing mandates*, 2 September 2010, p. 6.
31 See EP Resolution above, point 4.
32 Joined Cases C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council and Commission* [2008] ECR I-6351. On the link between guaranteeing the autonomy of the Union legal order in the emergence of the Union as a global actor in criminal matters and upholding fundamental rights and the rule of law, see *V. Mitsilegas*, The European Union and the Globalisation of Criminal Law, in: 2009-2010 *Cambridge Yearbook of European Legal Studies* 12, forthcoming.
33 On Europol, see Council Decision 2009/371/JHA establishing the European Police Office (Europol), O.J. L 121, 15 May 2009, p. 37, Art. 23. The European Parliament can merely request the Presidency of the Council, the Chairperson of the Europol Management Board, and the Director of Europol to appear before it to "discuss matters relating to Europol" – Art. 48. On Eurojust, see new Art. 26a inserted by Council Decision 2009/426/JHA "on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime," O.J. L 138, 4 June 2009, p. 14. The original 2002 Decision (O.J. L 63, 6 March 2002, p. 1) provides mainly for the European Parliament to be informed about the work of Eurojust via the submission of written reports (Art. 32). For details, see *V. Mitsilegas*, The Third Wave of Third Pillar Law: Which Direction for EU Criminal Justice? in: 2009 *European Law Review* 34, pp. 523-560.
34 See Art. 85 TFEU for Eurojust and Art. 88 TFEU for Europol.
35 See, in particular, Art. 12 TEU.
36 Art. 11.
37 *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for Law Enforcement Purposes*, COM (2007) 654 final, Brussels, 6 November 2007.
38 The Commission's Action Plan to Implement the Stockholm Programme (COM(2010) 171) envisages a legislative proposal on a common EU approach to the use of PNR data for law enforcement purposes, to be tabled in 2010 – p. 29.
39 See European Voice, *op. cit.* (fn. 30).

The Global Challenge of Cloud Computing and EU Law

Laviero Buono*

I. Introduction

In the world of information and communication technologies (ICTs), the phenomenon of cloud computing is almost inescapable these days,[1] and it seems to indicate the direction in which information infrastructures are moving. The concept, relatively simple, implies the migration of computing hardware, software infrastructures, and applications to third-party service providers' data centres which, to end users, appear to exist somewhere "in the clouds" of cyberspace. Cloud computing is therefore a new way of delivering computing resources and services, a new segment of the overall ICT portfolio, rather than a new technology per se.[2] The advantages of such a business model are readily identifiable and result in considerable cost savings (companies do not have to invest in new infrastructures, thereby reducing capital expenditure on hardware, software, licensing, and other services), location independence (users can access systems from anywhere, regardless of their location), multi-tenancy benefits (sharing of resources and costs among a large pool of users), low barriers to entry, and immediate access to a broad range of applications. Moreover, organisations using cloud models can take advantage of the best and latest technology without any upgrade of internal ICT infrastructures. Forward-thinking companies launched their business experiments based on cloud computing, and it is foreseen that massive investment will take place on a global scale in the coming years.[3] However, the many benefits of cloud computing may be offset by certain technical risks and legal concerns linked, *in primis*, to security privacy and the protection of confidential data. How best to ensure that personal information stored in data centres, in cyberspace, is properly managed and controlled by the host in order to avoid the leakage or manipulation of sensitive data?

Jurisdictional issues are another major area of legal difficulty in the domain of cloud computing. How should the jurisdiction that is necessary to initiate a criminal investigation of cloud computing-related offences be established when cyberspace

is, by definition, transnational and borderless in nature? Is the "territoriality principle" applicable? To this extent, there is little doubt that traditional jurisdictional concepts, such as *lex loci delicti commissi* and the principle of the "natural" judge, are seriously challenged here.

At the European Union (EU) level, the adoption of the multi-annual Stockholm Programme,[4] providing the overall policy agenda for 2010–2014 in the area of freedom, security and justice in the EU, as well as the entry into force of the Treaty of Lisbon[5] on 1 December 2009 have substantially enhanced the EU's mandate with regard to the fight against cybercrime. Art. 83 of the Treaty on the Functioning of the European Union (TFEU) enables the Union to establish minimum rules concerning the definition of criminal offences and sanctions in relation to serious crime with a cross-border dimension. Art. 83, paragraph 1 of the TFEU lists, *inter alia*, computer crime among the serious crimes. This means that the Union can adopt legally binding acts in this field of law in the near future if they are deemed appropriate.[6]

This paper will first look at the cloud computing phenomenon, framing the concept and shedding light on the most relevant pros and cons. It will then discuss the main legal implications of cloud computing with a particular focus on data protection and criminal jurisdictional issues, leaving aside other problems that may be associated with security "in the clouds"[7] and the most recent debate on the environmental impact of cloud computing (also known as *green computing*).[8] Finally, it will assess the preparedness of EU legislation to address these legal issues *rebus sic stantibus* and in light of the entry into force of the Lisbon Treaty.

II. Cloud Computing: The Phenomenon

Every day, thousands of Internet users engage in cloud computing activities without even realising it. In order to save a text file on the Google Docs website, to maintain an album of photos on Flickr, to store some profile photos on Facebook, to upload videos on YouTube, to use the email services of Yahoo!, and to blog and post comments from everywhere in the world using Blogger and Twitter − just to mention some of the most popular worldwide websites − requires the transmission of data and applications in cyberspace. Users no longer need to store photos and documents in traditional physical paper albums, CDs, mobile phones, or notebooks; these data can reside "in the clouds," and users can access them online through any web-connected device when and how they want. "In the clouds" is, of course, a metaphor to describe the worldwide platforms and data centres that host such data and applications, making them available on demand. A CNN report of 4 November 2009 entitled: "A trip into the secret, online cloud"[9] showed how, in cloud computing environments, *de facto*, data still remains in someone's building rather than in fluffy clouds. The author of the report visited an IBM cloud computing centre in California and reported that it was "nearly the size of a football field. It is in a metal building, part of an office complex. Inside, rows of black, refrigerator-sized computer towers, 4.000 of them in all". The conclusion can be reached that: "The cloud is an energy-sucking and fallible machine."[10] However, many international companies, like Amazon, Google, and Microsoft, do not only have one cloud computing centre but dozens of them located in every corner of the globe (often kept hidden for security reasons). Customers and clients can total millions.[11] In such a miasma of cloud platforms, where geography loses all meaning and where information flows ignore boundaries and time zones, it is difficult to be sure that personal data are adequately protected.

