eucrim
2016 / 4
THE EUROPEAN CRIMINAL LAW ASSOCIATIONS' FORUM

Focus: Anti-Money Laundering
Dossier particulier: La lutte contre le blanchiment des capitaux
Schwerpunktthema: Bekämpfung der Geldwäsche

2016/4 ISSUE / ÉDITION / AUSGABE

The Associations for European Criminal Law and the Protection of Financial Interests of the EU is a network of academics and practitioners. The aim of this cooperation 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.

Contents

News*

European Union

Council of Europe

Articles

Anti-Money Laundering

Imprint

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

Guest Editorial

Dear Readers,

Money laundering and other forms of illicit financial crime damage the integrity and stability of the social and economic system. Moreover, this phenomenon represents a scourge afflicting the trust of citizens in the market, both nationally and on the single market level. Especially since the nineties of the last century, when money launderers began to take advantage of the freedom of capital movements, money laundering and terrorism financing became significant problems. These forms of crime are therefore permanently on the political agenda in the EU and internationally, and remain a permanent challenge for national regulators, the European Union, and international standard setters. Among the latter, the Financial Action Task Force on Money Laundering (FATF) aims to counter this scourge efficiently by means of a multidisciplinary approach covering a broad set of preventive and repressive legal measures as well as better international co-operation. In reaction to new money laundering methods, this standard has been regularly updated and modified by tailoring these measures to a risk-based approach with more robust and sophisticated countermeasures, thus reflecting the vulnerabilities of transactions, business activities, financial products, and customer relationships.

This edition of eucrim pays close attention to the current reforms of countermeasures on the EU level, mainly to the Fourth EU Anti-Money Laundering Directive. According to the Commission, the adoption of this directive in May 2015 was a major step forward in improving the effectiveness of the EU's efforts to combat money laundering and the financing of terrorism.

This conflicts, however, with the fact that proposals to amend this directive – correctly described as the Fifth Anti-Money Laundering Directive – were already put on the table in February 2016, although the official deadline for implementation of the Fourth Anti-Money Laundering Directive is only 26 June 2017. Since 2014, some Member States, especially France and Germany, have been demanding a more robust and far-reaching strategy to strengthen the global response to the terrorist financing threat and to close significant loopholes in the current anti-money laundering regime by increasing transparency on virtual currencies and on which beneficial owner really owns companies and trusts. The recent terrorist attacks and the Panama Papers revelations have highlighted the need for the EU to take further measures. Therefore, it soon became apparent that it was not satisfactory that the Commission initially limited the scope of the Fourth Anti-Money Laundering Directive to the transposition of the 40 Recommendations of the FATF, which had already been updated in June 2012.

Michael Findeisen

There is a strong need for eucrim, among other institutions, to become a permanent forum for discussing strategies against money laundering, the financing of terrorism, and other forms of financial crime, based on objective research and scientific approaches. The current multidisciplinary approach, consisting of a bundle of measures from different legal fields such as administrative law, supervisory regulations, penal law, and judicial or administrative assistance, requires a just orchestration of the preventive and repressive approaches and a proportional set of measures protecting European citizens, the integrity of the single market, and civil liberties at the same time. A number of sensitive issues in this context are: the amended regulation on improving the flow of financial intelligence; enabling access to sources of financial information; and expanding the range of reporting entities subject to Suspicious Transaction Reports (STR).

It is the task of us – academics and practitioners alike – to contribute our knowledge and empirical or normative research to this process in order to achieve better regulation.

Michael Findeisen, Ministerialrat (retired)
Head of the Anti-Money Laundering Division of the German Federal Ministry of Finance (2002 –October 2016)

News

Actualités / Kurzmeldungen

European Union*

Reported by Thomas Wahl (TW) and Cornelia Riehle (CR)

Foundations

Fundamental Rights

EP Pushes for EU Mechanism on Democracy, the Rule of Law and Fundamental Rights

On 25 October 2016, the vast majority of MEPs voted for a resolution in which they advocated a stronger EU enforcement of possible breaches of the fundamental EU values. The resolution reacts to the current "crises-driven" approach of perceived breaches of democracy, the rule of law, and fundamental rights (DRF) in EU Member States. The resolution states that the EU has several enforcement instruments at its disposal, for policies involving competition, the police, and judicial cooperation. However, there is no mechanism in place that ensures a swift, effective response from Union institutions to defend the EU's core values. Furthermore, the observation was made that there is a gap between DRF monitoring in EU candidate countries and the lack of effective tools vis-à-vis those that are already EU Member States.

Against this background, the MEPs called for an "Union Pact on democracy, the rule of law and fundamental rights". The EP requested that the Commission submit a respective proposal by September 2017 and has already drawn up detailed recommendations as to how the monitoring and follow-up procedures on the situation of democracy, the rule of law, and fundamental rights should be designed.

The resolution also lays down the fundamental principles of the DRF mechanism. They should be:

- Evidence-based;
- Objective and not subject to outside influence, in particular political influence, non-discriminatory and assessing on an equal footing;
- Respectful of the principles of subsidiarity, necessity, and proportionality;
- Able to address both Member States and institutions of the Union;
- Based on a graduated approach, including both a preventative and corrective arm.

Procedurally, the DRF mechanism would work as follows:

Every year, the EU Commission, in consultation with an independent panel of experts, would draw up a "European DRF Report" on the state of DRF in Member States. This report would include country-specific recommendations, based on several indicators, such as the separation of powers, freedom and pluralism of the media, and access to justice (independence and impartiality, fair trial, constitutional justice, an independent legal profession).

The report would form the basis for any further action by the Commission and follow a clear, progressive approach, ranging from opening a dialogue with the Member State, through invoking Art. 7 para. 1 TEU to provide an early warning before a serious breach has materialised, to the final step of activating Art. 7 TEU, under which a Member State's voting right in Council can be suspended. (TW)

➤eucrim ID=1604001

EU Statement on Human Rights Day

On the occasion of the Human Rights Day, which is celebrated annually on 10 December, the EU's High Representative, *Federica Mogherini*, reaffirmed that the EU stands up for human rights worldwide. She also stressed the need to double the efforts to defend the rights of all people. *Federica Mogherini's* statement includes a brief overview of the EU activities to promote human rights on the global level.

December 10th marks the day on which the UN adopted and proclaimed the Universal Declaration of Human Rights – the first global enunciation of

* If not stated otherwise, the news reported in the following sections cover the period 16 October – 15 December 2016.

human rights and one of the first major achievements of the newly founded United Nations. In 1950, the UN General Assembly invited all states to commemorate this day. (TW)
➤eucrim ID=1604002

FRA Director Concerned about Europe's Human Rights Crises

In a speech held at the Institute for International and European Affairs in Dublin on 24 October 2016, the Director of the Fundamental Rights Agency, *Michael O'Flaherty*, expressed concerns about calling into question the European human rights framework in many EU Member States. "We've established an impressive human rights framework in EU Member States. But now for the first time, that very system is being called into question – and that's what is frightening," said *O'Flaherty*.

He also pointed out that anti-migrant sentiment often obscures the fact that the vast majority of those entering the EU over the last year have come from war-torn countries where they could face persecution or death if they had remained. He also spoke of the Fundamental Rights Agency's monthly overviews, which show alarming manifestations of hatred, including violent attacks on migrants as well as arson attacks on their accommodations. (TW)
➤eucrim ID=1604003

Area of Freedom, Security and Justice

Second Progress Report on Security Union

On 16 November 2016, the European Commission presented its second monthly progress report on the establishment of an effective and sustainable Security Union (for the first report and background information, see eucrim 3/2016, p. 123).

The report notes that, since the terrorist attacks in Paris on 13 November 2015, a wide range of non-legislative actions has been taken, but it is now up to the European legislator to reach agreement on several important legal acts, such as the proposed Directive on combatting terrorism, the proposed revision of the Firearms Directive, and the proposed amendments to the Schengen Borders Code.

As for achievements, the Commission's report highlights the launch of the European Border and Coast Guard on 6 October 2016 (see eucrim 3/2016, p. 126), the further development of the Radicalisation Awareness Network (bringing together local actors and sharing best practices on what works in the fight against radicalisation), and the proposal for a European Travel Information and Authorisation System (ETIAS, see news item below under "Schengen").

The next report will focus on progress made in the area of cybercrime and cyber security as well as the tackling of online radicalisation. (TW)
➤eucrim ID=1604004

Commission Aims to Better Tackle Travel Document Fraud

On 8 December 2016, the Commission presented an Action Plan setting out concrete measures to improve the security of travel documents. Detecting travel document fraud is one of the major issues within the EU to ensure internal security and better manage migration. The Action Plan is targeted at travel documents issued by EU Member States to EU citizens and third-country nationals, which are used for identification and border crossing. The Action Plan provides clear recommendations for Member States on how to tackle the phenomenon of travel document fraud and outlines measures in four key areas:

- Registration of identity;
- Issuance of documents;
- Document production;
- Document control.

The Commission will evaluate the progress made on the implementation of the Action Plan in 2018. The initiative to better tackle travel document fraud is also one element of the EU's own efforts to build up an effective and genuine security union. (TW)
➤eucrim ID=1604005

Schengen

Commission Proposes European Travel Information and Authorisation System

Together with its second progress report on the Security Union, the Commission tabled a proposal for a Regulation establishing a European Travel Information and Authorisation System (ETIAS) on 16 November 2016. ETIAS is designed to react to the problem that the competent border and law enforcement authorities currently have little information on people who are visa-free travellers and can therefore hardly identify whether those persons may pose a security or irregular migration risk before they arrive at the EU's external border.

The proposed rules would introduce a new mandatory condition, i.e., visa-free travellers must be in possession of a valid ETIAS travel authorisation before they enter the EU. ETIAS itself will be a new automated IT system that would be able to identify any risks associated with a visa-exempt visitor travelling to the Schengen area. ETIAS will mainly follow three steps:

- Verification of the information submitted by visa-exempt third-country nationals (such as information related to identity, travel documents, residence information, contact details, etc.) via an online application prior to their travel to the EU;
- Automated cross-checking of the information received with other EU information systems (such as SIS, VIS, Europol's database, Interpol's database, the EES, Eurodac, ECRIS) as well as automatic processing against a dedicated ETIAS watch list (established by Europol) and clearly defined screening rules to determine whether there are factual indications or reasonable grounds to refuse travel authorisation;

- Automatic issuing of travel authorisation if there are no hits or elements requiring further analysis.

ETIAS is not a visa. In sum, it will deliver advanced information as regards visa-exempt visitors coming to the Schengen border. The EU will ensure that all visitors are checked prior to arrival while not encroaching upon their visa-free status. The system is, however, especially relevant for land borders, because those visa-exempt third-country nationals travelling on land (by foot, car, bus, truck, train) do not generate Advance Passenger Information (API) or Passenger Name Records (PNR) as is the case with air and/or sea travel.

The proposal of the Commission has been aligned with similar information systems already in use in the USA, Canada, and Australia. ETIAS was already announced by Commission President *Jean-Claude Juncker* in his latest state-of-the-Union address in September 2016. It is also a first deliverable of the priorities for action identified in the "Bratislava Roadmap" in which the heads of state or government set clear priorities for EU action within the next 12 months. (TW)

➤eucrim ID=1604006

Systematic Checks of EU Citizens: EP and Council Pave the Way

On 5 December 2016, the European Commission announced that the European Parliament (EP) and the Council reached an agreement on the Commission's proposal to introduce mandatory systematic checks of all travellers, including EU citizens, against relevant databases when crossing the EU's external borders (see eucrim 1/2016, p. 3).

It is now up to the plenary of the EP and the JHA Council to finally adopt the legislative act. The EP is likely to vote in February 2017.

The Commission's legislative initiative is a direct response to the terrorist attacks in Paris in November 2015. It is part of the Commission's efforts to build up the Security Union (see news items above). (TW)

➤eucrim ID=1604007

Internal Border Controls Prolonged

The Commission had initially planned to lift all internal borders controls in the Schengen area by the end of December 2016. However, on 11 November 2016, the Council adopted a decision giving Austria, Germany, Denmark, Sweden, and Norway green light to again prolong proportionate temporary border controls for a maximum period of another three months (for the first decision on the prolongation, see eucrim 2/2016, p. 67). The decision must be seen in the context of the continuing deficiencies that Greece is experiencing in managing the refugee crisis. According to the Council, the current fragile situation in Greece still poses serious threats to safeguarding public order and internal security, resulting from the secondary movements of irregular migrants.

According to the Schengen rules, the Commission may propose a recommendation (to be adopted by the Council by qualified majority) to reintroduce controls at all or specific parts of the border of one or more Member States as a matter of last resort. The controls may be introduced for a period of up to six months, but they can be prolonged for additional six-month periods for a maximum duration of two years. The latest Council decision was based on the prolongation recommendation of the Commission of October 2016. (TW).

➤eucrim ID=1604008

Institutions

OLAF

OLAF Seals Cooperation with Taiwan

On 25 November 2016, OLAF Director-General *Giovanni Kessler* signed two administrative cooperation arrangements (ACAs) with Taiwan Customs and with the Bureau of Foreign Trade (BoFT) of Taiwan. The arrangements allow, *inter alia*:

- Cooperation with regard to enquiries that might indicate breaches of Taiwanese and/or European law;
- Provision of assistance to OLAF in checking the sources of products imported into the EU and declared as originating in Taiwan, e.g., by verifying companies and providing relevant data;
- Support to OLAF in tracking the movements of commercial goods;
- Exchange of lists of high-risk goods or relevant information on suspected false reports on rule of origin.

The arrangement stresses the importance of OLAF's international cooperation with the competent authorities in order to detect fraud affecting the EU's financial interests. (TW)

➤eucrim ID=1604009

OLAF and Anti-Corruption Practitioners Call for Transparency of Financial Transactions

At its 16th annual professional conference from 15 to 17 November 2016, the European Partners Against Corruption and the European Contact-point Network against corruption (EPAC/EACN) – a high-level European network of anti-corruption practitioners, composed of more than 70 organisations including OLAF – adopted the Riga Declaration. Alongside a better exchange of information, one of the key points of the declaration is the call for the transparency of financial transactions by promoting the disclosure of information on the beneficial ownership registers on companies and business-related trusts.

Increased action is also called for in the healthcare sector:

- Adoption of comprehensive policies to fight corruption within the healthcare system at national and international levels;
- Transparency and effective administrative control of the management of the public healthcare systems. (TW)

➤eucrim ID=1604010

Europol

Memorandum of Understanding Signed with RIPE NCC

On 14 December 2016, Europol signed a Memorandum of Understanding with RIPE NCC, a not-for-profit membership organisation acting as a Regional Internet Registry providing global Internet resources and related services to members in its service region, i.e., Europe, the Middle East, and parts of Central Asia.

Under the Memorandum of Understanding, the two organisations shall enhance their cooperation and share best practices in the areas of cybercrime and Internet security. (CR)

➤eucrim ID=1604011

International Standard ISO/IEC 17020 Accreditation

In December 2016, the Europol Forensics Laboratory was accredited against the criteria of the International Standard ISO/IEC 17020 for the forensic examination of banknotes. The laboratory complies with the requirements of a competent inspection body and the professional judgment of its inspectors to undertake forensic examinations. (CR)

➤eucrim ID=1604012

New Agreement with Ukraine Signed

On 14 December 2016, Europol and Ukraine signed an agreement on Operational and Strategic Cooperation to combat cross-border criminal activities. Under the agreement, both parties are allowed to exchange information, including the personal data of suspected criminals, and to jointly plan operational activities. (CR)

➤eucrim ID=1604013

Letter of Intent with ASEANAPOL Signed

On 8 November 2016, Europol signed a Letter of Intent to strengthen its cooperation with ASEANAPOL, the Association of Southeast Asian Nations Association of Chiefs of Police. The letter facilitates the mutual support for and the exchange of best practices and expertise between the two organisations.

ASEANAPOL, established in 1981, is a forum of Chiefs of Police of ten member states of the Association of Southeast Asian Nations (ASEAN). Its objectives are to:

- Enhance police professionalism;
- Forge stronger regional cooperation in policing;
- Promote lasting friendships amongst police officers of member countries.

ASEANAPOL has had a permanent secretariat since 2010, based in Kuala Lumpur/Malaysia. ASEANAPOL facilitates intelligence and information sharing/exchange, coordinates joint operations involving criminal investigations, maintains the e-ADS, and works to enhance the capacities of the subregion. It deliberates regional law enforcement and crime control matters, including terrorism, and conducts training courses and seminars for police officers of ASEAN states. (CR)

➤eucrim ID=1604014

Stakeholder Conference on the Evaluation of Regulation No. 883/2013

Brussels, 1–2 March 2017

In 1999, the Commission set up the European Anti-Fraud Office (OLAF) to investigate fraud and any other illegal activity affecting EU's financial interests and to help EU Member States fight fraud. The exercise of OLAF's mandate is now governed by Regulation (EU, EURATOM) No. 883/2013. The Commission is currently evaluating the application of this regulation with the intention of reporting to the European Parliament and the Council on it by October 2017.

The evaluation is a part of the policy cycle. It will provide evidence for any future revision of the regulation if shortcomings of the legislative framework and its implementation are identified. It is also expected to assess any necessary adaptations in order to clarify OLAF's role and added value vis-à-vis the EPPO as well as any possible need to adapt OLAF's mandate and powers to current needs and developments.

As part of the broad consultation of stakeholders carried out for the evaluation (mainly in the form of interviews and surveys), OLAF is organising a "Stakeholder conference on the evaluation of Regulation No. 883/2013" (Brussels, 1-2 March 2017).

The conference will bring together stakeholders from a wide range of anti-fraud backgrounds, such as AFCOS; EU institutions, bodies, offices, and agencies (IBOAs); international organisations, academics, judicial practitioners, etc. Conference participants will contribute (new) insights into the application of the regulation by discussing the preliminary evaluation findings and possible changes to the regulation that might need to be considered in the future. Registration will begin in January and will be carried out on a first come first serve basis. More information is available at *http://ec.europa.eu/anti-fraud/policy/olaf-regulation-evaluation_en*.

Eurojust

New Liaison Prosecutor for Norway

On 1 September 2016, *Hilde Stoltenberg* was appointed Liaison Prosecutor for Norway to Eurojust.

Prior to joining Eurojust, Ms. *Stoltenberg* worked as an assistant professor at the Norwegian Police Academy and as Regional Public Prosecutor for Nordland.

Ms. *Stoltenberg* succeeds the outgoing Liaison Prosecutor for Norway, *Petter Sodal*. (CR)

➤eucrim ID=1604015

Vice-Presidents Elected and Re-elected

On 8 November 2016, *Klaus Meyer-Cabri*, the Eurojust National Member for Germany was elected Vice-President of the College of Eurojust. Prior to joining Eurojust in 2014, Mr. *Meyer-Cabri* served as Head of the EU and International Department of the German Federal Ministry of Justice and Consumer Protection.

Furthermore, on 14 December 2016,

the Eurojust National Member for the Slovak Republic, *Ladislav Hamran*, was re-elected as Vice-President for a second three-year term. (CR)
➤eucrim ID=1604016

First Joint Publication with EMCDDA

On 15 November 2016, Eurojust and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) released their first joint publication entitled "New psychoactive substances (NPS) in Europe. Legislation and prosecution – current challenges and solutions."

The report, which is aimed at policy-makers, shows challenges in NPS control and describes the different legislative solutions in the EU Member States. Furthermore, it addresses legal practitioners by outlining the NPS judgment of the CJEU (joined cases C-358/13 and C-181/14) and its practical effects on transnational prosecution of NPS cases. It also describes the responses of those Member States most affected by the ruling. (CR)
➤eucrim ID=1604017

Kick-Off Meeting of the European Judicial Cybercrime Network

On 24 November 2016, the European Judicial Cybercrime Network met for the first time. The network was set up by the Council Conclusion of 9 June 2016, with the aim of providing a centre of specialised expertise to support prosecutors and judges dealing with cybercrime, cyber-enabled crime, and investigations in cyberspace. The network is composed of at least one national representative of the judicial authorities (designated by each Member State) with appropriate expertise to participate in the network. It is supported by Eurojust.

In this first meeting, the cybercrime experts, together with observers from Norway and Switzerland as well as representatives of the General Secretariat of the Council, the European Commission, the EJN Secretariat, and Europol's European Cybercrime Centre (EC3) discussed the technical and legal challenges in relation to encryption. They also discussed the legal obstacles to undercover investigations online. (CR)
➤eucrim ID=1604018

Frontex

Rapid Reaction Pool Launched

On 7 December 2016, Frontex launched its rapid reaction pool of 1500 border guards committed by EU Member States and Schengen-associated countries in order to assist Member States in emergency situations at the EU's external borders. Experts in the pool include surveillance officers, registration and finger scanning experts, advanced-level document officers, and nationality screening experts. Frontex is to be able to deploy them within five working days. (CR)
➤eucrim ID=1604019

European Border and Coast Guard Agency Launched

On 6 October 2016, the official launch of the European Border and Coast Guard Agency (see eucrim 3/2016, p. 126) took place at an event held at the Kapitan Andreevo Border Checkpoint at the Bulgarian external border with Turkey. (CR)
➤eucrim ID=1604020

Deployment of Liaison Officers

Following up on the decision of April 2016 to deploy liaison officers to countries outside the EU affected by migration flows, Frontex has now deployed a liaison officer to Turkey. Furthermore, a liaison officer for the Western Balkans will be deployed to Belgrade from spring 2017. (CR)
➤eucrim ID=1604021

Risks Analysis Reports for April–June 2016 Published

Frontex has published its FRAN, Western Balkans, and Eastern Partnership Quarterlies for the period from April to June 2016. The quarterlies provide an overview of irregular migration at the EU's external borders as well as irregular migration developments affecting the Western Balkans region and countries of the Eastern Partnership Risk Analysis Network (Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine). (CR)
➤eucrim ID=1604022

Specific Areas of Crime / Substantive Criminal Law

Protection of Financial Interests

Preliminary Agreement on PIF Directive

After two trilogue meetings, the Presidency of the Council, the European Parliament, and the Commission reached a preliminary agreement on the full text of the Directive on the fight against fraud to the Union's financial interests by means of criminal law ("PIF Directive"). As a result, the Council and the EP were also able to settle their disagreement on the inclusion of VAT-related fraud into the scope of the Directive. The representatives of the EP made clear that the EP will not accept the Directive without inclusion of at least some types of VAT fraud (see also eucrim 3/2016, p. 126).

The compromise found now foresees that the Directive will also apply to serious cross-border VAT fraud of a certain threshold. The draft text in this regard (Art. 2 (2)) reads as follows: "In respect of revenue arising from VAT own resources, this Directive shall only apply in cases of serious offences against the common VAT system. For the purposes of this Directive, offences against the common VAT system shall be considered serious when the intentional acts or omissions defined in Article 3(d) are connected with the territory of two or more Member States of the European Union and involve a total damage of at least EUR 10 million."

This is flanked by the introduction of a clause by which the Commission will have to evaluate the appropriateness of

the threshold 36 months after the implementation deadline.

At its meeting on 9 December 2016, the JHA Council agreed on its position. It is now for the Council and the EP to formally adopt the text of the Directive in the coming weeks.

The proposed directive provides common definitions of a number of offences against the EU budget, such as fraud and other fraud-related crimes, e.g., active and passive corruption, the misappropriation of funds, money laundering. Furthermore, it will stipulate minimum rules on prescription periods, within which the case must be investigated and prosecuted, as well as minimum rules on sanctions, including imprisonment for the most serious cases in order to strengthen the deterrent effect. It is expected that the new rules, which would replace the PIF Convention of 1995 and its protocols of 1996 and 1997, will also help to improve the investigation and prosecution of fraud damaging the EU's budget across the European Union. (TW)

➤eucrim ID=1604023

No Agreement on EPPO

On 5 December 2016, the Slovak Council Presidency tabled a consolidated version of the text of the proposed Regulation establishing the European Public Prosecutor's Office (Council doc. 15200/16) and invited Member States to agree on the text. However, the Justice Ministers of the EU Member States found no unanimous approach at their JHA Council meeting on 8-9 December 2016. As a result, the establishment of the European Public Prosecutor's Office (EPPO) was postponed. Whether a positive conclusion is in reach within the next few months remains open. The press release on the outcome of the discussion reads as follows:

"At the end of the debate, the presidency noted the broad support from member states for the text as a good basis on which further technical work could be done in the last few days of the year. The presidency also noted that a majority of member states supports the principle of the establishment of the public prosecutor. However, the presidency took note of the clear positions of certain delegations and concluded that these give a clear indication of the likely procedural way forward to ensure agreement on this regulation." (TW)

➤eucrim ID=1604024

Joint Action Dismantles VAT Fraudster Group

On 19 October 2016, a joint action involving ten European countries and coordinated by Eurojust and Europol was successful in exposing an organised criminal group responsible for defrauding the EU and its citizens. The group committed VAT fraud by using a sophisticated infrastructure – including buffer companies, missing traders, and companies functioning as alternative payment platforms – to facilitate money laundering and crime-related money transfers, spread over several EU Member States and a number of third states, such as Switzerland and Norway. The coordinated action was initiated by prosecution services and law enforcement authorities in Bavaria/Germany, Poland, and the Netherlands. It was reported that assets of more than GBP 570,000 were seized, and several bank accounts in Switzerland were frozen. The joint action resulted in 18 arrests. (TW)

➤eucrim ID=1604025

Money Laundering

Commission Tables Plans for Harmonisation of Money Laundering

On 21 December 2016, the Commission launched a proposal for a directive to counter money laundering by criminal law (COM(2016) 826 final). With this new EU instrument, the Commission is reacting to identified deficiencies resulting from different national legislation as to definition, scope, and sanctions of the money laundering offence. These differences mainly had two impacts, which the new directive aims to remedy. According to the Commission, the following problems were identified:

- First, police and judicial cooperation as well as the exchange of information is hindered;
- Second, the differences in law can be exploited by criminals and terrorists, who can carry out financial transactions where they perceive anti-money laundering measures to be the weakest (problem of "forum shopping").

Another aim of the new offensive is to implement international obligations on money laundering and terrorist financing, such as the Council of Europe's Warsaw Convention of 2005 and relevant recommendations from the Financial Action Task Force (FATF).

The proposed directive intends to establish minimum rules on the definition of criminal offences and sanctions in the area of money laundering offences. The proposal has two main features:

- The Commission intends to reduce the scope of what Member States consider a predicate offence, i.e., the underlying criminal activity that generates the property laundered. The proposal now lists a wide range of criminal activities that the Member States must recognise as predicate offences. The proposal limits itself to a "listing solution" instead of describing predicate offences, thus following, however, the recommendations of the FATF.
- The proposal defines the material elements of the money laundering offence, taking into consideration Art. 9 of the Warsaw Convention. In line with the Warsaw Convention, three types of money laundering must be criminalised: (1) conversion or transfer, (2) concealment or disguise, and (3) acquisition, possession, or use. The offences must be committed intentionally; an element of negligence is not foreseen.

In certain areas, the Commission's proposal goes beyond international requirements. It establishes, for instance, the minimum level of the maximum

sanctions. Furthermore, it criminalises so-called "self-laundering," i.e., the involvement of a perpetrator who tries to hide the illicit origin of the proceeds of a criminal activity by transferring or concealing and disguising property via the financial system, thus resulting in further damage than that already caused by the predicate offence, e.g., damage to the integrity of the financial system. Beyond international standards, the Commission has also included cybercrime and attacks against information systems in the list of predicate offences.

The presented proposal on harmonising the money laundering offence must be seen in a threefold context: First, it complements the measures planned for revision of the fourth Anti-Money Laundering Directive (see eucrim 2/2016, p. 73 and the articles in this issue). Second, it is part of a wider package of proposals, including proposals on illicit cash flows (see following news item) and the freezing and confiscation of assets (see below "Freezing of Assets"). Third, these legal proposals implement commitments made in the Action Plan from February 2016 against terrorist financing and are an integral part of the plans to build up the Security Union. (TW)

➤eucrim ID=1604026

Commission to Update Cash Control Regulation

An important complementary measure to the anti-money laundering directive is the EU's regulation on the control of cash movements. Since 2007, natural persons entering or leaving the EU through its external borders must mandatorily declare to the customs authorities whether they are carrying currency or bearer-negotiable instruments with a value of €10,000 or more (see eucrim 1-2/2006, p. 12). Evaluation of this regulation (called CRR) has identified several loopholes in the current system as well as challenges that the CRR does not meet. Among them, offenders have managed to circumvent the rules on cash controls, e.g., by sending cash through the post or in a parcel or even by using certain precious/high-value commodities such as gold.

As a result, on 21 December 2016, the Commission proposed a regulation on controls on cash entering or leaving the Union and repealing the previous Regulation (EC) No 1889/2005 (COM(2016) 825). It foresees mainly the following:

- Tightening controls on cash and precious commodities valued at €10,000 or more, which are sent in postal parcels or in freight consignments;
- Extending the definition of "cash" to gold and other high-value commodities as well as to prepaid payment cards that are not linked to a financial account;
- Creating a simplified and more robust mechanism for the exchange of information between national customs authorities and Financial Intelligence Units (FIUs);
- Enabling competent authorities to act on amounts lower than €10,000 in cash entering or leaving the Union if there are indications that the cash is related to criminal activity.

The Commission's proposal on the better control of illicit cash flows was presented together with a proposal for a Directive harmonising the money laundering offence (see above) and a proposal for a regulation to strengthen the mutual recognition of criminal asset freezing and confiscation orders (see below under "Freezing of Assets"). The legislative package must also be seen in the wider context of tackling the financing of terrorism and building up the Security Union. (TW)

➤eucrim ID=1604027

Council Adopts Position on Revision of AML Directive

On 20 December 2016, the Council agreed on a revised text of the Commission's proposal to amend the fourth Anti-Money Laundering Directive (COM(2016) 450 – cf. eucrim 2-/2016, p. 73 and the articles in this issue). The text forms the basis for further negotiations between the incoming Maltese Council Presidency and the European Parliament. The amendments to the Fourth AML Directive (EU) 2015/849 aim mainly at:

- Preventing the financial system from being used for the funding of criminal activities;
- Strengthening transparency rules to prevent the large-scale concealment of funds. (TW)

➤eucrim ID=1604028

Tax Evasion

Council Reaches General Approach on Tax Authorities' Access to AML Information

On 8 November 2016, the Council (composed of the Economics and Finance Ministers of the EU Member States) agreed – without discussion – on a general approach to the proposal on granting tax authorities access to information held by authorities responsible for the prevention of money laundering. Within the anti-money laundering (AML) framework, the EU has established a system of automated data exchange between the Member States, implementing the Global Standard for Automatic Exchange of Financial Account Information in Tax Matters.

By means of the further development of this legal framework, tax authorities should now be able to gain access to AML information processed by financial institutions. The EU institutions consider it necessary to ensure access on the part of tax authorities to the AML information, procedures, documents, and mechanisms to enhance the performance of their duties in monitoring the proper application of Directive 2011/16/EU by the financial institutions. As a result, the amendment to the said directive will enable tax authorities to access information on the beneficial ownership of intermediary entities and other relevant customer due diligence data. The main purpose of this access is to help tax

authorities prevent tax evasion and tax fraud.

The discussed proposal is one of a number of measures set out by the Commission in July 2016, in the wake of the April 2016 Panama Papers revelations (see also the Commission's respective communication in eucrim 2/2016, p. 74). By means of the general approach reached in the Council, the text can now be further debated in the EP. (TW)

➤eucrim ID=1604029

Organised Crime

EP Says EU Must Do More against Organised Crime and Corruption

In a non-legislative resolution of 25 October 2016, the European Parliament (EP) called for making a political priority a European action plan to fight organised crime, corruption, and fraud as well as better police and judicial cooperation in this field. The Commission is called upon to revise existing legislation in order to introduce effective, proportionate, and dissuasive penalties and to clarify the common definitions of crimes, including that of membership in a criminal organisation or association. The resolution takes into account a wide range of issues, including the following:

- Arranging for the correct transposition of existing rules, monitoring their application, and assessing whether they are effective;
- Priorities and operational structure for the fight against organised crime and corruption;
- Strengthening legislative frameworks;
- More effective police and judicial cooperation at the EU level;
- Seizing the assets of criminal organisations and facilitating their re-use for social purposes;
- Preventing organised crime and corruption from infiltrating the legal economy;
- Addressing specific areas requiring action, such as counterfeiting, tax havens, environmental crimes, and cybercrime;
- Addressing the external dimension requiring increased action and coherence.

The resolution, *inter alia*, recommends drawing up "blacklists of any undertakings which have proven links with organised crime or engaged in corrupt practices" and to "bar them from entering into an economic relationship with a public authority and benefitting from EU funds." It also recommends creating a specialist Europol unit designed to combat organised criminal groups "which operate in several sectors at the same time." MEPs also call for a proposal on common rules to protect whistle-blowers by the end of 2017.

Furthermore, the resolution suggests the establishment of several deterrents, such as setting up mandatory rules to ban people who have been convicted or have participated in organised crime or other serious offences, from running for election or working in/for the public administration – including EU institutions. Another suggestion relates to a common method of seizing criminal organisations' assets in the EU.

The resolution is based on a report by Italian MEP, *Laura Ferrara* (EFDD), and was adopted by 545 to 91 votes. (TW)

➤eucrim ID=1604030

Cybercrime

CJEU Ruling on Legitimate Interest in Storing Dynamic IP Addresses

Upon request of the Bundesgerichtshof (Federal Court of Justice, Germany), the European Court of Justice (CJEU) gave statements on the interpretation of the Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data). In the case (C-582/14) before the Bundesgerichtshof, an Internet user, *Patrick Beyer*, sought a court order restraining the operator of a website (in the case at issue: federal government institutions that provide topical information to the public) from storing the IP addresses of his host system.