Turning now from the individual Internet user who, often unwittingly, avails himself of cloud computing to stay in contact with friends on Facebook or to upload photos and videos on Flickr, MySpace, and YouTube, to the multinational corporations that, in the wake of the economic downturn, consciously entered cloud platforms to reduce the impact of falling sales, revenues, and profit margins, one notices that, over the past months, cloud computing has gained significant momentum. A recent survey conducted by the Computer Associates[12] (CA) in February 2010, with the intent to better understand the perspective of European enterprises on cloud computing, showed that interest in cloud platforms grows dramatically as company size grows. 63% of companies with between 1000 and 3000 employees have little interest in cloud computing, with that number dropping to 43% for businesses with over 3000 employees.[13] One of the most publicised success stories for cloud computing concerns the New York Times case.[14] The idea was to make the 1922–1951 New York Times archive available online. This required plenty of computer capacity that was not available in-house. As a result, capacity was outsourced to Amazon. By so doing, the New York Times achieved significant additional cost savings that could be converted into investment in internal capacity expansion.

Why are legal issues inextricably linked to cloud computing? Cloud platforms collect tremendous amounts of sensitive data and personal information. The countries in which they operate may address privacy and security issues in very different ways. At a macroscopic level (which means at the level of business and governments, rather than that of young social networks users), the risks of inappropriate disclosure, exploitation, unfair appropriation, or misuse of information are potential threats to the companies' competitiveness or reputation, or even to the sovereignty of the State if national governments decide to

store information on cloud platforms.[15] Business are generally very reluctant to enable direct competitors to have access to their commercially sensitive data, such as customer contact lists, detailed sales data, and know-how.

III. Legal Implications of Cloud Computing

Transnational data flows trigger legal obligations in different jurisdictions. These legal questions are only just beginning to emerge, but they could develop into major points of contention in the near future. The sharing and transfer of data "in the clouds" is a crucial issue that gives rise to legal problems. In many cases, it is difficult for the cloud customer to check the data handling practices of the cloud provider and to be sure that the data are processed in a lawful way. Some countries have comprehensive and strong data protection frameworks and, in the absence of specific compliance mechanisms, they are reluctant to (or in some cases even prohibit) transfer personal data to countries where data protection standards are considerably lower.[16]

Since location is irrelevant in cloud computing, in cases of dispute, complex legal jurisdictional issues arise. In fact, illegal access followed by illegal use of data or the manipulation of or interference with data flows can potentially lead to the commission of a number of (cyber)crimes related to identity theft, unauthorized access for the purpose of sabotage, intellectual property violations, online fraud, and other forms of crime. To this extent, one of the crucial challenges to which cloud computing gives rise is the question of how to resolve jurisdictional issues as a result of irregular online conduct that produces legal effects in multiple jurisdictions. If more than one State asserts jurisdiction, a dispute or even a conflict may occur among the States involved. It is therefore difficult to identify the authorities and the courts that are competent to launch an investigation, prosecute, and eventually adjudicate the case. For such criminal acts, committed through the extended use of ICT facilities, the different elements of the criminal plan may affect not one but various countries.

The discussion on cybercrime and Internet jurisdiction is an ongoing legal issue in public international law, particularly within the Council of Europe.[17] Arrangements for the settlement of jurisdictional conflicts, *ne bis in idem*, and the transfer of proceedings are also dealt with within the EU (see *infra* part 5).

IV. Brief Overview of EU Policy on Cybercrime

For the past decade, the EU has worked on different legal measures in the field of cybercrime. Already in 2000, in order to ensure that the targets set by the Lisbon European Council[18] would be reached by defining the necessary measures, the Council of the European Union and the Commission prepared the "*e*Europe Action Plan,"[19] which included actions to enhance network security and the establishment of a coordinated and coherent approach to cybercrime. In January 2001, the first Communication on cybercrime entitled: "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating computer-related crimes"[20] was published.

Moreover, in the former so-called "third pillar," the Union tried to approximate the laws and regulations of the Member States in the field of cybercrime with different framework decisions, notably the 2001 Framework Decision on combating fraud and counterfeiting of non-cash means of payment,[21] the 2002 Framework Decision on combating terrorism,[22] the 2003 Framework Decision on combating the sexual exploitation of children and child pornography,[23] and the 2005 Framework Decision on attacks against information systems.[24] In late 2008, the Justice and Home Affairs Council discussed cybercrime again in the context of European cooperation on internal security. It adopted conclusions on setting up national alert platforms and a European alert platform for reporting offences detected on the Internet as well as conclusions on promoting closer operational cooperation among the law enforcement authorities of the Member States.[25] On the wave of these Council conclusions, in January 2010, the Spanish presidency proposed an action plan for a concerted strategy to combat cybercrime,[26] calling upon the Member States to consider and discuss the next steps to be taken, examining which of the alternatives proposed best define the general guidelines that will serve as a basis for implementing the Union's anti-cybercrime strategy.

Recently, the 3010th General Affair Council meeting,[27] held in Luxembourg on 26 April 2010, adopted new Conclusions on the implementation of a concerted strategy to combat cybercrime. The Conclusions included short and medium term actions to be taken in order to specify how the main points of the strategy should be implemented.[28]

Finally, specific reference to the fight against cybercrime is made in the third multi-annual Programme in the area of freedom, security and justice, known as the Stockholm Programme,[29] which was endorsed by the European Council in December 2009.[30] Special attention to the fight against cybercrime is also evident in the the trio (Spanish, Belgian and Hungarian) presidency's Justice and Home Affairs programme for 2010–2011, presented in January 2010.[31]

Aside from developments in the legislative process, the EU in 2004 endeavoured to strengthen cyber-security by launching

an *ad hoc* agency, ENISA (the European Network and Information Security Agency),[32] with the aim of enhancing information exchange and cooperation on network and information security as well as stimulating cooperation between the public and private sectors, thereby ultimately providing assistance to the Commission and the Member States.[33] The entry into force of the Lisbon Treaty[34] on 1 December 2009 provides for a solid mandate for the EU with regard to computer crimes, listed among crimes with a cross-border dimension.[35]

V. Cloud Computing and EU Law

1. Data protection issues

The preceding sections highlighted two main legal aspects related to cloud computing: data protection and jurisdictional issues. Is European Union legislation adequate to face the potential challenges presented? The protection of personal data in the European Union is laid down in Art. 8 of the Charter of Fundamental Rights of the European Union[36] and is further detailed in three main legal instruments: the 95/46/EC Data Protection Directive,[37] the 2002/58/EC Directive on privacy and electronic communications,[38] and, within the framework of the former "third pillar," the 2008 Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (to be implemented by November 2010).[39] With the entry into force of the Treaty of Lisbon, the legal basis for secondary legislation to ensure the protection of personal data in the Union has now been laid down in Art. 16, paragraph 2, which provides that the European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure,

> lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.[40]

For the purpose of cloud computing, the key principle in the 95/46/EC Data Protection Directive is contained in Chapter IV on "Transfer of personal data to third countries". In particular, Art. 25, paragraph 1, states that:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.[41]

This means that a company that does its processing "in the clouds" may be violating EU law if data are processed (this might include operations, such as recording, storage, use, disclosure by transmission, erasure, or destruction, etc.) in servers located in third countries that do not meet the Union's adequacy standards for data protection.