The first question concerned whether an individual Internet user can benefit from the protection of his personal data under the Directive if his "dynamic IP addresses" are stored by the operator of a website. Dynamic IP addresses have the speciality that the IP address changes each time there is a new connection to the Internet. They do not enable the operator of the website to directly identify the user – identification can only be done when the operator calls in the Internet provider, i.e., a third party. Given this situation, the German courts had doubts as to whether dynamic IP addresses constitute "personal data" in the sense of the Directive.

In its judgment of 19 October 2016, the CJEU clarifies that a dynamic IP address registered by an "online media services provider" (i.e., by the operator of a website; in the present case, German federal institutions), when its publicly accessible website is consulted, constitutes personal data if the operator has the legal means to identify the visitor with the help of additional information provided by the visitor's Internet service provider. In this context, the CJEU observed that there appear to be legal channels in Germany enabling the online media services provider to contact the competent authority. This is especially true in the event of cyberattacks, so that the authority may take the necessary steps to obtain additional information from the Internet service provider and subsequently bring about criminal proceedings, thus making it possible to identify the data subject.

With regard to the second question, the Federal Court of Justice sought guidance as to the purposes for which the Directive (Art. 7 lit. f)) allows the storage of those IP addresses. The CJEU found that the Directive precludes the legislation of a Member State (under which an online media services provider may

collect and use a visitor's personal data without his consent) only to the extent that it is necessary to facilitate and invoice the specific use of services by that visitor. The objective aiming of ensuring the general operability of those services cannot justify the use of such data after the services have been accessed. (TW)
➤eucrim ID=1604031

"No More Ransomware" Programme – A Success Story

On 17 October 2016, Europol informed the public about the success of the project "No more ransomware" (see details in eucrim 3/2016, p. 128). The project was launched by the Dutch National Police, Europol, Intel Security, and Kaspersky Lab in July 2016. It was designed to establish an online platform for combining public law enforcement and private efforts as well as for tackling the current phenomenon of ransomware. The platform provides information on what ransomware is, how it works, and how users can protect themselves.

Europol now reports that more than 2500 people have successfully managed to decrypt their devices, without having to pay the cybercriminals, by using the main decryption tools provided for via the online portal <www.nomoreransom.org>.

Furthermore, 13 countries have signed up for the project within the first three months of its operation, including the non-EU countries Bosnia-Herzegovina, Columbia, and Switzerland. Many more law enforcement authorities and private entities are expected to join in the coming months. (TW)
➤eucrim ID=1604032

Environmental Crime

Council Conclusions on Countering Environmental Crime

At its meeting on 8 December 2016, the JHA Council adopted conclusions that aim at boosting efforts to better prosecute and prevent environmental crime. The conclusions refer to Europol's 2014-2017 Serious Organised Crime Threat Assessment, which identified environmental crime as an emerging threat and one of the world's most profitable organised criminal activities. It was also observed that environmental crime often has a link with fraud offences and the use of fraudulent documents and certificates. The Council states that combating environmental crime in an effective manner requires a comprehensive, multidisciplinary approach at all levels (EU, international, and national). The conclusions make a bulk of recommendations to the various institutions involved in the fight against environmental crime, in particular the competent Member States' authorities, the European Commission, and Europol.

The conclusions also highlight the work of various international, European, and regional networks, such as the informal network for countering environmental crime (EnviCrimeNet) and the European network for the implementation and enforcement of environmental law (IMPEL), in the field of combating environmental crime. The Council calls on them to better cooperate and coordinate European initiatives when dealing with environmental crime. (TW)
➤eucrim ID=1604033

Procedural Criminal Law

Procedural Safeguards

Directive on Legal Aid Published

On 4 November 2016, Directive (EU) 2016/1919 "on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings" was published in the Official Journal (L 297, p. 1). The Directive aims at the right to legal aid being provided and offered in a uniform way across the EU (see also eucrim 2/2016, p. 77). It entails several obligations for Member States, which must implement the provisions by 25 May 2019:

- To ensure that suspects and accused persons who lack sufficient resources to pay for the assistance of a lawyer have the right to legal aid when the interests of justice require the granting of legal aid (Art. 4 (1));
- To allow Member States to apply a means test, a merits test, or both in order to determine whether legal aid is to be granted. The Directive lays down various criteria that must be taken into account by the Member States if they carry out the tests;
- To ensure that Member States grant legal aid *without undue delay* and, at the latest, prior to questioning by the police, by another law enforcement authority, or by a judicial authority and before investigative or certain evidence-gathering acts [identity parades; confrontations; reconstructions of the scene of a crime] (see Art. 4 (5));
- To lay down the new right, i.e., to receive legal aid in European Arrest Warrant cases both in the executing and issuing Member States (Art. 5);
- To also include duties, beyond Art. 6 ECHR, for Member States in respect of the quality of legal aid services and training. In particular, Member States shall take the necessary action, including funding, with the aim of ensuring that a) there is an effective and qualitative legal aid system in place; b) legal aid services are of a quality that is adequate for safeguarding the fairness of the proceedings, with due respect for the independence of the legal profession. (Art. 7 Directive);
- To ensure that Member States, as in other EU directives on defence rights, see to it that suspects, accused persons, and requested persons have recourse to an effective remedy under national law in the event of a breach of their rights under the legal aid Directive.

The legal aid Directive is the sixth and last piece of legislation of the 2009 EU Roadmap to strengthen procedural rights of suspected or accused persons in criminal proceedings. It should be noted

that the Directive does not apply to Denmark, Ireland, and the United Kingdom. (TW)

➤eucrim ID=1604034

FRA Report on Rights to Interpretation, Translation and Information

In November 2016, the EU Agency for Fundamental Rights (FRA) presented a comparative report that looked into the legal framework and policies of the EU Member States on the two specific procedural rights:

- Rights to interpretation and translation in criminal proceedings (Directive 2010/64/EU);
- Right to information in criminal proceedings (Directive 2012/13/EU).

The report was requested by the European Commission and aims at providing EU and Member States with guidance on how the rights of suspected and accused persons can be improved in line with these two Directives. The report also identified practical means of effectively protecting these procedural safeguards throughout the EU.

Regarding the overall findings, the report states that, depending on the cases, both national laws and the application of legal provisions could be improved. Among the issues raised, the following can be highlighted:

- National rules must clarify that suspected and accused persons in all EU Member States are promptly provided with information about at least all the procedural rights listed in Art. 3 Directive 2012/13/EU;
- A uniform template of the Letter of Rights for persons deprived of their liberty should be used;
- Laws and practices restricting access to the materials of the case and their use should be interpreted strictly, and judicial review should be ensured for all decisions restricting access;
- In practice, the distinction between suspects and witnesses should be improved and rights granted to information equally if witnesses are really suspected of having committed a criminal offence;
- General concepts in the Directives, such as "without delay" or "within a reasonable period of time" should be interpreted strictly in practice;
- Low-quality interpretation and translation should be avoided by introducing mandatory training modules and guidelines for criminal justice professionals;
- Record-keeping mechanisms should be established and maintained concerning the provision of information or interpretation.

In addition to these general findings, the FRA report contains detailed opinions on several aspects of the directives, such as:

- The more effective assessment of the necessity of interpretation and translation;
- Eliminating obstacles to the effective communication with legal counsel;
- Safeguarding the confidentiality of communication between suspected or accused persons with their legal counsel;
- Taking into account the particular needs of vulnerable suspects and accused persons more effectively.

The report also lists a series of good practices that would help improve the applicability of the above-mentioned rights in all EU Member States. (TW)

➤eucrim ID=1604035

CJEU Rules on PreEffects of Directive on the Presumption of Innocence (C-439/16 PPU – Emil Milev)

The European Court of Justice (CJEU) had to decide on whether Bulgarian criminal procedure provisions may have to be set aside because they may be not in line with Arts. 3 and 6 of Directive 2016/343, entitled "Presumption of Innocence" (see eucrim 1-1/2016, p. 13 and *Cras/Erbeznik* in the same issue, p. 25) as long as the transposition period has not yet expired.

According to Bulgarian criminal procedure, the court at the trial stage is not entitled to assess whether there are reasonable grounds to suspect that the accused has committed an offence. This is also true if the court has to decide on review of a remand in custody pending trial. The Bulgarian Supreme Court of Cassation stated that the national criminal procedural provisions run counter to the ECHR and that it is up to the legislator to solve the conflict, therefore leaving it to the trial court whether it would like to give priority to the ECHR or to national law and whether it is in a position to rule in this context. The special court for criminal cases of Bulgaria is of the opinion that the decision of the Supreme Court is an interpretative decision that is binding for all national courts and not in conformity with Arts. 3 and 6 of Directive 2016/343. According to the case law of the CJEU, the competent national bodies, including the courts, should refrain from taking measures likely to compromise the attainment of the result prescribed in a directive. The special court referred the question to the CJEU as to whether this case law also applies in the case at issue: the accused, *Emil Milev*, had been charged with a number of offences, including armed robbery and attempted murder and applied for release from custody after the procedure entered the trial stage.

The CJEU confirms its general case law that, during the period prescribed for transposition of a directive, Member States must refrain from taking any measures liable to seriously compromise the result prescribed by that directive. In this context, it is immaterial whether or not such provisions of domestic law, adopted after the directive entered into force, are affected by the transposition of the directive. It follows therefrom that, from the date upon which a directive has entered into force, the authorities and courts of the Member States must refrain, as far as possible, from interpreting domestic law in a manner that might seriously compromise attainment of the objective pursued by that directive after the period for transposition has expired (see Case C-212/04, *Adeneler and Others*).

In the present case, the CJEU found that the attainment of the objectives pursued by the Directive on the Presump-

tion of Innocence is not at risk of being compromised because the decision of the Bulgarian Supreme Court does not prescribe a particular decision, but leaves the national courts free to apply either the ECHR or the national criminal procedure law. (TW)
➤eucrim ID=1604036

Data Protection

CJEU Opposes General Data Retention Regimes (Case Tele2 Sverige)

On 21 December 2016, the European Court of Justice (CJEU) – sitting as Grand Chamber – delivered its long-awaited judgment on the compatibility of national data retention regimes with EU law (for the case and the opinion of the Advocate General, cf. eucrim 3/2016, p. 129). The Court held that EU law does not allow Member States to impose on telecommunications providers the obligation to retain traffic data and location data in a general and indiscriminate way. The Court considers the targeted retention of said data possible solely for the purpose of fighting serious crime – but this only under certain conditions.

With this judgment (Joined Cases C-203/15, *Tele2 Sverige* and C-698/15, *Tom Watson and Others*), the CJEU continues its data protection- and privacy-friendly case-law (cf. cases *Digital Rights Ireland*, *Schrems*, *Google Spain*).

Regarding the concrete case, the CJEU first confirmed that the national measures at issue fall within the scope of Directive 2002/58/EC on "privacy and electronic communications" (as amended by Directive 2009/136/EC). Secondly, the CJEU stated that the possibility for the Directive to derogate from the principle of confidentiality of communications and related traffic data for state security interests must be read in the light of Arts. 7, 8, and 11 of the Charter of Fundamental Rights. This, in turn, raises questions of proportionality (Art. 52 of the Charter).

Against this background, the Court states in a third step that interference with the retention of personal data is particularly serious. Similar to the jurisprudence of the German Federal Constitutional Court, the Luxembourg judges further stated that – although legislation does not permit retention of the content of a communication – the retention of traffic and location data without the subscriber or user being informed "is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance." Therefore, national measures can only be considered justifiable if they are strictly necessary. The CJEU found that this is not the case for national legislation providing for the general and indiscriminate retention of all traffic and location data, i.e., mass storage without differentiation.

By contrast, the Court makes clear that the Directive does not preclude national legislation from imposing targeted retention of data for the purpose of fighting serious crime. However, this legislation must also pass the "strict necessity" test according to the CJEU's case law. This means, *inter alia*:

- Clear, precise, and binding rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authority access to the data;
- Access must be governed by rules laying down substantive and procedural conditions;
- As a general rule, access can only be granted – in relation to the objective of fighting crime – to the data of individuals suspected of planning, committing, or having committed serious crime or of being implicated in such crime; an exception is allowed in specific situations, e.g., when a terrorist attack threatens vital national security interests;
- Access to retained data should, except in cases of urgency, be subject to prior review, carried out by either a court or an independent body;
- Given the sensitivity of retained data, national legislation must provide for the data to be retained within the EU and to be irreversibly destructed at the end of the retention period.

In conclusion, the CJEU held that Swedish and British legislation on data retention is not compatible with the said requirements of the EC Directive read in light with the Charter. The "echo from Luxembourg" may have an impact on respective legislation in other EU Member States. German data retention law (only passed at the end of 2015) indeed provides for shorter retention periods than British law (10 weeks instead of 12 months), but it is also a blanket retention measure without limiting itself to the fight against serious crime. (TW)
➤eucrim ID=1604037

EP and Council Back EU-US Umbrella Agreement

Both the European Parliament (on 1 December 2016) and the Council (on 2 December 2016) backed the conclusion of the so-called "Umbrella Agreement" between the EU and the United States. The agreement enshrines a set of data protection safeguards for all transatlantic information sharing between the relevant authorities in the areas of/for the purpose of prevention, investigation, detection, and prosecution of criminal offences, including terrorism.

The Umbrella Agreement in itself is not a legal basis for the transfer of personal data – this requires another legal basis. The agreement is instead mainly about giving EU citizens certain rights within transatlantic data exchange for law enforcement purposes, e.g., the right to be informed in the event of data security breaches or to have inaccurate information corrected. Furthermore, the agreement ensures EU citizens' equal treatment with US citizens when it comes to judicial redress rights before US courts.

Other safeguards include provisions on clear purpose limitations on data use, the obligation to seek prior consent prior to any onward transfer of data, and the

obligation to define appropriate retention periods.

The Umbrella Agreement was signed by the EU Commission and US authorities on 2 June 2016. MEPs in the LIBE Committee first expressed reluctance to the agreement. However, at their vote on 1 December 2016, the majority of MEPs in the plenary rejected a proposal from the ALDE and GUE groups to seek an opinion from the European Court of Justice on the Umbrella Agreement's compatibility with the EU Treaties. After the endorsement of the Umbrella Agreement by the Council, it is now up to the US authorities to complete their internal procedures before it can enter into force. For the development of the Umbrella Agreement and critical statements, see also eucrim 1/2016, p. 15 and eucrim 2/2016, p. 79. (TW)

➤eucrim ID=1604038

Freezing of Assets / Confiscation

Commission Presents New Mutual Recognition Instrument of Freezing and Confiscation Orders

On 21 December 2016, the Commission tabled a proposal for a Regulation on the mutual recognition of freezing and confiscation orders (COM(2016) 819). It will repeal the current system of cross-border cooperation in this field as set up by

- Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence; and
- Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition of confiscation orders.

The Commission's proposal is a response to identified deficiencies: The current legal framework remains underused and is complicated for practitioners, so that a unified legal instrument is called for. It is estimated that 98.9% of criminal profits are currently not confiscated and remain at the disposal of criminals. Furthermore, the legal framework on cooperation is considered not in line with the latest new EU rules on harmonising the national freezing and confiscating regimes, in particular Directive 2014/42/EU.

The proposed new legal framework aims at making the freezing and confiscation of assets in an EU Member State other than the one where the order was issued faster and more efficient. The proposal mainly changes the following by:

- Covering mutual recognition of all types of freezing and confiscation orders issued during criminal proceedings, i.e., classic, extended, and third-party confiscation as well as non-conviction-based confiscation as decided by a criminal court (orders issued in civil and administrative proceedings are excluded);
- Setting short deadlines for the recognition and execution of freezing orders;
- Establishing a standard certificate for the mutual recognition of confiscation orders and a standard form for freezing orders, allowing for speedy execution of requests (domestic freezing order need not be accompanied);
- Establishing communication duties between the competent authorities, in particular before applying one of the grounds for refusal;
- Improving victims' rights in cross-border situations: in cases in which the issuing state confiscates property, the victim's right to compensation and restitution are to have priority over the executing and issuing states' interests.

The Commission states that fundamental rights safeguards have also been included. For instance, the regulation includes grounds for refusal when the right to be present at the trial (*"in absentia"*) or when the rights of third parties "in good faith" ("*bona fide*") are not respected. In addition, relevant primary and secondary EU law applies, in particular Arts. 47 and 48 of the Charter of Fundamental Rights as well as the directives on procedural rights in criminal proceedings.

This is the first time that a regulation in the field of mutual recognition in criminal matters has been proposed since the entry into force of the Lisbon Treaty. The regulation will be directly applicable in the Member States. As a result, uniformity in the application of the instrument is ensured and problems due to late or incorrect transposition by Member States avoided.