In 2000, in order to bridge the different data protection approaches and provide a streamlined means for American companies to comply with EU law, the US Department of Commerce, in consultation with the European Commission, developed the "Safe Harbour" framework.[42] On 26 July 2000, the Commission adopted Decision 520/2000/EC[43] recognising that the Safe Harbour respected international privacy principles. Since 2000, the overall operation of the Safe Harbour has been periodically monitored by the European Commission through staff working papers,[44] which provided assessments on the functioning of the agreement. However, the Safe Harbour certification allows data transfer exclusively from the EU to the United States but not from the EU to other countries. As a result, cloud computing often circumvents the scope of such a framework.

For the transfer of personal data to third countries outside the United States, a different scheme is offered to multinational companies to meet their legal obligations and ensure a proper level of protection of personal information: the so-called Binding Corporate Rules (BCRs). The Art. 29 Data Protection Working Party,[45] in its documents WP74[46] and WP108,[47] provided guidance on the necessary content of BCRs. Moreover, to improve the communication on BCRs and to allow companies concerned with international data transfers to receive more precise information on the structures of the BCRs, the Art. 29 Working Party has developed a toolbox designed both for companies and for data protection authorities, which is composed of Frequently Asked Questions and a checklist.[48] The aim of the toolbox is to provide operational answers to concrete questions regarding the international transfer of data.

Recently, on 15 May 2010, a new set of European Union standard contract clauses for processing European personal data abroad, known as "model contracts," came into effect by means of the Commission Decision of 5 February 2010,[49] which repealed Decision 2002/16/EC.[50] The latter was originally adopted in order to facilitate the transfer of personal data from a data controller in the EU to a processor in a third country but, unfortunately, without an adequate level of protection. Regarding cloud computing, a major change from the 2002 model contracts is that, with the new Decision, the data importer may not disclose the personal data to a third party without the prior written consent of the data exporter. In this context, however, it is also crucial to establish the obligations of "controllers" and "processors," which is not always clear in cloud computing services.[51] In a recent paper entitled "Data Protection and Cloud Computing under EU law," presented at the

Third European Security Awareness Day on 13 April 2010, the European Data Protection Supervisor, *Peter Hustinx*, stressed that, in many cases, cloud providers are data processors. However, when they determine not only the means but also the purpose of the processing, they are also data controllers.[52] Besides the unclear role played by cloud providers, in his paper Mr. *Hustinx* also emphasised other challenges like, *inter alia*, the applicability of EU law in cloud computing and how to monitor the processing of data for purely personal purposes. In his view, in relation to the proposed updating of the Data Protection Directive, four areas may require amendments: applicable law, international data transfers, accountability, "privacy by design," and the need to impose "processor" obligations where services are provided to individuals acting in a purely personal capacity.[53]

2. Criminal jurisdictional issues

Where online and Internet-related crimes are committed as a result of transnational data flows, numerous jurisdictional scenarios can arise. The *lex loci delicti commissi* principle requires that, in order to apply the territoriality principle, it is necessary to establish the place where the crime has been committed, and this is not always evident or is subject to plural interpretation. Where the locus delicti is uncertain (this is very frequent in cloud computing), there is a major risk that more than one country can assert jurisdiction. Moreover, even if the place where the crime has been committed is precisely determined, this often does not coincide with the place where perpetrators are physically located.

In order to increase efficiency in criminal proceedings and improve the proper administration of justice in an area of freedom, security and justice, the EU has put in place instruments that contribute to mitigating the legal uncertainty. Such instruments are, *inter alia*, the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union,[54] the 2009 Council Framework Decision on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings,[55] and the 2009 proposal for a Council Framework Decision on transfer of proceedings in criminal matters presented by a group of 16 Member States.[56] Aside from these legal instruments, the EU agency Eurojust stimulates and improves the coordination of investigations and prosecutions between competent authorities of the Member States. Under Art. 6, paragraph 2 of the new Eurojust Council Decision,[57] the agency is now entitled to put forth a non-binding opinion on how a jurisdictional conflict between two or more EU Member States should be settled. If a Member State does not accept this opinion, it must explain and reason its argument.

The aim of these legal instruments, however, is to contribute to the fight against cross-border crime (including cybercrime) and to create a common solution exclusively for the 27 Member States of the EU. But what about specific jurisdictional cybercrime conflicts or disputes over concurring jurisdictional claims involving countries outside the EU? In this regard, the central piece of legislation remains the 2001 Council of Europe Convention on Cybercrime,[58] which, in Art. 22, specifies the criteria under which the contracting States are obliged to assert jurisdiction over criminal offences as provided in Arts. 2 to 11 of the Convention.[59]

VI. Concluding Remarks

Cloud computing is a phenomenon still in its infancy, but it represents an impressive shift away from the "traditional" methods of delivering ICT services. Consistent investment will take place worldwide in the coming years, and the legal impact of the cloud computing models needs to be carefully scrutinised. Framing legal relations "in the clouds" may prove to be a labour of Sisyphus, since the transborder and instantaneous flows of data makes cloud computing a constant "moving target." From among the range of different legal issues, this paper focused on the safeguarding of data protection and jurisdictional aspects of cloud computing within the context of existing EU legislation. Regarding data protection, the paper showed that, besides the comprehensiveness of the EU's data protection framework, *ad hoc* legal instruments also exist, such as the Safe Harbour Certification, the Binding Corporate Rules (BCRs), and the new set of EU standard contract clauses (SCCs or "model contracts"). However, the role played by cloud providers is not always clear. The distinction between "controller" and "processor" becomes blurred. Moreover, it is not always easy to determine whether EU law applies. In fact, this is subject to precise conditions (such as the establishment of the cloud provider in the EU) and might not cover a range of services.[60] Since the Data Protection Directive is in the process of being reviewed and modernised in response to the latest technological developments,[61] these *lacunae* can hopefully be filled, thus enabling the Union's legal framework to be better equipped to deal with the challenges brought about by cloud computing.

As ICTs have developed, so have criminal offences associated with their use. As a result of the migration of personal data in cyberspace, new methods of perpetrating crimes have developed. National criminal codes were not written with the language of the Internet in mind. In this regard, ICT has a universal, technically harmonised, standard language. Legislators and regulators are trying hard to keep pace. Even relatively modern legal instruments, such as the Council of Europe Con-

vention on Cybercrime, do not address phenomena, such as "skimming," "phishing," or "cloud computing," since such phenomena were not as relevant in 2001 as they are today. Despite the legal instruments that are in place at the EU level, as referred to in this paper, jurisdictional issues remain unclear in cases of disputes over information technology crimes. The ubiquity of cloud computing undermines legal certainty as regards the *locus delicti* and other traditional principles of jurisdiction. This can lead to a multiplication of assertions of jurisdiction with the consequent involvement of not one but a range of States. At any rate, due to their nature, cybercrime jurisdictional issues cannot be addressed solely within the EU but must be addressed at the international level. In this regard, the insertion of "computer crimes" in the list of serious crimes with a cross-border dimension by means of Art. 83 of the TFEU provides a much needed opportunity to reflect on the main challenges in the fight against cybercrime and on how the EU intends to address these challenges in the future.

Laviero Buono

Head of Section for European Public and Criminal Law, Academy of European Law (ERA)

* All comments and views expressed in this article are those of the author only.

1 The 5th Internet Governance Forum (IGF) 14-17 September 2010 in Vilnius, Lithuania, continuing from the Sharm El Sheikh IGF of November 2009, has devoted an entire workshop to the topic: "Emerging issue: Cloud Computing". More information can be found at: http://www.intgovforum.org/cms/.

2 See the European Network and Information Security Agency report of November 2009: Cloud Computing – benefits, risks and recommendations for information security, p. 4. Available at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

3 According to the International Data Corporation's (IDC) analysis "Western European Software-as-a-Service Forecast 2009-2013", April 2009 (Doc # LT02R9, 2009), $44.2 billion will be invested in cloud computing worldwide by 2013, with the European market ranging from €971 million in 2008 to € 6,005 million in 2013.

4 The Stockholm Programme − An open and secure Europe serving and protecting the citizens. Presidency Conclusions − Brussels, 10-11 December 2009 (Council of the European Union, Brussels, 3 March 2010, 5731/10).

5 For the consolidated versions of the Treaty on European Union and of the Treaty on the Functioning of the European Union, together with the annexes and protocols thereto, incorporating the amendments introduced by the Treaty of Lisbon, see O.J. C 83, 30 March 2010, p. 1.

6 On this point, see *M. Gercke*: Impact of the Lisbon Treaty on Fighting Cybercrime in the EU – the redefined role of the EU and the change in approach from patchwork to comprehensiveness, 2010 *Computer Law Review International* 3, pp. 75-80.

7 In 2000, in response to certain legal aspects of information society services and, *inter alia*, on the liability of Internet Service Providers (ISPs), the European Union adopted Directive/2003/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (e-commerce Directive), (O.J. L 178, 17 July 2000, p. 1).

8 The Organisation for Economic Cooperation and Development (OECD) is analysing the emerging impact of cloud computing and related policy implications as well as its environmental benefits, such as energy efficiency and energy use. A policy recommendation on ICTs, the environment, and climate change was issued in 2010. Available at: http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=259&InstrumentPID=259&Lang=en.

9 Watch the entire CNN video here: http://edition.cnn.com/2009/TECH/11/04/cloud.computing.hunt/index.html.

10 *J. Sutter*: A trip into the secret, online 'cloud'. CNN report of 4 November 2009. Available at: http://edition.cnn.com/2009/TECH/11/04/cloud.computing.hunt/index.html.

11 According to the Google Apps official website, more than two million businesses run Google Apps with thousands more signing up every day. Source: http://www.google.com/apps/intl/en/business/index.html (*last visited: 10 July 2010*).

12 An independent private IT management software company.

13 Computer Associates (CA) Survey: Unleashing the Power of Virtualization 2010 – Cloud Computing and the Perceptions of European Business, February 2010, p. 5. Available at: www.ca.com/mediaresourcecentre.

14 For an illustration of this and other cloud computing cases, see *G. Petri:* Shedding light on Cloud Computing. Computer Associates (CA), January 2010, p. 5. Available at: http://www.ca.com/files/whitepapers/mpe_cloud_primer_0110_226890.pdf.

15 To this extent, see *C. Arthur,* Government to set up own cloud computing system. *The Guardian*, 27 January 2010. On the British Government strategy to create an internal cloud computing system as a plan that it claims could save up to £3.2 billion a year on an annual bill of at least £16 billion. Available at: http://www.guardian.co.uk/technology/2010/jan/27/cloud-computing-government-uk.

16 Under certain circumstances, prohibition of transfer of personal data is explicitly provided for in the EU Data Protection Directive, see *infra* part 5.

17 On this point, see the (draft) discussion paper of *H. Kaspersen,* Cybercrime and Internet jurisdiction. Council of Europe, Project on Cybercrime, version 5 March 2009. Available at: http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2009)%20draft%20discussion%20paper%20Cybercrime%20and%20jurisdiction.pdf.

18 The Lisbon Special European Council, Lisbon, 23-24 March 2000: Towards a Europe of Innovation and Knowledge. Available at: www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/00100-r1.en0.htm.

19 Action Plan: *e*Europe − An Information Society for all, Brussels, 14 June 2000. Available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/2002/action_plan/actionplan_en.pdf.

20 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions − Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crimes (COM(2000) 890 final).

21 Council Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment (O.J. L 149, 2 June 2001, p. 1).

22 Council Framework Decision 2002/475/JHA on combating terrorism (O.J. L 164, 22 June 2002, p. 1) and Framework Decision amending the framework decision on terrorism (O.J. L 330, 9 December 2008, p. 21).

23 Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography (O.J. L 13, 20 January 2004, p. 44). A new proposal to repeal this measure is currently under discussion.

24 Council Framework Decision 2005/222/JHA on attacks against information systems (O.J. L 69, 16 March 2005, p. 67).

25 Council of the European Union, Justice and Home Affairs, 2899th Council meeting, Luxembourg, 24 October 2008.

26 Council of the European Union, Multidisciplinary Group on Organised Crime (MDG): "Proposal by the Spanish presidency for an action plan on the concerted