The Commission's proposal for a Regulation on mutual recognition of freezing and confiscation orders is part of a legislative package that strives to strengthen the EU's action against money laundering and terrorist financing. Together with this proposal, the Commission tabled proposals for a Directive on money laundering and for an updated regulation on cash controls (see, for both, "Money Laundering" above). All the legislative acts form part of the EU's plan for a Security Union. (TW)

➤eucrim ID=1604039

Cooperation

European Arrest Warrant

CJEU Rules on the Interpretation of the Term "Judicial Authority"

On 10 November 2016, the European Court of Justice (CJEU) rendered three judgments interpreting the term "judicial authority" in Art. 1 para. 1, Art. 6 para. 1, and Art. 8 para. 1 lit. c) of the Framework Decision on the European Arrest Warrant (FD EAW). All three cases were referred to the Court by the Rechtbank Amsterdam (District Court, Amsterdam, Netherlands), which casts doubts on the practice of EU Member States relating to the authority issuing a EAW. The Rechtbank Amsterdam is the Dutch court responsible for executing EAWs from other EU Member States.

The FD EAW only says that the EAW must be issued by a "judicial authority" and be based on an enforceable "judicial

decision," but does not further define the terms. In all three cases that had to be decided, the questions arose as to whether the terms "judicial authority" issuing a EAW and "judicial decision" must be interpreted as an autonomous concept of EU law. If so, what are the criteria for determining whether the authority of the issuing Member State is such a "judicial authority" and whether the EAW it issues is, consequently, such a "judicial decision" in the meaning of the relevant provisions of the FD EAW?

Each of the cases had specific characteristics, as a result of which the CJEU did not join the cases, but rendered three separate judgments. In all judgments, however, the CJEU laid down the general principles of interpreting the legal notion of "judicial authority" in the FD EAW. The three cases – Cases C-452/16 PPU *(Poltorak)*, C-477/16 *(Kovalkovas)*, and C-453/16 *(Özcelik)* – are presented separately in the following news items. (TW)

➤eucrim ID=1604040

Police Service Is Not a "Judicial Authority" Within the Meaning of the FD EAW

In the case C-452/16 PPU (*Krzystof Marek Poltorak*), the CJEU had to decide whether a police service can be regarded as "issuing judicial authority" within the meaning of the FD EAW. In the case at issue, the Rechtbank Amsterdam (District Court, Amsterdam, Netherlands) had to decide on the execution of a EAW that was issued by the Rikspolisstyrelsen (National Police Board, Sweden). The EAW requested the execution of a sentence against Mr. *Poltorak*, which had been imposed by the District Court, Gothenburg, Sweden.

By way of preliminary remarks, the CJEU reiterated its standing case law that the FD EAW is:

- To replace the traditional, multilateral extradition regime;
- Designed to make the surrender of persons within the EU more effective and speedier;
- Based on the principle of mutual recognition as the cornerstone of judicial cooperation within the EU.

As a result, refusing the execution of a EAW issued by a "judicial authority" of another EU Member State is only possible in exceptional cases.

Nevertheless, the CJEU states that only a judicial authority is competent to issue a EAW and thereby implicitly recognises that this approach offers sufficient judicial protection at the stage of its issuing. Furthermore, the CJEU makes clear that the meaning of "judicial authority" requires an autonomous and uniform interpretation, which must take into account the terms of the relevant provision, its context, and the objective pursued by the FD EAW. In the view of the CJEU, the term "judicial authority" must be interpreted as referring to the Member State authorities that administer criminal justice.

The CJEU maintains that a police service, such as the Swedish police board in the case at issue, cannot be subsumed under this definition and therefore be regarded as a "judicial authority." The Court also says that a meaning also covering police services would run counter to the objectives of the FD: The FD requires that the issue of the EAW has undergone judicial approval, which only suffices to justify the high level of confidence between the Member States. In this regard, the specific organisation of police services (within the executive and the degree of autonomy they might have) is irrelevant.

The CJEU further notes that this interpretation cannot be called into question by the fact that, under Swedish law, the police service is competent only within the strict context of executing a criminal court judgment. It must be borne in mind that, in fact, the Swedish police board acts on the request of the prison service. It does not act on request of the judge who adopted the verdict and furthermore has discretion over the issuing of a EAW, so that – given these considerations – the police service cannot be regarded as a "judicial authority". (TW)

➤eucrim ID=1604041

Organs of the Executive Are Not an "Issuing Judicial Authority"

In the second case referred to the CJEU by the Rechtbank Amsterdam (Case C-477/16 PPU, *Ruslanas Kovalkovas*), it was the Lithuanian Ministry of Justice that issued a EAW against Mr. *Kovalkovas*, with a view to executing, in Lithuania, the remainder of a sentence imposed on him by the Janova Region, District Court, Lithuania. Under Lithuanian law, it is up to the Lithuanian Ministry of Justice to take the decision on issuing a EAW, mainly so as to observe the necessary conditions for its issuing and to exercise discretion as regards proportionality.

The CJEU followed the reasoning as given in the C-452/16 PPU (*Krzystof Marek Poltorak;* see news item above). Based upon the principles developed, it decided that ministries or other government organs, which are within the province of the executive, cannot be construed as the authorities that administer justice and are therefore not a "judicial authority" within the meaning of the FD EAW.

The CJEU also noted the following in this context: Although the FD EAW (Art. 7) allows the designation of central authorities, their competences are restricted to practical and administrative assistance and cannot mean substituting the competent judicial authority by a "central authority." Under Lithuanian law, the Ministry of Justice is, however, considered the authority competent to issue a EAW, having corresponding decision-making powers in the surrender procedure.

As in the *Poltorak* judgment, the CJEU ultimately rejected the argument of the Lithuanian Government that the Lithuanian Ministry of Justice acts only within the strict context of executing a judgment that has become legally binding, handed down by a criminal court following court proceedings and at the

request of that court. The CJEU pointed out in this context that the issuing of EAWs is in fact up to the Ministry. (TW)
➤eucrim ID=1604042

Prosecutor's Confirmation of EAW Previously Issued by Police is "Judicial Decision"

In the third case that was referred by the Rechtbank Amsterdam, the CJEU had to make a statement on the practice of issuing a EAW under Hungarian law (Case C-453/16 PPU, *Halil Ibrahim Özçelik*). In the present case (criminal proceedings against a Turkish national, Mr. *Halil Ibrahim Özçelik*, in Hungary), the EAW form referred to a national arrest warrant that was issued by a Hungarian police department and subsequently confirmed by a decision of the public prosecutor's office.

The CJEU clarifies that the term "arrest warrant" in Art. 8 para. 1 lit. c) FD EAW, refers only to the national arrest warrant, which is to be understood as referring to a judicial decision that is distinct from the European Arrest Warrant (cf. case C-241/15, *Bob Dogi*, eucrim 2/2016, p. 80). Thus, the question was whether the decision of a public prosecutor's office validating a national arrest warrant of the police is covered by the term "judicial decision" within the meaning of Art. 8 FD EAW. The CJEU, in answering this question, follows the same principles laid down in its judgments *Poltorak* and *Kovalkovas* on the interpretation of what is meant by "issuing judicial authority" in Art. 6 para. 1 of the FD EAW. (see above-mentioned news items).

In the light of these findings, the CJEU states that the public prosecutor's office constitutes a Member State authority responsible for administering criminal justice. It also in line with the objectives of the FD EAW if the prosecutor's office confirms a national arrest warrant previously issued by the national police services. The CJEU reiterates that confirmation by the prosecutor under Hungarian law follows judicial approval and can thus be regarded as sufficiently guaranteeing the "high level of confidence which should exist between the Member States" under the new EAW scheme. (TW)
➤eucrim ID=1604043

European Supervision Order/ Transfer of Sentenced Persons

FRA Report Assesses FDs on Transfer of Persons and Detention Alternatives

In November 2016, the EU Agency for Fundamental Rights (FRA) presented a report that evaluates the fundamental rights aspects in the implementation and application of the three Framework Decisions (FD) that aim to enhance social rehabilitation of offenders or defendants:

- FD 2008/909/JHA on the transfer of prisoners, which encourages having post-trial detainees serve their sentences "closer to home";
- FD 2008/947/JHA on probation and alternative measures, which encourages the monitoring of early releases and using alternatives to post-trial detention, e.g., because of family, work, or education;
- FD 2009/829/JHA on the European Supervision Order, which encourages using and transferring alternatives to pre-trial detention in order to permit individuals to maintain social connections in an EU Member State while awaiting trial in another EU Member State.

The report identifies the fundamental rights impacts of the three FDs as well as current barriers to applying the EU's legal instruments more effectively. Based on the research findings, the FRA offers several guidelines on the fundamental rights issues of the FDs. These relate, *inter alia*, to the following:

- The need to assess the non-application of the European Supervision Order;
- Assessing social rehabilitation on a case-by-case basis and avoiding simply sending persons back to their country of nationality;
- Strictly evaluating the individual situation in accordance with European human rights standards and jurisprudence, in particular avoiding transferring people to places with degrading detention conditions; making more easily available information on detention conditions (as well as on alternatives) in all EU Member States;
- Seeking the general reduction of detention, in particular pre-trial detention, and making full and indiscriminate use of the Framework Decisions;
- Making increased use of alternatives to detention, both pre- and post-trial; ensuring a more harmonised EU-wide approach regarding the use of detention, alternatives to detention, time of detention, etc.;
- Taking into full account persons in situations of vulnerability;
- Better involvement of and information for potential transferees;
- Ensuring that the victims have the right to information in cross-border settings.

The report concludes that the potential impact of the three Framework Decisions on fundamental rights is still underestimated. It also underscores that the instruments have not yet been fully used and that they are an important contribution towards enhancing mutual trust (TW).
➤eucrim ID=1604044

CJEU Rules on Cross-Border Reduction in Sentence

On 8 November 2016, the European Court of Justice (CJEU) gave answers in a preliminary ruling that concerned interpretation of the law governing enforcement according to the Framework Decision (FD) 2008/909/JHA on the transfer of sentenced persons. In the case at issue (Case C-554/14, *Ognyanov*), Mr. *Atanas Ognyanov*, a Bulgarian national, was sentenced in Denmark to 15 years of imprisonment for murder and aggravated robbery. After having served part of this period of imprisonment in Denmark and having worked

some while during his detention in Denmark, Mr. *Ognyanov* was transferred to Bulgaria for the further enforcement of the Danish sentence.

The question arose as to whether the Bulgarian court (Sofia City Court, Bulgaria) was able to grant a reduction of sentence for the period spent working in prison in the issuing state (Denmark). Bulgarian and Danish law follow opposing positions on this point. While Danish legislation does not permit any reduction in custodial sentence on the grounds that work was carried out during detention, Bulgarian law provides that work done in prison is to be taken into account for the purpose of reducing the length of sentence. In an interpretative ruling, the Supreme Court of Bulgaria took the view that the rule under Bulgarian law also applies in a situation in which a sentenced person has carried out work during detention in a Member State other than Bulgaria prior to being transferred to Bulgaria for the enforcement of the remainder of the sentence.

The referring Sofia City Court had doubts on whether the interpretation of the Bulgarian Supreme Court is in conflict with the FD on the transfer of prisoners, which governs the general rules on the enforcement of the sentence.

According to the CJEU, it particularly follows from Art. 17 and section (i)2.2 of the template certificate that, before the recognition of the judgment passing sentence by the executing state (here: Bulgaria) and the transfer of the sentenced person to the executing State, it falls to the issuing state (here: Denmark) to determine any reductions in sentence that pertain to the period of detention served on its territory. The issuing state alone is competent to grant a reduction in sentence for work carried out before the transfer and, where appropriate, to inform the executing state of a reduction in the certificate referred to in Art. 4 of the FD 2008/909. Consequently, the executing state cannot, retroactively, substitute its law on the enforcement of sentences and, in particular, its rules on reductions in sentence, to accommodate the law of the issuing state with respect to that part of the sentence already served by the person concerned on the territory of the issuing state.

In the present case, the Danish authorities expressly stated that Danish legislation did not permit any reduction in a custodial sentence for reasons of work carried out during the period of detention. According to the principles of mutual recognition and mutual trust that underpin FD 2008/909, the Bulgarian courts must respect this law of the issuing state (Denmark).

In addition, the Court reminded the referring Bulgarian court to give full effect to the Union law (FD 2008/909) and, if necessary, to disapply, on its own authority, the interpretation adopted by the Bulgarian Supreme Court. (TW)

➤eucrim ID=1604045

Council of Europe*

Reported by Dr. András Csúri

Specific Areas of Crime

Corruption

GRECO: Fourth Round Evaluation Report on the Czech Republic

On 2 November 2016, GRECO published its Fourth Round Evaluation Report on The Czech Republic. This latest evaluation round was launched in 2012 in order to assess how states address corruption prevention in respect of Members of Parliament (MPs), judges, and prosecutors (for more recent reports, see eucrim 3/2014, p. 83; 4/2014, pp. 104-106; 1/2015, p. 11; 2/2015, pp. 43-45; 3/2015, pp. 87-88; 1/2016, pp. 20-22; 2/2016, pp. 82-83; 3/2016, p. 134-135).

The report calls on the Czech authorities to make substantial reforms in order to strengthen the prevention of corruption among parliamentarians, judges, and prosecutors. As regards MPs, the report recommends improving the transparency of the legislative process, especially in the absence of any lobbying regulations. Rules need to be introduced on how MPs should interact with third parties seeking to influence the legislative process, and rules on parliamentarians' asset declarations need to be further amended. In this regard, GRECO welcomes the currently pending draft legislation to amend the Act on Conflicts of Interest but calls for more effective supervision and enforcement of the rules in practice.

As regards judges, GRECO recommends amending the regulation on the recruitment and career advancement of judges, ensuring in particular that decisions are based on pre-established objective criteria, notably merit.

The report welcomes the current reform process to improve the independ-

* If not stated otherwise, the news reported in the following sections cover the period 16 October 2016–15 December 2016.

ence of public prosecutors from political influence and to increase their individual accountability. In this regard, GRECO recommends a more transparent selection procedure for the appointment of the Supreme Public Prosecutor and other chief prosecutors as well as basing their recall solely on disciplinary proceedings.

For all three areas, GRECO generally recommends the adoption of codes of conduct complemented by practical measures such as awareness raising and dedicated professional trainings.

➤eucrim ID=1604046

Money Laundering

MONEYVAL: Fifth Round Evaluation Report on Hungary

On 30 November 2016, MONEYVAL published its latest report on Hungary. Although it welcomes the increasing number of investigations and prosecutions into money laundering since the country's last evaluation in 2010, the report comes to the conclusion that the fight against money laundering is not a priority objective in the country. MONEYVAL acknowledges that Hungary is aware of many money laundering threats but recommends carrying out more thorough risk assessments.

The report states that even the higher numbers of prosecutions are not commensurate with the risks and threats identified in Hungary, on the one hand, and, on the other, do not address the different types and structured schemes of money laundering. Moreover, the country's seizure/confiscation rules are not applied effectively and successfully.

On a positive note, MONEYVAL considers the use of financial intelligence and other information on money laundering and terrorist financing effective, notably through the good work by the Hungarian Financial Intelligence Unit (FIU). In addition, Hungarian authorities are seeking and providing good and timely international cooperation in investigations.

The report calls on Hungary to achieve full criminalisation of the financing of terrorism, also with respect to the financing of foreign terrorist fighters. Furthermore, law enforcement sections specialised in countering the financing of terrorism are to be established in the future.

➤eucrim ID=1604047

Council of Europe Treaty	State	Date of ratification (r), signature (s), accession (a) or approval (app)
Criminal Law Convention on Corruption (ETS No. 173)	Liechtenstein San Marino	9 December 2016 (r) 30 August 2016 (r)
Convention on Cybercrime (CETS No. 185)	Senegal Andorra	16 December 2016 (a) 16 November 2016 (r)
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189)	Senegal Andorra	16 December 2016 (a) 16 November 2016 (r)
Additional Protocol to the Criminal Law Convention on Corruption (CETS No. 191)	Liechtenstein San Marino	9 December 2016 (r) 30 August 2016 (r)
Council of Europe Convention on the Prevention of Terrorism (CETS No. 196)	Czech Republic Liechtenstein Armenia	15 November 2016 (s) 22 November 2016 (r) 30 August 2016 (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)	Azerbaijan	7 November 2016 (s)
Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201)	Estonia	22 November 2016 (r)
Convention on preventing and combating violence against women and domestic violence (CETS No. 210)	Liechtenstein	10 November 2016 (s)
Convention on the counterfeiting of medical products and similar crimes involving threats to public health (CETS No. 211)	Belgium France	1 August 2016 (r) 21 September 2016 (r)
Protocol No. 15 amending the Convention for the Protection of Human Rights and Fundamental Freedoms (CETS No. 213)	Armenia Russia	30 August 2016 (r) 19 September 2016 (s)
Council of Europe Convention against Trafficking in Human Organs (CETS No. 216)	Switzerland	10 November 2016 (s)
Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (CETS No. 217)	Czech Republic Denmark Monaco Montenegro Slovakia	15 November 2016 (s) 3 November 2016 (app) 4 October 2015 (r) 4 October 2015 (s) 14 September 2016 (s)

Compiled by Antonia Meyer

➤eucrim ID=1604048

Articles

Articles / Aufsätze

The articles in this issue focus on the EU's fourth Anti-Money Laundering Directive of May 2015 and provide a first analysis of the new proposals for its revision, presented by the Commission in July 2016 (see also eucrim 2/2016, p. 3). Anti-money laundering (AML) is not only a prevailing topic, as can be seen by the flurry of legislative action at the EU level (see the Commission's most recent proposals of 21 December 2016, reported in the news section of this issue), it also raises many fundamental questions that are indicative of the emergence of today's security law.