strategy to combat cybercrime" (Council of the European Union, 5071/10, 8 January 2010)
27 3010th General Affairs Council meeting: Conclusions concerning an Action Plan to implement the concerted strategy of combat cybercrime, Luxembourg, 26 April 2010. Available at: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/114028.pdf.
28 Among the medium term actions, the Council conclusions include, *inter alia*, the Ratification of the Council of Europe Cybercrime Convention and the improvement of the training of the police, judges, prosecutors, and forensic staff to a level appropriate for carrying out cybercrime investigations.
29 The Stockholm Programme – An open and secure Europe serving and protecting the citizens (Council of the European Union 17024/09).
30 European Council 10-11 December 2009 – Conclusions, Brussels, 11 December 2009 (EUCO 6/09).
31 Council of the EU "JHA trio Presidency Programme (January 2010–June 2011)" (Council of the EU, 5008/10, p. 14).
32 Regulation (EC) No. 460/2004 establishing the European Network and Information Security Agency (O.J. L 77, 13 March 2004, p. 1). More information at: www.enisa.europa.eu.
33 To this extent, it is worth noting ENISA's work in the field of CERTs (Computer Emergency Response Teams). Ideally established in each country to effectively respond to information security incidents, CERTs must act as primary security service providers for government and citizens. ENISA gives support to EU Member States and other stakeholders with the establishment and operation of CERTs. More information at: www.enisa.europa.eu/act/cert.
34 For the consolidated versions of the Treaty on European Union and of the Treaty on the Functioning of the European Union, together with the annexes and protocols thereto, as they result from the amendments introduced by the Treaty of Lisbon, see O.J. C 83, 30 March 2010, p. 1.
35 On the impact of the Lisbon Treaty on the fight against cybercrime, see *M. Gercke,* Impact of the Lisbon Treaty on Fighting Cybercrime in the EU – the redefined role of the EU and the change in approach from patchwork to comprehensiveness, 2010 *Computer Law Review International* 3, pp. 75-80.
36 Charter of Fundamental Rights of the European Union (O.J. C 83, 30 March 2010, p. 389).
37 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. L 281, 23 November 1995, p. 31).
38 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (O.J. L 201, 31 July 2002, p. 37).
39 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (O.J. L 350, 30 December 2008, p. 60).
40 See the consolidated versions of the Treaty on European Union and of the Treaty on the Functioning of the European Union in conjunction with Declaration 21, attached to the Lisbon Treaty, which states, however, that specific rules "may prove necessary because of the specific nature of these fields" (O.J. C 83, 30 March 2010, p. 1).
41 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. L 281, 23 November 1995, p. 31).
42 For more information on the Safe Harbor arrangement, see http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/adequacy-faq1_en.htm. A full list of companies that have signed up for the "Safe Harbour" and details of how to sign up can be found on the website of the US Department of Commerce, available at http://www.export.gov/safeharbor/.
43 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) (O.J. L 215, 25 August 2000, pp. 7-47).
44 Commission staff working paper: the application of Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, (SEC(2002) 196) and Commission staff working document: the implementation of Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (SEC (2004) 1323).
45 Article 29 Data Protection Working Party was set up as an independent European advisory body on data protection under Article 29 of Directive 95/46/EC. Tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. More information available at: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.
46 Working Document WP 74: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 3 2003. Available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm.
47 Working Document WP 108: Establishing a model checklist application for approval of Binding Corporate Rules, adopted on 14 April 2005. Available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm.
48 Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, adopted on 24 June 2008 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp153_en.pdf and Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, adopted on 24 June 2008 as last revised and adopted on 8 April 2009. Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp155_rev.04_en.pdf.
49 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance) (O.J. L 39, 12 February 2010, p. 5).
50 2002/16/EC: Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (Text with EEA relevance) (notified under document number C(2001) 4540) (O.J. L 6, 10 January 2002, p. 52).
51 In this regard, see Article 29 Working Group Opinion 1/2010 on the concepts of "controller" and "processor". Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.
52 *P. Hustinx,* Data Protection and Cloud Computing under EU law. Third European Cyber Security Awareness Day, BSA, European Parliament, 13 April 2010, Panel IV – Privacy and Cloud Computing. Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf.
53 *P. Hustinx,* pp. 5-6.
54 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (O.J. C 197, 12 July 2000, p. 3).
55 Council Framework Decision of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (O.J. L 328, 15 December 2009, p. 42).
56 Proposal for a Framework Decision on the Transfer of proceedings in criminal matters (Council of the European Union, Brussels, 26 November 2009, 16437/1/09 REV 1, COPEN 231).
57 Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (O.J. L 138, 4 June 2009, p. 14).
58 Council of Europe Convention on Cybercrime, Budapest 21.XI.2001 (ETS 185) and the Protocol on Xenophobia and Racism (ETS 189). Further information about the Convention, including the text of the instrument itself, the text of its Explanatory Report, and a current list of signatories and ratifying States, are available at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=1&DF=07/01/2010&CL=ENG.
59 On this point see *H. Kaspersen,* Cybercrime and Internet Jurisdiction, Discussion paper (draft), version 5 March 2009, prepared in the framework of the Project on Cybercrime of the Council of Europe. Available at: http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2009)%20draft%20discussion%20paper%20Cybercrime%20and%20jurisdiction.pdf.
60 Article 3 of the The Data Protection Directive excludes from the scope of application the data processing carried out "by natural persons in the course of a purely personal or household activity". As pointed out by Mr. *Hustinx* in his paper (see supra fn. 52): "In the context of the review of the data protection Directive, it is necessary to consider a way to fill this gap".
61 On this point see Commissioner *Reding* paper: *V. Reding*, Data Protection in the EU – Challenges Ahead, 2010 *eucrim* 1, p. 25. Available at: http://www.mpicc.de/eucrim/archiv/eucrim_10-01.pdf.

Passenger Name Record Agreements: The Umpteenth Attempt to Anticipate Risk

Dr. Francesca Galli

Over the last decade, the United States and the European Union have become increasingly important partners in combating terrorism and have further developed intertwined security interests.

The signing of the so-called SWIFT II agreement[1] on 28 June 2010 (approved by the European Parliament on 8 July 2010) raises, once again, issues concerning the potential conflict between data protection and security matters in the context of transatlantic cooperation.[2] The aim of this instrument is

> to make sure that designated providers of international financial payment messaging services (and primarily the company "Swift") make available to the United States Department of the Treasury financial payment messaging data stored in the territory of the European Union necessary for preventing and combating terrorism and its financing.

In fact, a great amount of the data managed by Swift will soon be stored only in the EU and no longer in the US.

The debate surrounding the adoption of the new instrument gives civil libertarians another chance to discuss the evolving content of the controversial PNR agreements. Indeed, although the PNR agreement signed by the Council in July 2007[3] would only expire in 2014, the entry into force of the Lisbon Treaty requires the consent of the European Parliament in order for the agreement to be formally concluded and to preserve its legal effect.

I. Legal and Factual Background

The use of databases and the cross-referencing of elements to identify suspects has long been a powerful tool for law enforcement authorities in the prevention and prosecution of organized crime. In the aftermath of September 11, information exchange and information sharing was seen as crucial in the fight against terrorism.

Within this framework, US law enforcement authorities asserted the need to monitor and control flights over their territory. In fact, as many as 400 flights depart for the US each day from around 80 different European destinations. The US Aviation and Transport Security Act of 19 November 2001 (as amended by the 2004 Intelligence Reform and Terrorism prevention Act), required airlines that operate passengers to, from, or through the US to provide advance information on air travelers by means of the US customs and border patrol access to the electronic Passenger Name Records.[4]

Airlines were thus confronted with a dilemma: either facing severe fines and possibly the loss of landing rights if they refused to forward the information requested or infringing the data protection rules enshrined in the EU Data Protection Directive in order to respond to the security request made by the US.

The Data Protection Directive entered into force in 1995 to regulate the transfer of personal data within the EU and to third countries. It provides several fundamental principles that are at the heart of the current right to data protection as recognized in the EU: the principle of fair and lawful processing of data; the purpose limitation principle (the gathering of personal data requires specified, explicit, and legitimate purposes – the collection of data for future purposes and their use for purposes other than those for which they were collected or compatible therewith is prohibited); the principle of transparency; and the right of individuals to access and to redress personal information. Most importantly, according to Art. 25(1), the transfer of personal data from EU Member States to third countries may take place only where the third country in question ensures an adequate level of data protection.

At the source of the dispute is the fact that the concept of privacy and of data protection is approached in a completely different manner in the EU (where Member States' views are far from being harmonized) and in the US. In US constitutional law, the right to privacy is conceived as a restriction of the powers of the government to interfere with citizens' private lives. The right to privacy does not convey the idea that citizens should be able to monitor and control how their personal data are derived, analyzed, and processed. Individual privacy and personal data are not protected directly but through a combination of provisions, each of a different nature (constitutional law, Supreme Court case-law, sector-specific legislation, etc.) leading to a piecemeal result.[5]

The EU Commission had to find an agreement in order to reconcile two opposite necessities and strike a provisional balance between the different issues at stake: not only the prevention of crime and terrorism as well as the protection of fundamental rights but also the fragile EU/US relationship.

In an Area of Freedom, Security and Justice, allegedly becoming all the more an area of only security, PNR agreements have not always been considered a necessary and proportionate measure to fight terrorism.[6] At times, the European Parliament expressed doubts as to the adequate level of data protection in the US and fiercely criticized successive PNR agreements, not always considered a necessary and proportionate measure to fight terrorism. The European Data Protection Supervisor and Art. 29 Working Party raised similar concerns as to the impact on fundamental rights and the need to redraft the agreements to introduce better safeguards.[7]

Parliaments' actions led to the pronouncement of the judgment of the European Court of Justice on 30 May 2006 aimed at the 2004 PNR agreement.[8] The Court addressed the Commission adequacy decision, recognizing that, as required by Art. 25(1) of the Data Protection Directive, the US provide an adequate level of protection for the transfer of PNR information; the international agreement was concluded on the basis of such decision by the Council. The Luxembourg Court held that the agreement had been concluded on the wrong legal basis (art 95 TUE) as it pertains to third pillar security issues and not first pillar commercial matters. However, to the disappointment of civil libertarians, the ECJ annulled the PNR agreement without touching upon its content or assessing whether fundamental rights had been infringed. The ECJ judgment focused on a rather technical issue and did not amount to a key decision on the balance between liberty (and particularly the right to privacy) and security in the aftermath of September 11. There were no major changes in the newly negotiated agreement.

II. Causes for Concern

Firstly, the *purpose of the agreement* is too broad and vague. It is not limited to counter-terrorism purposes but is directed at "other serious crime including organized crimes that are transnational in nature." The vagueness of this wording allows great discretion in its interpretation and the consequent application of the agreement. Thus, it raises not only legal certainty issues but also concerns in relation to the balance between the necessity of this measure and the intrusiveness of state intervention in this context.

Secondly, the *quality and proportionality of the data* is problematic: PNR are a particularly expansive category, which can include sensitive information such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, and/or data concerning health or sex of the individual. The gathering of sensitive data without any judicial oversight, coupled with the lack of accountability and a broad definition of the scope of the PNR agreement, could give a renewed impetus to racial profiling. This selective practice implies the reliance upon group characteristics such as race, national or ethnic origin, and religion as part of a profile to determine the targets of preventive police power. In the absence of any objective criteria to identify those individuals who belong to the category of "dangerous people," sensitive data could establish policing on prejudice about identity and racial profiling so that criteria such as race, religion, and ethnicity are considered and used as indicators of dangerousness under counter-terrorism policies.

In addition, PNR agreements allow for a bulk collection of personal data as it is not focused on individuals supposedly presenting a risk. Risk assessment analyses are thus carried out in an undifferentiated manner, from terrorist suspects and alleged criminals to innocent passengers. Such wide scale data gathering, analysis, and storage raises legitimacy and proportionality issues and is potentially in conflict with the right to privacy under Art. 8 ECHR as interpreted by the Strasbourg Court. In *S and Marper v UK* (2008), the ECtHR noted that the British legislation on the retention of DNA samples failed to strike a proper balance between public and private interests, the power of retention having a "blanket and indiscriminate nature." The Court highlighted that

> it is as essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[9]

The access to PNR data is not simply meant for identification purposes but is supposedly useful to deduce the dangerous or suspicious intention of passengers who are worth further investigation. Data mining programmes are able to generate automated profiling based on PNR information and computer-generated risk assessment scores to identify passengers who may pose a risk without being on any government's watch list. A wrongful interpretation of the information provided by the computer could, however, lead to misleading conclusions.

While personal data must be collected and analyzed accurately, the quality of the assessment could be biased by the fact that PNR information are collected by airlines for commercial purposes, with low data protection standards, and then used for public security purposes by law enforcements authorities.

Civil libertarians have also repeatedly questioned the duration of the storage itself and the possibility to share personal data with agencies that are not responsible for counter-terrorism and thus would use it for different purposes. A comparison with similar PNR agreements concluded with Australia and Canada shows that a more complex regulatory framework of safeguards is attainable.[10]

III. Liberty vs. Security

These issues have to be placed in the greater context of the balance between liberty and security and the numerous competing interests existing in this area. How is the protection of personal data balanced against the need for security? Is the gathering and sharing of personal information the price to be paid for enhanced security or simply abuse of the right to privacy?[11]

There has been a lot of misleading public debate about the alleged opposition between data protection law and security concerns of governments and law enforcement agencies. In fact, a possible hindrance to the investigation and prosecution of criminal offences and criminals constituted by data protection provisions is simply a myth. Nonetheless, a number of questions arise as to the boundaries of both data protection provisions and security measures. In particular, the access of law enforcement authorities to personal data of individuals who are not suspected or convicted of a criminal offence should be strictly limited and regulated. The fight against organized crime should not allow the indiscriminate use of data collected for one purpose (e.g., commercial purposes) for a different one.

IV. The Prediction and Prevention of Future Risks

In the context of PNR agreements, there is an increasing quantity of data to be processed and analyzed. Such an analysis has the ambitious purpose not only of spotting known or potential terrorists but also of carrying out risk assessments of individuals prior to boarding. PNR agreements apply to all passengers regardless of whether they are suspected of having committed or being about to commit an offence. However, they do not specify how and on the basis of which criteria personal data are processed to carry out such risk assessment.

In a broader context, the growing threat represented by terrorism and organized crime has modified the means and legitimization of state intervention placing risks and damage control at its centre. For instance, the criminologists Feeley and Simon describe a risk management strategy for the administration of criminal justice aiming at securing at the lowest possible cost-dangerous classes of individuals.[12] The focus is on targeting and classifying suspect groups and making assessments of their likelihood to offend in particular circumstances or when exposed to certain opportunities.

There is a need to act with great urgency to cope with potential risk, and there is no time to obtain a clear view on whether there would be sufficient evidence to support an investigation or a prosecution. Law enforcement authorities hence act on the lower standard of risk rather than on proof of criminal activities for purposes connected with protecting members of the public from a risk of terrorism.