AML deals with the impact of *globalization*, since money launderers operate across borders and often run their transactions through sham companies and financial institutions in foreign tax havens. The EU AML Directives are also lucid examples of the *multi-level nature* of security law: they address the call to combat money laundering and terrorist financing of the UN Security Council and the Financial Action Task Force (FATF), they are implemented by national law, and they must – at the same time – respect the guarantees of EU fundamental rights and the European Convention on Human Rights. In addition, the hybrid nature of AML law illustrates the *paradigm shift of today's security law from repression to prevention*. Additional changes in this security architecture towards *privatization* are also readily apparent in the EU's legal framework for AML (starting with Directive 91/308/EEC in 1991), which calls for the increased involvement of private enterprises in crime control by means of due diligence checks on the part of the financial sector.

The authors of the following articles reflect on some of these crucial developments and fundamental changes in today's global risk society and provide in-depth analyses of (established and planned) individual provisions of the EU's AML legislation.

Prof. Dr. Dr. h.c. mult. Ulrich Sieber, Editor in Chief of eucrim,
Director Max Planck Institute for Foreign and International Criminal Law

The Fight against Money Laundering in the EU

The Framework Set by the Fourth Directive and Its Proposed Enhancements

Alexandre Met-Domestici, Ph.D.

I. Introduction

The recent terrorist attacks that struck France and Germany in the past year unfortunately demonstrated that the EU is far from being immune to the worst criminal threats. As a response, the Union adopted the European Agenda on Security[1] and an Action Plan to strengthen the fight against terrorist financing.[2] In the former, the Commission stressed the need for a new directive on combatting terrorism, while also adopting another Action Plan against the trafficking of firearms and controlling the use of explosives. The latter is part of a comprehensive approach aimed at fighting money laundering and terrorist financing.

The fight against money laundering consists in a three-pronged approach in general: At the international level, the FATF adopts recommendations.[3] The EU adopts directives implementing

FATF recommendations and sometimes adding further obligations – the most recent directive having been added in 2015 (the so-called Fourth Anti-Money Laundering Directive).[4] EU directives are then transposed into national law by the Member States. The first anti-money laundering (AML) directive was adopted in 1991.[5] It has been amended by each subsequent directive (the second directive being adopted in 2001,[6] the third directive in 2005[7] and the fourth directive in 2015[8]), all of them extending its scope and aiming at increasing the effectiveness of the fight against money laundering.

The anti-money laundering (AML) mechanism is greatly decentralized. At the national level, a Financial Intelligence Unit (FIU) can be found in each EU Member State. On the ground, it relies upon professionals (obliged entities) in charge of monitoring transactions. FIUs are small units in charge of receiving Suspicious Transaction Reports (STRs) and investigating alleged money laundering cases.

In keeping with the FATF recommendations, the EU has been implementing a risk-based approach (RBA) since the entry into force of the third AML Directive.[9] This approach departs from the former rule-based approach that lacked flexibility, requiring professionals to report transactions meeting specific quantitative criteria. The RBA further highlights the role played by obliged entities. The latter are required to assess the risk level of money laundering presented by transactions. Professionals are to apply specific kinds of Customer Due Diligence (CDD), depending on the level of risk. Should they determine that the transaction is suspicious, they are required to file an STR with their national FIU. The role played by professionals is therefore paramount to the efficiency of the anti-money laundering mechanism.

In the wake of the adoption of the fourth AML Directive and given the urge to fight terrorism financing, the Commission issued a proposal for a new directive amending Directive 2015/849 in July 2016.[10] This proposal pursues three main goals:

1) Fighting terrorist financing;
2) Increasing transparency in order to better fight money laundering;
3) Strengthening the fight against tax avoidance.[11]

Member States are furthermore required to bring forward the entry into force of the fourth AML Directive.

Which improvements can be expected from the entire reform process? This article will attempt to answer by focusing on the tweaks to the AML framework put forward by the Commission in its July 2016 proposal as well as by describing the changes brought about by the fourth AML Directive 2015/849. The article further focuses on analysing the different aspects that are followed by the objectives of the ongoing reform process: First, responding to specific threats (below II.) and second, improving cooperation in the implementation of the AML mechanism (below III.).

II. Responding to Specific Threats

The current reform – and especially the new Commission proposal of July 2016 – can be considered a response to increased threats of money laundering and terrorist financing. More precisely, the 2015 and 2016 terrorist attacks shed a light on the new ways to launder money and often to channel it to terrorists, thanks especially to the use of online services. The response relies on further broadening the scope of the AML Directive (below 1.) and places a renewed focus on high-risk third countries (below 2.).

1. Broadening the Scope of the Fourth AML Directive

In a meanwhile traditional manner, the reform follows in the footsteps of the previous directives by requiring more obliged entities to fight money laundering, expanding the category of suspected persons (below a)), and adding more predicate offences to the scope of the fourth AML Directive 2015/849 (below b)).

a) More obliged entities required to fight money laundering

A growing number of professionals are now subject to the decentralized anti-corruption mechanism. Originally, only finance professionals were required to report suspicious transactions.[12] Bankers are indeed obviously needed by money launderers willing to introduce funds stemming from criminal activities into the legal economy. Most importantly, the second AML Directive included legal professionals.[13] The current list of obliged entities therefore includes finance and legal professionals as well as auditors, accountants, real estate agents, insurance agents, money remittance officers, art dealers, and persons trading in goods where payments are made in cash for amounts of €10,000 and more.[14] Furthermore, Directive 2015/849 replaced casinos with "providers of gambling services,"[15] thus encompassing online gambling service providers. Such professionals provide "a service which involves wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services."[16]

The exemption for lawyers

A very important issue is the case of lawyers. The reporting duty imposed on them since the entry into force of the second AML Directive may be in breach of their professional obligations. The role of lawyers is indeed to represent and defend their clients in judicial proceedings. Filing STRs against them is probably far from being the best way to defend them. The obligation for them to report may furthermore fail to comply with Art. 6 ECHR – which provides for the right to a fair trial and, more specifically, the rights of the defence – and Art. 8 ECHR – which provides for the right to privacy, thus protecting correspondence exchanged between a lawyer and his client – as well as with the corresponding guarantees of the Charter of Fundamental Rights of the EU.

In order to comply with these fundamental rights, the Directive provides for exceptions. In fact, the obligation to report shall apply to legal professionals "only to the strict extent that those persons ascertain the legal position of their client, or perform the task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings."[17]

This exemption also stems from case law. In its famous *Ordre des barreaux* ruling,[18] the ECJ held that the obligation to report imposed on lawyers by the second AML Directive complied with fundamental rights. Hence, "the obligations of information and of cooperation with the authorities responsible for combating money laundering […] do not infringe the right to a fair trial."[19] The ECtHR reached a similar conclusion in its *Michaud vs. France* ruling, asserting that the reporting obligation was in line with both Art. 6 and Art 8 ECHR. Hence, "the obligation for lawyers to report suspicions […] does not constitute disproportionate interference with the professional privilege of lawyers."[20] As a matter of fact, "the obligation to report […] only concerns tasks performed by lawyers which are similar to those performed by the other professions subjected to the same obligation, and not the role they play in defending their clients,"[21] thanks to the exemption provided for in the Directive. It should also be noted that lawyers are not required to report suspicious transactions directly to the FIU. They are required to report to their local bar association, which acts as a filter and may then report to the FIU.

Virtual currencies exchange platforms and electronic money

According to the Commission's proposal of July 2016, virtual currency[22] exchange platforms and custodian virtual wallet providers should be considered as obliged entities. Whereas the former are electronic exchange offices trading virtual currencies for real currencies (dubbed *"fiat"* currencies); the latter are online service providers holding virtual currency accounts on behalf of their customers, by providing virtual wallets from which payments can be performed. In the Commission's proposal, such exchange platforms are defined as "providers engaged primarily and professionally in exchange services between virtual currencies and *fiat* currencies"[23] and wallet providers are defined as those "offering custodial services of credentials necessary to access virtual currencies."[24] Wallet providers can be considered online banks or payment institutions. Both types of entities are gateways to virtual currencies. These entities will therefore be required to apply customer due diligence, especially when performing exchanges between virtual and *fiat* currencies. Such exchanges will therefore no longer benefit from anonymity.

Prepaid instruments

It is further planned that prepaid instruments – such as prepaid credit cards – be more intensively monitored, too. The Commission thus aims at limiting the possibility to carry out anonymous payments. To this end, the threshold above which the use of anonymous prepaid cards is prohibited will be lowered from €250 to €150.[25] Professionals issuing such cards will be required to check their customers' identity and implement due diligence when the amount exceeds the new threshold provided for in the recent proposal.

Politically Exposed Persons

Directive 2015/849 broadens a very specific category of potentially suspect persons, namely politically exposed persons (PEPs). Business relationships with public officials are indeed very sensitive and may harbor increased risks of money laundering. Hence, the directive requires obliged entities to implement a specific kind of enhanced CDD.

According to the fourth AML Directive, a PEP is "a natural person who is or who has been entrusted with prominent public functions. This includes heads of State, heads of government, ministers and deputy or assistant ministers; members of parliament; members of the governing bodies of political parties; members of supreme courts, of constitutional courts or of other high-level judicial bodies; members of courts of auditors or of the boards of central banks; ambassadors, *chargés d'affaires* and high-ranking officers in the armed forces; members of the administrative, management or supervisory bodies of state-owned enterprises; directors, deputy directors and members of the board of an international organization."[26] PEP's family members and close associates are also considered as being politically exposed and therefore fall into the same category.

Quite strikingly, Directive 2015/849 adds national PEPs to the list. This seems to be a welcome addition, with a view to improving the efficiency of the AML mechanism – as can be easily inferred from some recent high-profile cases.[27] This new obligation may nonetheless be quite tricky to implement, since reporting on a senior public official in a professional's own country might prove very sensitive.

b) Predicate offences: origin of the funds being laundered

The list of predicate offences has grown with each new AML directive. Under the first anti-money laundering directive, only drug trafficking was considered a predicate offence.[28] The 2001 directive (second AML Directive) added several serious criminal offences, such as corruption and offences affecting the financial interests of the EU as well as serious crimes.[29] The third AML Directive further expanded the list of predicate offences to encompass terrorism, drug trafficking, activities of criminal organizations, fraud to the EU's financial interests, and corruption and offences punishable by a maximum prison term of at least one year. The latter category of offences provides a partially harmonized definition of serious crimes.[30] Nevertheless, the very definition of the offences themselves and the establishment of the sanctions corresponding to such predicate offences is still up to the Member States.

■ The inclusion of tax crimes

More recently, the fourth AML Directive of 2015 added tax crimes to the list of predicate offences. Whereas this inclusion is likely to provide a much needed increase in the efficiency of the fight against tax crimes at a time of huge budgetary deficits, its relevance to the fight against money laundering is debatable. It might lead to an increase in the workload of FIUs, thus failing to achieve one of the goals pursued by the risk-based approach, i.e., preventing FIUs from being overwhelmed. Moreover, the very nature of tax crimes is different from that of the other predicate offences. The money may well have originally be earned through a legal activity and therefore not originate from crime. The illegal behavior is, in fact, not paying in taxes the part of this income which is owed to the state. At any rate, tax crimes have now been included in the scope of the directive. As a consequence, however, only serious and organized tax crimes will probably be investigated by FIUs.

■ The future scenario: further criminalization of money laundering

The July 2016 proposal of the Commission does not provide for new predicate offences. However, on 25 October 2016, the Commission issued the roadmap on criminalization of money laundering[31] in which it advocates the adoption of a specific directive. The Commission thus aims at bolstering harmonization of the definition of money laundering and its predicate offences and at bridging "enforcement gaps and obstacles to information exchange and cooperation between the competent authorities in different countries."[32] To this end, the foreseen directive would further harmonize the definition of money laundering, thus expanding its scope and making it more coherent. It would also probably provide for the criminalization of self-laundering and negligent money laundering throughout the EU. Last but not least, it would offer more thorough and consistent definitions of predicate offences across Member States.

2. Focusing on High-Risk Third Countries

Enhanced CDD has to be performed where transactions involve countries with flaws in their anti-money laundering or their legal counter-terrorism mechanisms. In this respect, the Commission has to implement a requirement put forward in the fourth AML Directive, i.e., harmonizing the checks professionals are required to apply to such transactions.[33] Hence, a delegated regulation providing for a list of such countries was adopted by the Commission on 14 July 2016.[34]

Such high-risk third countries fall into three categories:[35]

1) Some countries have presented a written, high-level political commitment to address the identified deficiencies and have designed an AML action plan together with the FATF. These countries are Afghanistan, Bosnia and Herzegovina, Guyana, Lao PDR, Syria, Uganda, Vanuatu, and Yemen.[36]
2) One country has provided the same type of commitment and decided to seek assistance from the FATF, namely Iran.[37]
3) Lastly, one country represents ongoing and substantial money laundering and terrorist financing risks and has repeatedly failed to address deficiencies, namely North Korea.[38]

The list was established by applying criteria concerning the legal AML/CFT framework of each country, the competences, powers, and procedures of the country's AML institutions, and the overall effectiveness of the AML mechanism.[39] Once a country has been listed by the Commission, it can submit objections during a one-month period, which can be renewed once.[40] The Commission is to regularly review the list,[41] at least after each FATF plenary meeting.

When dealing with high-risk third countries, professionals are required to implement a specific kind of enhanced CDD comprising supplementary monitoring measures. The latter consists in thorough checks meant to reduce the risk of mon-

ey laundering as far as possible. Hence, "when dealing with natural persons or legal entities established in high-risk third countries […] obliged entities shall apply at least the following enhanced customer due diligence measures: […] (a) obtaining additional information on the customer; (b) obtaining additional information on the intended nature of the business relationship; (c) obtaining additional information on the source of funds or source of wealth of the customer; (d) obtaining information on the reasons for the intended or performed transactions; (e) obtaining the approval of senior management for establishing or continuing the business relationship; (f) conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination."[42]

It is striking that this impressive list of measures is not comprehensive; it is, in fact, a minimum requirement.[43] Member States may require professionals to apply additional mitigating measures such as "additional elements of enhanced due diligence," "enhanced relevant reporting mechanisms," and even "systematic reporting of financial transactions" or "limiting business relationships or financial transactions."[44]

III. Improving Cooperation in the Implementation of the AML Mechanism

The need for increased cooperation arising from the new ways to launder money and fund terrorism is highlighted in the current reform process. As a result, the implementation of the AML mechanism is sure to improve, thanks to the enhancement of both beneficial ownership transparency (below 1.) and the role played by FIUs (below 2.).

1. Enhancing Beneficial Ownership Transparency

Each new AML directive has strengthened the obligations imposed on obliged entities in order to increase the efficiency of the AML mechanism. A breakthrough resulted from the entry into force of the third AML Directive, thanks to the shift from the rule-based approach to the risk-based approach.[45] Whereas the rule-based approached required professionals to file STRs whenever pre-defined criteria were met, they enjoy more leeway under the risk-based approach. Obliged entities are now required to assess the level of risk presented by transactions. Based upon this assessment, they are to implement customer due diligence and to decide when to file STRs, depending on whether they deem transactions suspicious or not.

Building on this approach, the fourth AML Directive 2015/849 reinforces professionals' anti-money laundering duties by streamlining CDD and imposing stricter obligations on them. The Commission's proposal of July 2016 aims at further enhancing this mechanism. The reform process will lead to enhanced beneficial ownership transparency, thanks to improvements regarding the identification of the beneficial owner and cooperation between public authorities. These new issues are addressed in more detail in the following.

a) Identification of the beneficial owner

When implementing their anti-money laundering obligations, professionals are required to search for the origins of the funds and, most importantly, the identity of the beneficial owner. The latter is defined as "any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted."[46] The criteria meant to help professionals determine who the beneficial owners of legal entities is be streamlined.

■ Simplified Customer Due Diligence

Simplified CDD applies to situations presenting a low risk of money laundering.[47] Such situations may stem from the customer – regular customers, public authorities, companies listed in regulated markets, or financial institutions licensed in a jurisdiction complying with FATF standards. The transaction itself may be characterized by a low risk of money laundering – common transactions, such as wages or transactions where the origin of the funds is clearly known and the identity of the beneficial owner is established in a transparent manner.

In this respect, an improvement stemming from the fourth AML Directive is that non-face-to-face banking relationships are no longer systematically considered to present a high risk of money laundering. They may therefore be subject to simplified CDD. This is mainly due to the development of online banking, which does not require the client to be physically present and may not be suspicious at all.

■ Enhanced Customer Due Diligence

In situations presenting a high risk of money laundering, however, obliged entities are required to implement enhanced CDD. They have to perform extra checks and search for two key elements, namely the origin of the funds and the identity of the beneficial owner.