Policy-making and crime-fighting strategies are increasingly concerned with the prediction and prevention of future risks (in order, at least, to minimise their consequences) rather than the prosecution of past offences.[13] Zedner describes a shift towards a society "in which the possibility of forestalling risks competes with and even takes precedence over responding to wrongs done,"[14] and where "the post-crime orientation of criminal justice is increasingly overshadowed by the pre-crime logic of security."[15] The crime prevention logic is characterised by "calculation, risk and uncertainty, surveillance, precaution, prudentialism, moral hazard, prevention and, arching over all of these, there is the pursuit of security." An analogy has been drawn with the "precautionary principle" developed in environmental law in relation to the duties of public authorities in a context of scientific uncertainty, which cannot be accepted as an excuse for inaction where there is a threat of serious harm.[16]

Although it certainly existed prior to September 11, the counter-terrorism legislation enacted since then has certainly expanded all previous trends towards anticipating risks. The aim of current counter-terrorism measures is mostly that of preventive identification, isolation, and control of individuals and groups who are deemed dangerous and allegedly represent a threat to society. The risk in terms of mass casualties resulting from a terrorist attack is thought to be so high that traditional due process safeguards are considered unreasonable or unaffordable, and prevention becomes a political imperative. In the words of the UK Anti-Terrorism Branch:

> The threat from international terrorism is so completely different that it has been necessary to adopt new ways of working (…). The advent of terrorist attacks designed to cause mass casualties, with no warning, sometimes involving the use of suicide, and with the threat of chemical, biological, radiological or nuclear weapons means that we can no longer wait until the point of attack before intervening. The threat to the public is simply too great to run that risk … the result of this is that there are occasions when suspected terrorists are arrested at an earlier stage in their planning and preparation than would have been the case in the past.[17]

During the last decade, for instance, parliaments have been active in defining and adopting new offences in the "inchoate

mode" and criminalising preparatory activities even if they are several steps away from the actual perpetration of the crime. Not only do inchoate offences expand criminal liability, but they also allow the use of enhanced preventive powers and police intervention before the commission of any substantive crime.

In relation to terrorism, additional tension arises between criminal justice, which is supposed to be impartial, and the politically charged concept of national security.[18] The risk of potential harm is often assessed on the basis of secret evidence and based on political considerations, possibly prior to the filing of a criminal charge. In cases of judicial review, this tension has sometimes led to a certain level of judicial deference towards the executive, which is perceived to be better placed to make decisions where national security is at stake.[19]

This paradigm shift towards preventive action poses critical challenges for the protection of individual rights. First, the boundaries of what constitutes dangerous behaviour are highly contentious, and problems arise with the assessment of future harm. Secondly, "suspicion" has replaced the more objective criterion of "reasonable belief" in most cases in order to justify police intervention at an early stage in terrorism cases, without the need to see evidence-gathering with a view to a prosecution. Governments can thus act on the lower standard of possibility of future harm rather than the higher standard of proof of past criminal activities. This allows a shift towards greater governmental discretion for reasons of national security at the expense of judicial scrutiny.[20] Lastly, preventive measures encompass a larger number of activities and affect a broader range of people. In fact, many powers are not explicitly limited in their scope to the terrorism context, international or otherwise. As a result of the disengagement of anti-terrorism legislation from a specific situation in time and/or space, the current policies have become applicable to a much wider range of circumstances. Whereas the use of ordinary powers implies a curtailment of the rights of a specific suspect, special powers/these kinds of agreements tend to affect more broadly the individual rights of all citizens, whatever risk he or she may (or may not) represent to the community.

V. Conclusions

In relation to preventive measures based on suspicion and risk-assessment procedures, serious dangers of dreadful injustice arise. Do governments really dispose of any means by which to assess whether an individual poses a risk to the public? Are they able to appraise the likelihood that an (otherwise only potential) harmful act will occur? What are the criteria to identify whether the measures adopted would effectively prevent an event from occurring? The question is also whether alternative ways of managing risk are possible.

The Stockholm Programme foresees the establishment in the area of Justice and Home Affairs of a comprehensive EU approach to the use of Passenger Name Record (EU-PNR) data for law enforcement purposes and the creation of a European framework for the communication of PNR data to third countries.

In 2007 already, the Commission made a proposal for a Framework Decision for a European PNR Agreement. It would create a coherent legal framework at the EU-level requiring airlines to transfer PNR information to law enforcement authorities for the purpose of preventing, investigating, and prosecuting terrorism and organised crime.[21] While increasing legal certainty, the new framework would also constitute an EU attempt to strike the right balance between privacy, security, and transparency. In addition, it would avoid unequal protection of individual rights currently resulting from the many differences between existing PNR agreements with the US, Canada, and Australia. Moreover, the EU legal framework for the transfer of personal information to third countries will have to comply with the requirements of the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which was adopted on 30 December 2008, after several years of discussion. This instrument established a common level of privacy protection and a high level of security in the exchange of personal information throughout Europe and in the transfer of personal data to third countries.[22]

The entry into force of the Lisbon Treaty and the greater institutional involvement of the European Parliament have suspended the discussions on the establishment of an EU-PNR processing system. The plan is strongly supported by the Council and the Commission, but the negotiations will be complex due to the different approaches to privacy and data protection in the EU Member States. It is remarkable that, with the Lisbon Treaty, any PNR agreements require the consent of the Parliament before they can be concluded by the Council.

1 Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program ("Swift Agreement"), Council 11222/1/10 REV 1, 11222/1/10 REV 1 COR 1 and 11350/2/10.
2 The interim agreement had previously been rejected by the European Parliament in February 2010. The approval of the European Parliament became necessary following the entry into force of the Lisbon Treaty.
3 Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and

Dr. Francesca Galli
FNRS Post-Doctoral Research, Institut d'Etudes Européens – ECLAN, ULB – Brussels
francesca.galli@ulb.ac.be

the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) and Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement).

4 Passenger Name Record is the general name given to elements gathered by airlines for each passenger journey, such as identification data (full name, date of birth and citizenship, sex, passport number and country of issuance), information on departure and return, billing and payment, services required.

5 See *V. Papakonstantinou* and *P. de Hert*, The PNR agreement and transatlantic anti-terrorism co-operation: no firm human rights framework on either side of the Atlantic, 2009, 46 *CML Rev* 885, pp. 892-898.

6 See, for instance, *E. De Busser*, Data protection in the EU and US criminal co-operation, Antwerpen, Maklu 2009; *B. Siemen*, The EU-US Agreement on Passenger Name Records and EC-Law: Data Protection, Competences and Human Rights Issues in International Agreements in the Community, 2004 *German Yearbook of international Law* 47, p. 629; Assemblée nationale, Rapport sur la proposition de decision cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record, PNR) à des fins répressives, COM (2007) 654 final/ n° E 3697, n°1447, 11 février 2009.