In order to increase transparency, the Commission stresses the need for professionals to obtain their customers' identity from an independent and reliable source and acknowledges the possibility of using electronic means of identification. Obliged

entities are thus required to check "the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means."[48]

Quite strikingly, in situations presenting a high level of risk of money laundering, the Commission's proposal of July 2016 not only requires professionals to identify such risks, but also to mitigate them. Hence, in cases of "higher risk that are identified by Member States or obliged entities, Member States shall require obliged entities to apply enhanced customer due diligence measures to manage and mitigate those risks."[49]

The fourth AML Directive provides guidance to obliged entities in their search for the beneficial owner.[50] To this end, it distinguishes two types of structures that can be used to conceal the origin of the funds and the identity of the beneficial owner, and which are therefore subject to enhanced due diligence measures. These are corporate and other legal entities, on the one hand, and trusts and other arrangements, on the other.[51]

If the customer is an incorporated company, the beneficial owner is the person controlling its capital or exercising control over its board or executives. A person who directly or indirectly controls 25% of the shares of a given company is therefore considered its beneficial owner. In its proposal, the Commission suggests lowering the beneficial ownership threshold to 10% when professionals are faced with entities that present a specific risk.[52] As far as control over the board or executives is concerned, the fourth AML Directive does not provide for a quantitative criterion. In this case, the beneficial owner is the person who ultimately controls the company, no matter what his/her official position is.

■ Applying due diligence to existing customers

The improvement brought about by the Commission's proposal is remarkable. It ensures that professionals keep monitoring transactions performed by existing customers. Existing bank accounts as well as new ones will be subject to CDD, should a risk of money laundering arise. According to the proposal, "Member States shall require that obliged entities apply the customer due diligence measures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis, or when the relevant circumstances of a customer change, or when the obliged entity has a duty in the course of the relevant calendar year, to contact the customer for the purpose of reviewing any information related to the beneficial owner(s)."[53] Existing accounts will therefore no longer be able to be used as a stealthy way to perform transactions involving money stemming from illegal activities.

■ Central registers of beneficial owners

According to Directive 2015/849, legal entities are required to hold detailed information about their beneficial owners. Hence, "corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held."[54] The Directive also creates an obligation for Member States to gather such information in national registers of beneficial ownership. Hence, "Member States shall ensure that the information" about beneficial ownership "is held in a central register in each Member State, for example a commercial register, companies register […] or a public register."[55] Such registers will also feature information on beneficial owners having at least 10% ownership in companies presenting a risk of being used for money laundering.

Building on this requirement, the Commission adds in its proposal that "Member States shall ensure that the information held in the register […] is accessible in a timely and unrestricted manner by competent authorities and FIUs, without alerting the parties to the trust concerned. They shall also ensure that obliged entities are allowed timely access to that information." Such authorities also include "tax authorities and authorities that have the function of investigating or prosecuting money laundering, associated predicate offences and terrorist financing and seizing or freezing and confiscating criminal assets."[56]

Further enhancing the requirements of Directive 2015/849, the proposal requires Member States to grant public access to the beneficial ownership registers that legal entities are required to hold. Hence, "Member States should […] allow access to beneficial ownership information in a sufficiently coherent and coordinated way, through central registers in which beneficial ownership information is set out, by establishing a clear rule of public access, so that third parties are able to ascertain […] who […] the beneficial owners of companies [are]."[57] Such broad access to central registers will provide guarantees to third parties wishing to do business with the relevant entities and allow for greater scrutiny of beneficial ownership information by civil society.

■ Trusts

Trusts provide a means of transferring assets in a discreet manner, especially when family trusts are concerned. The identity of the beneficiary of the trust may only be revealed when the trust ends. Such structures may therefore be used by money launderers. The Commission now advocates much stricter due diligence rules as regards trusts. All trusts will have to be registered in the country in which the trust is administered.[58] Beneficial ownership information about trusts will be held in

national beneficial owner registers. Quite remarkably, this requirement will be binding for all EU Member States, including those that do not recognize trusts in their national law.

The Commission's proposal clearly establishes a distinction between two types of trusts, namely trusts involved in business-like activities and other types of trusts (referring to family trusts). On the one hand, the identity of beneficial owners of "trusts which consist in any property held by or on behalf of a person carrying on a business which consists of or includes the management of trusts, and acting as trustee of a trust in the course of that business with a view to gain profit"[59] should be made public. On the other hand, access to the identity of the beneficial owners of any other trusts should be granted only to "parties holding a legitimate interest."[60] Applicants will therefore have to demonstrate a legitimate interest in order to be granted access to information related to non-profit-making trusts.[61] Obliged entities will, however, be systematically granted access to such information, no matter what type of trust is concerned.[62]

Most interestingly, the proposal adds a provision aimed at protecting the safety of beneficial owners: "in exceptional circumstances laid down in national law, where the access to" information about his/her identity "would expose the beneficial owner to the risk of fraud, kidnapping, blackmail, violence or intimidation, or where the beneficial owner is a minor or otherwise incapable, Member States may provide for an exemption from such access to all of part of the information on the beneficial ownership on a case-by-case basis."[63]

■ National registers of bank account holders

Such central registers are to be established: "Member States shall put in place automated centralized mechanisms, such as central registries or centralized mechanisms, which allow the identification, in a timely manner, of any natural or legal persons holding or controlling payment accounts […] and bank accounts held by a credit institution within their territory."[64] Moreover, "Member States shall ensure that the information held in the centralized mechanisms […] is directly accessible, at national level, to FIUs and competent authorities for fulfilling their obligations under"[65] the fourth Directive. Member States will have to create an automated central mechanism enabling investigators to match an account with the corresponding identity of its holder.

b) Cooperation between public authorities

The Commission aims at enhancing cooperation both between national authorities and between Member States.

■ Cooperation between national authorities

The proposal of July 2016 requires Member States to facilitate cooperation between the various authorities involved in the fight against money laundering, terrorist financing, and tax avoidance. Hence, "Member States shall not prohibit or place unreasonable or unduly restrictive conditions on the exchange of information or assistance between competent authorities. In particular, Member States shall ensure that competent authorities do not refuse a request for assistance on the grounds that
(a) the request is also considered to involve tax matters;
(b) national legislation requires obliged entities to maintain secrecy or confidentiality, except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies;
(c) there is an inquiry, investigation or proceeding underway in the requested Member State, unless the assistance would impede this inquiry, investigation or proceeding;
(d) the nature or status of the requesting counterpart authority is different from that of requested competent authority."[66]
The latter is a very welcome addition. It aims at overcoming obstacles to cooperation stemming from the different natures of FIUs. The proposal requires Member States to facilitate such cooperation even though some FIUs are judicial bodies, whereas others are administrative or police FIUs.

Cooperation between national authorities should also apply to sharing the identity of beneficial owners of trusts. Hence, "Member States should ensure that their authority in charge of the register set up for the beneficial ownership information of trusts cooperates with its counterparts in other Member States, sharing information concerning trusts governed by the law of the first Member State and administered in another Member State."[67]

■ Cooperation between Member States

According to the proposal, cooperation between Member States will be enhanced, thanks to the interconnection of registers. Bank account holder registers and especially beneficial ownership registers held by national authorities will be interconnected, thanks to a designated European platform, thus allowing for the fast and efficient exchange of information between Member States. Hence, "Member States shall ensure that the central registers […] are interconnected via the European Central Platform."[68]

2. Enhancing the Role of FIUs

As mentioned above, the central role played by FIUs in implementing the AML mechanism is another important issue

in the framework of improving cooperation. The role of the FIUs will be enhanced by the Commission's proposal, thanks to both the strengthening of their powers and their increased cooperation efforts.

a) Strengthening the powers of FIUs

As a welcome improvement, the units will be granted the power to increase the scope of information available. FIUs will thus be able to request any information, even when no STR has been filed. Hence, "in the context of its functions, each FIU shall be able to obtain from any obliged entity information […] even if such obliged entity did not file a prior report."[69] This new power granted to FIUs is worth taking note of. They will thus be allowed to access information directly, without relying exclusively on obliged entities' diligence. The speed and efficiency of investigations should therefore increase. Such a change is a remarkable contribution to strengthening the fight against terrorist financing. The limited amount of money involved and the effort made by terrorists in order to stay undercover sometimes make it hard for professionals to realize the suspicious nature of some transactions.

Most importantly, the units will be granted access to central bank and payment account registers as well as to central data retrieval systems. Member States will be required to establish such mechanisms in order to facilitate sharing the identity of bank account holders. Cooperation between FIUs and other authorities is also to improve. To this end, "Member States shall ensure that policy makers, the FIUs, supervisors and other competent authorities involved in AML/CFT, such as tax authorities, have effective mechanisms to enable them to cooperate and coordinate domestically."[70]

b) Increasing cooperation between FIUs

FIUs are to increase their cooperation, which has already been facilitated by the network "FIU.net" and the Egmont group.[71] The latter is an international network of FIUs whose goal is to foster cooperation and share best practices. Such cooperation encompasses areas such as information exchange, training and sharing of expertise.

Moreover, Decision 2000/642 already provides for cooperation between FIUs at the European level.[72] However, the CJEU acknowledged the shortcomings of the mechanism set up by this decision in its famous *Jyske Bank* ruling.[73] Hence, this "mechanism for cooperation between FIUs suffers from certain deficiencies," according to the CJEU.[74] The Court further stated that decision indeed "provides for important exceptions to the requirement for the requested FIU to forward the information requested to the applicant FIU."[75] Moreover, "Decision 2000/642 does not lay down a time-limit for information to be forwarded by the requested FIU, nor does it provide for sanctions in case of unjustified refusal on the part of the requested FIU to forward the requested information."[76]

In its proposal, the Commission aims at further fostering practical cooperation in investigations. As a result, "Member States shall ensure that FIUs exchange, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by the FIU related to money laundering or terrorist financing […], regardless of the type of associated predicate offences and even if the type of associated predicate offences is not identified at the time of the exchange."[77]

Diligence is also expected from FIUs: "the requested FIU's prior consent to disseminate information to competent authorities" shall be "granted promptly and to the largest extent possible […] The requested FIU shall not refuse its consent to such dissemination unless it would fall beyond the scope of its AML/CFT provisions, could lead to impairment of a criminal investigation, would be clearly disproportionate […], or would otherwise not be in accordance with fundamental principles of national law […] Any such refusal to grant consent shall be appropriately explained."[78] Thanks to this information exchange mechanism, the Commission's proposal also takes a small step towards the harmonization of tax offences. It thus provides that "differences between national definitions of tax crimes shall not impede the ability of FIUs to provide assistance to another FIU and shall not limit the exchange, dissemination and the use of information" pursuant to money laundering investigations.[79]

IV. Conclusions

The current reform provides a response to specific threats of money laundering and terrorist financing as well as means to step up cooperation. In this respect, both the fourth AML Directive 2015/849 and the new Commission's proposal of July 2016 provide for significant changes to the AML framework. The proposal demonstrates a strong emphasis on the cooperation and sharing of information, both at the national and European levels.

These are welcome improvements. However, there is still a need for greater cooperation in order to respond to global criminal threats, especially terrorism. To this end, the creation of a European Financial Intelligence Unit, above and beyond the network of national FIUs, could be a major asset. Such an "EU FIU" would be in charge of receiving STRs, analyzing

them, and disseminating the results to the competent national bodies. Its creation nonetheless remains a long-term project, even though it is being discussed in the impact assessment of the proposal.[80]

Another noteworthy project, which is currently being debated at the Council, is the creation of a European Public Prosecutor Office (EPPO).[81] Creating such a European Prosecutor – whose jurisdiction would be limited to offences affecting the EU's financial interests – may well achieve a breakthrough on the road to strengthening criminal justice throughout the Union. Adding money laundering and terrorism to the EEPO's jurisdiction would be an even greater step forward.

Alexandre Met-Domestici

Associate Professor – Maître de Conférences – Jean Monnet Chair on «The EU's Role in the Fight against Economic Crime»; CHERPA; Sciences-Po, Aix-en-Provence, France

1 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – the European Agenda on Security, COM (2015) 185 final, 28 April 2015.
2 European Commission, Communication from the Commission to the European Parliament and the Council on an Action Plan for Strengthening the Fight against Terrorist Financing, COM (2016) 50/2, 2 February 2016.
3 The FATF comprises 37 Member States: all EU Member States, Argentina, Australia, Brazil, Canada, China, Hong Kong, Iceland, India, Japan, Malaysia, Russia, Singapore, South Africa, South Korea, Switzerland, Turkey and the USA. There are also associate members and observer organizations.
4 Directive (EU) 2015/849 of the European Parliament and the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 541/73, 5 June 2016.
5 Council Directive 91/308/EEC on the Prevention of the Use of the Financial System for the Purpose of Money Laundering, O.J. L 166, 28 June 1991.
6 Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on Prevention of the Use of the Financial System for the Purpose of Money Laundering, O.J. L 344, 28 December 2001.
7 Directive 2005/60 EC of the European Parliament and the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing, O.J. L 309/15, 25 November 2005.
8 Directive 2015/849.
9 Directive 2005/60.
10 European Commission, Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and amending Directive 2009/101/EC, COM (2016) 450 final, 5 July 2016. See also eucrim 2/2016, p. 73.
11 European Commission, Commission strengthens transparency rules to tackle terrorism financing, tax avoidance and money laundering, Press Release, IP/16/2380, Strasbourg, 5 July 2016.
12 Directive 91/308/EEC, Art. 1.
13 Directive 2001/97/EC, Art. 1, point 2.
14 Directive 2015/849, Art. 2, point 1, Par. 3.
15 Directive 2015/849, Art. 2, point 1, Par. 3 (f).
16 Directive 2015/849, Art. 3, Par. 14.
17 Directive, 2015/849, Art. 14, Par. 4.
18 ECJ, Grand Chamber, case C-305/05, *Ordre des barreaux francophones et germanophones, Ordre français des avocats du barreau de Bruxelles, Ordre des barreaux flamands, Ordre néerlandais des avocats du barreau de Bruxelles v. Conseil des Ministres*, 26 June 2007.
19 ECJ, Grand Chamber, case C-305/05, *Ordre des barreaux …*, § 37.
20 ECtHR, appl. no. 12323/11, *Michaud vs. France*, 6 December 2012, § 161.
21 ECtHR, *Michaud vs. France*, § 128.
22 A virtual currency is "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a *fiat* currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically," COM (2016) 450, Art. 1, point 2 (c).
23 COM (2016) 450, Art. 1, point 1 (g).
24 COM (2016) 450, Art. 1, point 1 (h).
25 COM (2016) 450, Art. 1, point 3 (a).
26 Directive 2015/849, Art. 3, Par. 9.
27 For instance, as regards France, read *Fraude fiscale : trois ans de prison ferme requis contre l'ex-ministre Jérôme Cahuzac*, Le Monde, 14 September 2016, http://www.lemonde.fr/police-justice/article/2016/09/14/requisitoires-attendus-au-proces-cahuzac-pour-fraude-fiscale_4997496_1653578.html
28 Council Directive 91/308/EEC on the Prevention of the Use of the Financial System for the Purpose of Money Laundering, O.J. L 166, 28 June 1991, Art. 1.
29 Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on Prevention of the Use of the Financial System for the Purpose of Money Laundering, O.J. L 344, 28 December 2001, Art. 1.
30 Actual harmonization is possible on the basis of Art. 83 TFEU, which provides for the possibility for the European Parliament and the Council to adopt harmonized substantial rules of criminal law in order to "establish minimum rules concerning the definition of criminal offences and sanctions in the area of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis."
31 European Commission, Roadmap – Proposal for a Directive on the Criminalization of Money Laundering, 25 October 2016.
32 European Commission, Roadmap, 25 October 2016.
33 Directive 2015/849, Art. 9.
34 European Commission, Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 by identifying High-Risk Third Countries with Strategic Deficiencies, C (2016) 4180 final, 14 July 2016, O.J. L 254 20 September 2016. See also eucrim 2/2016, p. 73.
35 Delegated Regulation (EU) 2016/1675, Annex 1.
36 Delegated Regulation (EU) 2016/1675, Recital 9.
37 Delegated Regulation (EU) 2016/1675, Recital 10.
38 Delegated Regulation (EU) 2016/1675, Recital 11.
39 Directive 2015/849, Art. 9, point 2 (a), (b) and (c) and Delegated Regulation, Recital 4.
40 Directive 2015/849, Art. 9, point 3 and Delegated Regulation, Recital 12.
41 Delegated Regulation (EU) 2016/1675, Recital 13.
42 COM (2016) 450, Art. 1, point 7.
43 COM (2016) 450, Art. 1, point 7.
44 COM (2016) 450, Art. 1, point 7.
45 Directive 2005/60 EC.
46 Directive 2015/849, Art. 3, point 6.
47 Directive 2015/849, Art. 15, point 2.
48 COM (2016) 450, Art. 1, point 4 (a).
49 COM (2016) 450, Art. 1, point 6.
50 Directive 2015/849, Art. 3, point 6 (a).
51 COM (2016) 450, Art. 1, point 10.
52 COM (2016) 450, Art. 1, point 2.
53 COM (2016) 450, Art. 1, point 5.
54 Directive 2015/849, Art. 30, point 1.
55 Directive 2015/849, Art. 30, point 3.
56 COM (2016) 450, Art. 1, Par. 10
57 COM (2016) 450, Recital 25.

58 COM (2016) 450, Art. 1, point 10 (b).
59 COM (2016) 450, Recital 34.
60 COM (2016) 450, Recital 35.
61 COM (2016) 450, Art. 1, point 10 (d).
62 COM (2016) 450, Art. 1, point 10 (c).
63 COM (2016) 450, Art. 1, point 10.
64 COM (2016) 450, Art. 1, Par. 12.
65 COM (2016) 450, Art. 1, Par. 12.
66 COM (2016) 450, Art. 1, Par. 18.
67 COM (2016) 450, Recital 36.
68 COM (2016) 450, Art. 1, Par. 10.
69 COM (2016) 450, Art. 1, Par. 11.
70 COM (2016) 450, Art. 1, Par. 17.
71 http://www.egmontgroup.org.
72 Commission Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, JOUE N° L 271/4, 24 October 2000.
73 CJEU, case N° C-212/11, *Jyske Bank Gibraltar Ltd vs. Administracion del Estato*, 25 April 2013.
74 CJEU, case N° C-212/11, *Jyske Bank Gibraltar, §* 73.
75 CJEU, case N° C-212/11, *Jyske Bank Gibraltar, §* 74.
76 CJEU, case N° C-212/11, *Jyske Bank Gibraltar* § 76.
77 COM (2016) 450, Art. 1, Par. 19.
78 COM (2016) 450, Art. 1, Par. 20.
79 COM (2016) 450, Art. 1, Par. 21.
80 COM (2016) 450, Impact Assessment.
81 European Commission, Proposal for a Council Regulation on the Establishment of the European Public Prosecutor's Office, COM (2013) 534 final, 17 July 2013.

Recent Developments in EU Anti-Money Laundering

Some Critical Observations

Dr. Benjamin Vogel and Jean-Baptiste Maillart

Since the adoption of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances in 1988,[1] many efforts have been made to strengthen the anti-money laundering (AML) regime at the international level and also within the European Union, where several directives to this effect have been adopted since 1991.[2] The fourth and latest EU Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorism financing (4AMLD) was adopted by the European Parliament and the Council in May 2015 in order to reinforce the efficacy of the European Union's action in this area,[3] thereby to a large extent following the Recommendations of the Financial Action Task Force (FATF), which had been revised in 2012.[4] In response to recent terrorist attacks across Europe, the European Commission then published an action plan in February 2016 to "further step up the fight against the financing of terrorism."[5] This action plan sets out a series of measures pertaining directly to money laundering and terrorism financing, which eventually led to the publication (on 5 July 2016) of a Proposal for a Directive amending Directive 2015/849[6] and furthermore to the Roadmap of 25 October 2016 aiming at harmonising the criminalisation of money laundering.[7] This article will assess some of the most innovative measures adopted in the 4AMLD or proposed in 2016 by the European Commission. It will address the enlargement of the scope of the anti-money laundering/counter-terrorism financing (AML/CTF) regime, the proposed rules for high-risk third countries, the creation of national beneficial ownership registries, the proposed enhancement of the powers of Financial Intelligence Units (FIUs), and finally the envisaged harmonisation of the criminal offence of money laundering. Although some measures can be welcomed, others must be subjected to a more nuanced appraisal.

I. Scope of the AML Regime

The 4AMLD further strengthened the European AML framework. Notably, the scope of obliged entities has been extended to sectors that are particularly vulnerable to money laundering. The Directive rightly[8] addressed the risks relating to gambling services by extending its applicability to all providers of such services[9] and not only to casinos as provided for by the 2005 third Anti-Money Laundering Directive (3AMLD).[10] Moreover, the threshold for cash transactions above which persons trading in goods qualify as obliged entities has been reduced from €15,000 EUR to €10,000.[11]

However, the 4AMLD still contains important *lacunae* with respect to the scope of obliged entities. Some economic activities with high money laundering potential have indeed not yet been included in the EU AML framework. In particular, virtual currency exchange platforms (e.g., Bitcoin, Litecoin, Liberty Reserve)[12] and custodial wallet providers are not covered by

the 4AMLD.[13] Yet, as the European Commission points out, "[t]ransactions with virtual currencies benefit from a higher degree of anonymity than classical financial fund transfers"[14] and therefore entail a money laundering risk, especially with respect to the concealment phase.[15] This risk is amplified by the "opaque and technologically complex nature of the industry, and the lack of regulatory safeguards."[16] Hence, the Commission proposes designating "all gatekeepers that control access to virtual currencies, in particular exchange platforms and wallet providers"[17] as obliged entities under the 4AMLD, therefore subjecting them to appropriate customer due diligence obligations (CDD) and reporting obligations.[18] Such an extension of the scope of obliged entities constitutes a potentially[19] important improvement. In contrast, it seems unsatisfactory that neither the 4AMLD nor the current proposal addresses the presumably high money laundering risk in the construction sector, especially with regard to property developers.[20] Furthermore, the 4AMLD remains somewhat ambiguous on whether letting agents are considered obliged entities.[21] Finally, the Commission proposes new rules for payment cards, which are rather questionable in terms of their effectiveness, by lowering the threshold from 250 EUR to 150 EUR for non-reloadable pre-paid instruments to which customer due diligence measures apply. It is indeed hard to see how this rather modest reduction of the threshold amount could significantly affect the use of such cards for money laundering or terrorism financing.

II. Enhanced Customer Due Diligence Obligations

The 4AMLD provides for enhanced customer due diligence (ECDD) for cases that represent a higher risk of money laundering or terrorism financing. However, with the exception of cross-border correspondent relationships of credit institutions with a third country,[22] and transactions or business relationships with politically exposed persons (PEPs),[23] the Directive does not specify which ECDD measures the obliged entities are required to undertake in order to adequately respond to the qualified risk. With regard to dealing with entities in high-risk third countries, the Commission now fears that the lack of harmonisation of such measures could lead to forum-shopping, depending on the stringency of individual Member States' legal frameworks.[24] In its 2016 proposal, it therefore proposes the insertion of a cumulative list of ECDD that obliged entities would need to apply to transactions with high-risk third countries.[25]

While concerns regarding deficient harmonisation and forum-shopping are pertinent, it should be noted that their relevance is not confined to ECDD with respect to high-risk third countries. Similar concerns could also be directed at standard AML CDD. The 2012 FATF Recommendations and the 4AMLD have reinforced the "risk-based" approach to CDD, thereby avoiding ineffective rigidity (the so-called "tick-the-box approach"). However, the risk-based approach does effectively allow for considerable flexibility on the part of national legislators and obliged entities in the imposition and application of AML/CTF measures.[26] Such flexibility not only creates problems with regard to the effective harmonisation of AML measures. Too much leeway in obliged entities' risk assessment is also problematic with regard to the rights of customers, as it can undermine their contractual rights vis-à-vis the obliged entity. By citing their individual risk policy, obliged entities will often be provided with a relatively easy way out of their contractual obligations, even in the absence of an objectively substantiated AML/CTF risk. This gives rise not least to the risk of illegitimate discriminatory business practices. One might therefore argue that the Commission's attempt to provide clearer rules for ECDD signals a more general need to recalibrate and further specify the risk-based approach to CDD. In this respect, however, the 2016 proposal also suggests that overly strong reliance on a CDD "rules-based" approach will not necessarily enhance the effectiveness of AML efforts. The proposed provision is very burdensome and cost-intensive and might therefore invite frequent "de-risking" by obliged entities, potentially pushing business with high-risk third countries into the hands of less regulated or illicit operators and thereby making the competent authorities lose access to valuable financial intelligence. While the Commission's proposal repeats the entirety of the FATF Recommendation's ECDD measures,[27] one should note that, according to the FATF, its list of measures constitutes "*examples* of enhanced CDD measures that could be applied for higher risk business relationships,"[28] while, for high-risk third country transactions, the Commission proposal now states that obliged entities "shall apply *at least all* the [FATF] enhanced customer due diligence measures" (emphasis added).[29] Although such a wholesale adoption of the FATF ECDD measures might be justified in view of the special risk posed by high-risk third countries, in other constellations of ECDD, a blanket reference to the FATF's list would hardly ensure reasonable risk management. One can only hope that future action by the European legislator and guidelines by European supervisory authorities will lead to greater refinement of ECDD measures.

III. Beneficial Ownership of Legal Entities and Trusts

In line with the FATF Recommendations,[30] the 4AMLD obliges Member States to "ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership,"[31] and to "ensure that this information

is held in a central registry in each Member State."[32] Similar obligations are required for the trustees of any express trust governed under the law of a Member State.[33] By ensuring the transparency of financial flows involving legal entities and trusts, such beneficial ownership registries (BORs) are arguably the most innovative element of the 4AMLD, but also one of its most controversial elements. The current framework raises questions, particularly with regard to its effectiveness and the adequate protection of personal data.

First, regarding the framework's effectiveness, it is important to note that neither the 4AMLD nor the Commission's new proposal specifies a mechanism that would ensure the accuracy of BORs' content. This is worrisome, as legal entities involved in money laundering or terrorism financing are likely to actively conceal their backers. Without an effective verification mechanism, BORs will likely lead to serious infringements of the data protection rights of legitimate economic actors without delivering a tangible benefit over illegitimate ones. Incidentally, the Directive does not oblige Member States to provide for sanctions in the event that legal entities or trustees provide the authorities with inaccurate beneficial ownership information. Second, the Commission's proposal amplifies data protection issues regarding access to BORs. Besides access by competent authorities, FIUs, and obliged entities for the purpose of CDD, the 4AMLD grants BORs access to any person that can demonstrate a "legitimate interest" in obtaining the beneficial ownership information of corporate and other legal entities. In this respect, the Commission now intends to go a significant step further. It proposes an amendment to Directive 2009/101/EC[34] requiring corporate and other legal entities as well as such trusts that are conducting a business[35] to disclose certain beneficial ownership information, thereby allowing for the identification of the beneficial owners as well as the nature and extent of the beneficial interest held. This information would be publicly available, in this way forgoing the hitherto existing "legitimate interest" access requirement.[36] The proposed amendment to Directive 2009/101/EC explains that such publication of beneficial ownership information is meant to enable third parties and civil society at large to contribute to the preventive efforts through enhanced public scrutiny. While the proposal's objective is laudable, one must question whether data protection implications have been sufficiently addressed. The 4AMLD[37] and the proposed amendment to Directive 2009/101/EC[38] both acknowledge the potential for abuse of beneficial ownership information – explicitly mentioning the dangers of fraud, kidnapping, blackmail, violence or intimidation − and therefore allow for exemptions from making this information public on a case-by-case basis in exceptional circumstances. To ensure effective and proportionate harmonisation throughout the Union, one wishes that the European legislator would specify what these circumstances are. Furthermore, the 4AMLD implies that access by obliged entities to BORs can be limited (as only competent authorities and FIUs are granted access "without any restriction"),[39] thereby avoiding an excessive dissemination of details of a beneficial interest. Here too, clarification regarding the extent of possible restriction to access would allow for a more coherent harmonisation and thereby a strengthening of BORs.

IV. Enhanced Powers of FIUs

The European Commission's 2016 proposal also aims at enhancing the powers of FIUs in two respects. First, it proposes to significantly expand the data-gathering powers of FIUs, authorising them to request data "from any obliged entity information […] even if such obliged entity did not file a prior [suspicious transaction] report".[40] Under the 4AMLD, access by FIUs to information held by obliged entities is indeed limited, as FIUs are only authorised to obtain "additional information."[41] Consequently, as the Commission points out, "[t]hat information is currently limited in certain Member States by the requirement [of] a prior suspicious transaction report."[42] This new power would certainly help FIUs to improve their analytical capacity. Insofar as the Commission refers to "the latest international standards"[43] to justify this reform, however, it must be noted that the current FATF Recommendations still refer to FIUs' power to obtain "*additional* information from reporting entities" (emphasis added).[44] With regard to other "commercially held data," the FATF requires FIU access to this data only "where appropriate."[45] Given that the Commission's 2016 proposal entails the potential to transform FIUs into investigative bodies in their own right, it seems crucial to further specify the FIUs' new investigative competence, in particular by clarifying when a request for information is appropriate. Otherwise, the new power will not only cause serious data protection problems, but likely lead to great incoherence in the way in which different Member States define its scope.

Second, the Commission's proposal envisages the creation of an automated central mechanism – such as a central registry or an electronic data retrieval system – at the Member State level, allowing for the swift identification of bank and payment account holders by the competent authorities, including FIUs. Up until now, the 4AMLD had only "recommended" such an instrument, but refrained from making it mandatory.[46] As the Commission rightly states, the new mechanism would undoubtedly "lead to a faster detection – both nationally and internationally – of suspicious ML/TF transactions, and improve preventive action."[47] However, although the content of the envisaged central mechanism is currently very limited (including the customer-account holder and IBAN number), the

Commission appears to anticipate that some Member States might go beyond this minimum and feed the mechanisms with other information they consider necessary for the prevention of money laundering and terrorism financing. Given that the proposal requires Member States to ensure that FIUs are able to provide information contained in the mechanism to any other FIU – i.e., to ensure a cross-border exchange of the information – one should caution against too broad a content of the mechanism. This might otherwise create data protection problems in other Member States and thereby complicate cross-border cooperation.[48]

V. Criminalisation of Money Laundering

On 25 October 2016, the European Commission published a roadmap on a proposal for a Directive on the Criminalisation of Money Laundering, which would be the very first directive of its kind, since the European Union has so far focused only on preventive measures in this respect. The aim of the proposal is to "introduce minimum rules regarding the criminal offence of money laundering and to approximate sanctions."[49] According to the Commission, "[t]he current criminal framework against money laundering across Europe is neither comprehensive nor sufficiently coherent to be fully effective, with the consequence of enforcement gaps and obstacles to information exchange and cooperation between the competent authorities in different countries."[50] The Commission assumes that "the current situation does not ensure effective enforcement or adequate deterrence," and that an "often low level of sanctions" and "low prosecution rates" contribute to a risk of "forum shopping" in that criminals are "carrying out financial transactions where they perceive anti-money laundering measures to be weakest."[51]

So far, it is not yet clear what exact shape harmonisation would take. It will be important to see how the Commission addresses a number of issues, as the offence of money laundering does indeed raise a number of difficult questions that can even pose challenges for some Member States' constitutional law. To begin with, one could contemplate whether or to what extent self-laundering (i.e., laundering of the proceeds of one's own criminal activity) is covered. Not least due to the privilege against self-incrimination, some legal orders find it difficult to extend the offence's scope accordingly. In order to address such concerns, any harmonisation at least requires a sufficiently delimited statutory definition of self-laundering.[52] Furthermore, drafters of the Directive need to thoroughly think about the adequate scope of predicate offences (i.e., those offences resulting in generation of the criminal proceeds). While the FATF recommends that "[c]ountries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences,"[53] the European legislator will have to address both proportionality concerns and unwanted practical consequences of an overly broad catalogue of predicate offences. Given that the offence of money laundering serves as the bedrock of and overreaching reference point for the preventive anti-money laundering framework (especially CDD), the drafters must take into account the resulting knock-on effects on obliged entities, in particular the overburdening effect and resulting phenomenon of "de-risking."[54] The purported current ineffectiveness of criminal law enforcement should thus only be one of several important considerations. Finally, as regards the *mens rea* element, the Commission may be tempted to go beyond the intent requirement (as included in the 1988 Vienna Convention[55] and the 2000 United Nations Convention against Transnational Organized Crime),[56] and also criminalise the negligent commission of money laundering, as optionally provided for by the 2005 Council of Europe Convention.[57] While an offence of negligence might alleviate the prosecutor's evidential burden, it is not entirely clear whether this would improve the effectiveness of anti-money laundering. Negligence would not only often be treated as relatively little blame-worthy, consuming scarce resources of prosecuting agencies without ultimately leading to the imposition of deterrent sanctions. One also needs to question the impact that the threat of criminal punishment might have on obliged entities' willingness to cooperate extensively with the authorities in the fight against money laundering, given that simple mistakes in compliance practice might make them criminally liable. If the legislator is seeking to enhance public-private partnerships in AML/CTF, a broad threat of punishment might not offer the most constructive framework for dialogue. Consequently, instead of criminalizing the negligent handling of proceeds of crime, it would better to focus legislative attention and enforcement practice on breaches of obliged entities' preventive duties, especially their reporting requirements. Priority should thus be given to an effective implementation of the 4AMLD's existing sanctions provisions.[58]

1 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 20 December 1988.
2 The first one was Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.
3 See the Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and the Proposal for a regulation on information accompanying transfers of funds to secure "due traceability" of these transfers, both adopted by the European Commission on 5 February 2013.
4 FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, updated October 2016.
5 Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing, COM/2016/050 final, 2 February 2016.

Dr. Benjamin Vogel
Senior Researcher at the Max Planck Institute for Foreign and International Criminal Law, Freiburg i.Br.