7 See, for instance, The Future of privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 1 December 2009, 02356/09/EN, WP 168.

8 *M. Mendez*, Annulment of Commission Adequacy Decision and Council Decision Concerning Conclusion of Passenger Name Record Agreement with US, 2007 *EuConst* 3, pp. 127-147; *G. Gilmore/J. Rijpma*, Joined Cases C-317/04 and C-318/04' 2007 *CML Rev* 44, pp. 1081-1099.

9 In support of its judgment, the ECtHR refers back, *mutatis mutandis*, to its previous case-law: *Kruslin v France*, 1990, §§ 33 and 35; *Rotaru v Romania*, 2000, §§ 57-59; *Weber and Saravia v Germany*, 2008; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, 2007, §§ 75-77; *Liberty and Others v UK,* 2008, §§ 62-63.

10 Mandates for the renegotiation of these PNR agreements, as well as the one with the US have been adopted on 21 September 2010 in connection with Commissioner Malmström's idea of developing a "PNR package" with minimum requirements – mostly regarding data protection – for this type of agreements. The proposal for the PNR package was also adopted on 21 September.

11 See *J. Lodge*, Eu Homeland Security: citizens or suspects?, 2004 *European Integration* 26, 3, p. 253.

12 *M.M. Feeley* and *J. Simon*, The new penology, 1992 *Criminology* 30, 4, p. 449.

13 *L. Zedner*, Fixing the Future? in *S. Bronnit et al.* (eds), *Regulating Deviance*, Oxford, Hart Publishing, 2008.

14 *L. Zedner*, Pre-crime and post-criminology?, 2007 *Theoretical Criminolog*, 11, p. 261.

15 Ibid, p. 262.

16 See *E. Fisher*, Precaution, precaution everywhere, 2002 *Maastricht Journal of European and Comparative Law* 9, p. 7. The analogy is made by *Zedner*, Fixing the Future?, 2008, pp. 187-88.

17 London Anti-Terrorism Branch (SO13), Submission in support of three month pre-charge detention (2005), appendix of Home Affairs Committee, Terrorism Detention Powers HC (2005-06) 910-I, 54 as quoted by *J. McCulloch/S. Pickering*, Pre-crime and counter-terrorism, 2009 *British Journal of Criminology* 49, 5, pp. 628-632.

18 *McCulloch/Pickering,* Pre-crime, 2009 (see fn. 16).

19 For instance, the House of Lords in the Belmarsh case (2004) had to consider whether sufficient evidence of a "public emergency threatening the life of the nation" had been provided to justify the issue and continuance of the derogation notice under Art. 15 ECHR. The majority of the Court accepted that it was within the government's margin of appreciation to say that, after September 11, the terrorist threat amounted to a national emergency that could be said to threaten the life of the nation.

20 In this respect, it is significant to mention that Art. 16 of the Italian Law decree 144/2005 would have required the public prosecutor to obtain a specific authorisation from the Minister of Justice in order to proceed with the investigation of international terrorism offences. In order to avoid inappropriate interferences in what are meant to be independent judicial activities, Parliament has fortunately decided not to convert the controversial provision into law.

21 *P. de Hert/V. Papakonstantinou,* The EU PNR framework decision proposal: Towards completion of the PNR processing scene in Europe, 2010 *Computer Law & Security Review* 26, 4, p. 368; *M. Nino*, The protection of personal data in the fight against terrorism, 2010, *Utrecht Law Review*, Vol. 6, 1, pp. 82-84.

22 On this instrument and other models of data protection in transatlantic cooperation, see *E. De Busser*, EU Data protection in transatlantic cooperation in criminal matters. Will the EU be serving its citizens an American meal?, 2010 *Utrecht Law Review* 6, 1, p. 86.

Imprint

Impressum

Published by:

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

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

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

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

Typeset: Ines Hofmann, Max Planck Institute for Foreign and International Criminal Law, Freiburg
Produced in Cooperation with: Vereinigung für Europäisches Strafrecht e.V. (represented by Prof. Dr. Dr. h.c. mult. Ulrich Sieber)
Layout: JUSTMEDIA DESIGN, Cologne
Printed by: Stückle Druck und Verlag, Ettenheim/Germany

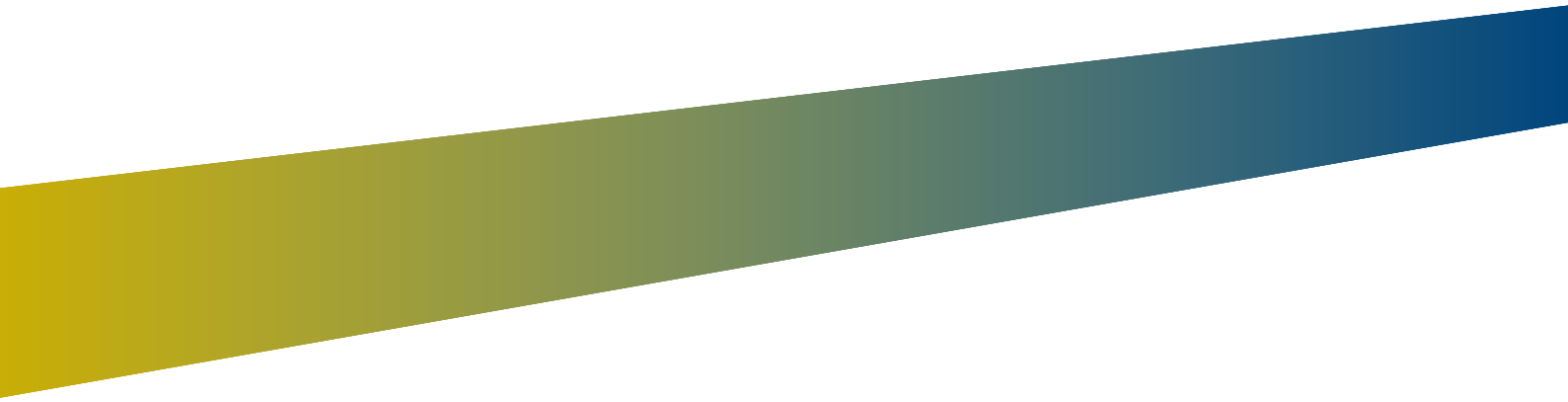
Subscription:
eucrim is published four times per year and distributed electronically for free.
In order to receive issues of the periodical on a regular basis, please write an e-mail to:
eucrim-subscribe@mpicc.de.
For cancellations of the subscription, please write an e-mail to:
eucrim-unsubscribe@mpicc.de.

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)761-7081-227 or +49(0)761-7081-0 (central unit)
Fax: +49(0)761-7081-294
E-mail: e.busser@mpicc.de

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



Max-Planck-Institut
für ausländisches und
internationales Strafrecht