Jean-Baptiste Maillart
Ph.D. Candidate at the University of Geneva, Researcher at the Max Planck Institute for Foreign and International Criminal Law, Freiburg i.Br.

6 Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, COM/2016/450 final, 5 July 2016.
7 Proposal for a Directive on criminalisation of money laundering, Roadmap, 25 October 2016.
8 See, e.g., 4AMLD, recital 21: "The use of gambling sector services to launder the proceeds of criminal activity is of concern".
9 4AMLD, article 2(1)(3)(f). However, according to article 2(2), Member States can remove these providers – with the exception of casinos – partially or completely from the list of obliged entities if a low money laundering risk is evidenced.
10 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, article 2(1)(3)(f).
11 4AMLD, article 2(1)(3)(e). For comparison, see 3AMLD, article 2(1)(3)(e).
12 637 crypto-currencies exist at the moment (www.coinmarketcap.com, last accessed on 7 December 2016).
13 On the vulnerability of virtual currency exchange platforms and custodial wallet providers to money laundering, see, e.g., FATF (2014), *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*.
14 *Supra* note 6, p. 12.
15 Money laundering is traditionally understood as a threefold process: 1) Concealment of the criminal proceeds in the financial system; 2) Conversion of the criminal proceeds, the purpose of which is to further conceal the origin and ownership of the initial criminal money by transferring it several times; 3) Integration into the formal or legal economy. See, e.g., R. Booth, S. Farrell, G. Bastable & N. Yeo, *Money Laundering: Law and Regulation*, Oxford, 2011, pp. 3–4; R. Durieu, *Rethinking Money Laundering and Financing of Terrorism in International Law: Towards a New Global Legal Order*, Leiden, Boston, 2013, pp. 240–262.
16 *Supra* note 6, p. 12.
17 *Ibid.*, p. 7.
18 The Commission proposes to extend article 2(1)(3) 4AMLD to cover "(g) providers engaged primarily and professionally in exchange services between virtual currencies and fiat currencies" and "(h) wallet providers offering custodial services of credentials necessary to access virtual currencies". For legal certainty reasons, a definition of "virtual currency" is also proposed in article 3(c)(18): "(18) 'virtual currencies' means a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically".
19 One must note, that, for the time being, the relevance of virtual currencies for money laundering or terrorism financing remains limited. However, this situation is likely to change once virtual currencies are more increasingly used in the legitimate economy. See, e.g., HM Treasury/Home Office, *UK national risk assessment of money laundering and terrorism financing*, London, October 2015, p. 79.
20 Cf. K. Bussmann, *Dark figure study on the prevalence of money laundering in Germany and the risks of money laundering in individual economic sectors*, Summary, Halle, August 2015, p. 9.
21 Whilst article 2(1)(3)(d) 4AMLD only mentions "estate agents", it is conceivable that this includes letting agents as mentioned in recital 8. However, a recent draft resolution by Members of the European Parliament recommends amending article 2(1)(3)(d) to explicitly include "letting agents" (see draft European Parliament legislative resolution on the proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849, 7 November 2016).
22 4AMLD, article 19.
23 4AMLD, article 20. It is worth pointing out that the 4AMLD has extended the requirement to apply ECDD with respect to domestic PEPs and PEPs of international organisations. The 3AMLD had envisaged this requirement only with respect to foreign PEPs, i.e., PEPs who reside in another Member State or in a third country (see 3AMLD, article 13)
24 *Supra* note 6, p. 15.
25 *Ibid.*, pp. 31–32. Note that article 18(4) of the 4AMLD already provides that the European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority ("ESAs") shall issue guidelines addressed to competent authorities and to credit institutions and financial institutions on the risk factors to be taken into consideration and the measures to be taken in situations where ECDD are appropriate. However, it appears that such guidelines are judged as insufficient in ensuring comprehensive harmonisation of ECDD throughout the Union.
26 See 4AMLD, article 13(2).
27 Cf. FATF Recommendations 2012, p. 67.
28 *Ibid.*
29 *Supra* note 6, p. 31.
30 *Supra* note 4.
31 4AMLD, article 30(1).
32 4AMLD, article 30(3).
33 4AMLD, article 31(1) and (4). Note that article 31(4) only applies to trusts that generate tax consequences.
34 Directive 2009/101/EC of the European Parliament and the Council of 16 September 2009 on the coordination of safeguards for the protection of the interests of members and third parties, which Member States require of companies within the meaning of the second paragraph of article 48 of the Treaty, with a view to making such safeguards equivalent.
35 *Supra* note 6, p. 39.
36 *Ibid*, p. 40.
37 4AMLD, article 30(9).
38 *Supra* note 6, p. 40.
39 4AMLD, article 30(5).
40 *Supra* note 6, p. 35.
41 4AMLD, article 32(3).
42 *Supra* note 6, p. 14.
43 *Ibid.*, p. 13.
44 *Supra* note 4, p. 98
45 *Ibid.*
46 4AMLD, recital 57.
47 *Supra* note 6, p. 14.
48 The Commission merely provides that "such registries should store the minimum data necessary to the performance of AML/CFT investigations, the concerned data subjects should be informed that their data are recorded and accessible by FIUs and are given a contact point for exercising their rights of access and rectification" (*supra* note 6, p. 15).
49 *Supra* note 7.
50 *Ibid.*
51 *Ibid.*
52 For an example of such delimitation, cf. the new Section 261 para. 9 of the German Penal Code: according to this provision, any party to the commission of the predicate offence is punishable for money laundering only when he distributes the proceeds to others and, in doing so, conceals their unlawful origin.
53 *Supra* note 4, see Recommendation 1.
54 See *supra*.
55 *Supra* note 1, article 3(2).
56 United Nations Convention against Transnational Organized Crime,15 November 2000, article 6(1).
57 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 16 May 2005, article 9(3). See also Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, 8 November 1990, article 6(3)(a).
58 4AMLD, articles 56–62.

La révision de la quatrième directive anti-blanchiment à la lumière des droits fondamentaux

Maxime Lassalle

The Commission's proposal for a directive amending the fourth AML Directive raises numerous issues concerning respect of the rights to privacy and to protection of personal data. The main challenges are related to the creation of central and public registries of beneficial ownership information and to the extension of the powers of the financial intelligence units concerning access to financial data. The latter is of utmost concern, as this new power of access to personal data is not balanced with explicit legal guarantees. Financial data, however, are private data deserving adequate protection.

En 2015, le nouveau système européen de lutte contre le blanchiment de capitaux et le financement du terrorisme était adopté.[1] Quelques mois plus tard voilà que la Commission annonce déjà son intention de l'amender.[2] Ce projet s'explique en partie par les attaques terroristes qui ont touché le territoire européen en 2015 et en 2016. Il avait d'ailleurs été annoncé en février 2016 par la Commission dans son plan d'action pour renforcer la lutte contre le financement du terrorisme.[3] Il s'explique aussi par l'affaire des « panama papers », qui a convaincu la Commission d'agir plus fermement contre l'évasion fiscale et la fraude fiscale. L'analyse d'impact de ce projet soulève plusieurs questions relatives à la protection des droits fondamentaux et l'objectif de cet article est de les analyser. Il se concentrera sur les enjeux en matière de protection des données et de droit à la vie privée au sens de la charte des droits fondamentaux de l'Union européenne.

Le cadre européen de lutte contre le blanchiment de capitaux est basé sur la collecte et le traitement d'une quantité considérable de données personnelles par les entités assujetties et en particulier par les institutions financières.[4] Le nouveau projet présenté par la Commission repose toujours sur la même logique de collecte de données personnelles en l'approfondissant (I). L'un des éléments principaux du nouveau projet est qu'il entend grandement faciliter l'accès à ces données collectées par le secteur privé. L'accès à ces données nécessite un encadrement pour être compatible avec le respect du droit à la vie privée et du droit à la protection des données (II). Si la nécessité d'encadrer l'accès aux données relatives aux bénéficiaires effectifs a été prise en compte dans une certaine mesure par la Commission (III), il n'en va pas de même pour l'accès aux autres données financières collectées par les établissements financiers (IV).

I. Un approfondissement du système existant

Le système préventif de lutte contre le blanchiment de capitaux repose sur un élément essentiel : la collecte et la rétention par les institutions financières de quantités très importantes de données personnelles. Cette obligation est aujourd'hui imposée par l'article 40 de la quatrième directive anti-blanchiment qui prévoit que les institutions financières doivent conserver les données relatives à leurs clients pendant au moins cinq ans. Cette obligation n'est pas modifiée par le nouveau projet de la Commission. En revanche, le projet a bien d'autres incidences sur les droits fondamentaux, et la plupart d'entre eux sont analysés par l'analyse d'impact de la Commission. Ainsi, en souhaitant inclure les établissements d'échange de monnaies virtuelles dans le champ d'application de la directive, le projet augmente automatiquement la quantité de données collectées.[5] De même, le projet accroît le contrôle des instruments prépayés qui avait été mis en place par la quatrième directive, ce qui a pour conséquence un plus grand degré de contrôle de la part des institutions financières.[6]

En outre, la proposition modifie la définition de bénéficiaire effectif d'une construction juridique en abaissant le seuil de participation requise dans la structure, augmentant ainsi la quantité d'informations recueillies par les entités assujetties.[7] De la même manière, l'obligation générale de *due diligence* est précisée dans le cas particulier des relations financières avec les pays tiers à haut risque, ce qui accroît le degré de contrôle appliqué par les institutions financières.[8] Pour toutes ces raisons, la quantité de données collectées et l'intensité du contrôle exercé sur leurs clients par les entités assujetties va augmenter. Cela renforce l'atteinte à la vie privée exercée par le système préventif de lutte contre le blanchiment de capitaux. Pour l'ensemble de ces propositions, la Commission renvoie au chapitre V de la quatrième directive anti-blanchiment[9] qui encadre le droit à la protection des données des clients des entités assujetties. Cet encadrement n'est lui-même pas entièrement satisfaisant et certains éléments pourraient être améliorés,[10] mais de manière générale la lutte contre le blanchiment de capitaux et le financement du terrorisme justifie ces atteintes au droit à la vie privée et du droit à la protection des données.[11]

En plus de cet approfondissement du système préexistant, d'autres bases de données sont créées. La Commission entend en effet faciliter et accélérer l'identification des détenteurs de comptes bancaires et de comptes de paiement. Il n'existe à l'heure actuelle pas d'obligation pour les Etats membres de mettre en place des systèmes centralisés permettant un accès rapide des autorités compétentes à ces données. Au niveau des Etats membres, on retrouve trois situations différentes. Soit (i) il existe un registre central permettant d'identifier directement les détenteurs de comptes bancaires et de paiement,[12] soit (ii) il existe un système d'extraction de données qui permet d'accéder directement aux registres des comptes bancaires et de paiements enregistrés auprès des banques et des établissements de paiement,[13] soit (iii) il est nécessaire de contacter l'ensemble des établissements bancaires et de paiement afin de leur demander de vérifier dans leurs registres s'ils ont ouvert un compte au nom d'une personne précise. Pour la Commission, ce dernier cas n'est pas satisfaisant car il empêche un accès rapide à ces données[14]. De ce fait, elle suggère de demander aux Etats membres de choisir entre un registre central et un système centralisé d'extraction de ces données.[15] La Commission est consciente de l'encadrement nécessaire afin de garantir le droit à la protection des données des personnes concernées par ces mécanismes de rétention des données.[16] Cependant, d'autres propositions visent à renforcer les possibilités d'accès aux bases de données financières et c'est ici que se situe le véritable enjeu pour les droits fondamentaux.

II. La nécessité d'encadrer l'accès aux données financières

L'accès aux données financières devrait tenir compte des exigences qui existent en matière d'encadrement de l'accès aux données personnelles par les autorités chargées de l'application de la loi. Dans son fameux arrêt *Digital Rights Ireland Ltd,*[17] la Cour de justice de l'Union européenne avait fermement critiqué la rétention de données de toute personne « de manière généralisée »,[18] sans que les personnes concernées se trouvent « même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales ».[19] L'obligation de rétention s'appliquait même « à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves » et sans prévoir d'exceptions pour les personnes protégées par le secret professionnel[20]. Ce qui est important ici, c'est que la rétention massive et indiscriminée de données personnelles n'est pas en tant que telle disproportionnée pourvu qu'elle soit accompagnée de « garanties strictes concernant l'accès aux données, la durée de conservation ainsi que la protection et la sécurité des données ».[21] Outre la durée de rétention et la sécurité des données, l'encadrement de l'accès à ces données est une garantie primordiale pour la Cour. En particulier, elle exige la présence d'un « critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données »[22] et de « conditions matérielles et procédurales »[23] relatives à cet accès. La Cour souhaite également la présence d'un « critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès » et, surtout, d'un contrôle préalable permettant de limiter « l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi ».[24] Comme les métadonnées de communications, les obligations de rétention des données financières sont très générales et concernent l'ensemble des personnes qui font usage des services bancaires et financiers. Il n'existe pas d'exception, y compris pour les personnes soumises au secret professionnel, par exemple pour les avocats. L'accès à ces données doit donc aussi être strictement encadré.

Aujourd'hui, le système prévoit seulement que les entités assujetties sont chargées de détecter des comportements suspects et d'effectuer des déclarations d'opérations suspectes auprès des cellules de renseignement financier. Ces dernières se doivent alors d'analyser ces déclarations et peuvent pour cela accéder aux données financières nécessaires à leurs analyses avant de déterminer si l'ouverture d'une enquête pénale est pertinente.[25] Avec le système actuel, l'accès aux données en l'absence de déclaration d'opération suspecte n'est pas encadré au niveau européen. Il est possible d'accéder à ces données dans le cadre d'une enquête pénale et les conditions de cet accès sont prévues par le droit national. L'encadrement de cet accès au niveau national laisse parfois à désirer[26] et a récemment retenu l'attention de la CEDH. En effet, l'accès à ces données doit faire l'objet d'une procédure susceptible de prévenir les abus, par exemple pour l'accès aux données bancaires des avocats ou aux données relatives à des personnes non visées par une enquête pénale.[27] Si la procédure d'accès en matière pénale relève des Etats membres et ne constitue pas l'objet de la proposition de la Commission, les pouvoirs d'accès aux données financières par les cellules de renseignement constituent bien, eux, l'objet de la proposition. Or, étendre ces pouvoirs via une Directive ne peut se faire sans respecter les conditions strictes prévues par l'arrêt *Digital Rights Ireland Ltd*. Cela est fait en ce qui concerne l'accès aux données relatives aux bénéficiaires effectifs.

III. L'identification des bénéficiaires effectifs

La quatrième directive anti-blanchiment avait été très innovante en imposant la création de registres centralisés pour faciliter l'accès aux informations relatives aux bénéficiaires effectifs des sociétés et autres entités juridiques[28] ainsi que des trusts et fiducies.[29] Cette nouvelle forme de collecte des

données était justifiée par l'existence de preuves selon lesquelles ces structures étaient utilisées pour couvrir des activités illicites.[30] Les règles relatives à l'accès aux deux types de registres sont actuellement différentes. Contrairement au registre des sociétés et autres entités juridiques, l'accessibilité des données relatives aux trusts et fiducies n'est pas rendue obligatoire pour « toute personne ou organisation capable de démontrer un intérêt légitime ».[31] Cette différence de traitement est justifiée par le fait que les sociétés et autres entités juridiques ne sont utilisées que pour des fins strictement économiques, alors que les trusts peuvent aussi être utilisés pour d'autres raisons, par exemple en relation avec la gestion d'un patrimoine familial.[32]

La Commission, motivée en cela par la récente affaire des « panama papers », entend désormais permettre un accès public à ces registres, non limité aux personnes pouvant démontrer un intérêt légitime.[33] La démonstration d'un intérêt légitime ne serait nécessaire que pour les trusts qui ne sont pas utilisés dans le cadre d'une activité purement économique.[34] Cette modification qui prévoit le principe d'un accès public a plusieurs objectifs, à savoir renforcer la transparence de l'information vis-à-vis des tierces personnes souhaitant engager une activité commerciale avec une certaine société ou structure juridique,[35] faciliter l'accès de la presse et de la société civile à ces informations, renforcer la confiance dans l'intégrité du système financier et supprimer tout obstacle à l'accès aux données par les institutions financières et par les autorités compétentes y compris depuis des pays tiers.[36] La Commission estime que cette transparence peut contribuer à combattre l'abus de constructions juridiques. Cette proposition répond à une revendication de longue date de la société civile.[37]

La Commission reconnaît que cette solution est risquée et mérite de plus amples analyses en ce qui concerne sa compatibilité avec la Charte des droits fondamentaux de l'Union européenne.[38] Cette crainte est justifiée. Le Conseil constitutionnel français vient de rendre une décision illustrant le risque de créer une base de données personnelles relative aux trusts et accessible librement. Le Conseil constitutionnel a estimé que constituait une ingérence dans le droit à la vie privée le fait de fournir dans un registre public des « informations sur la manière dont une personne entend disposer de son patrimoine ».[39] Bien qu'il reconnaisse que la mesure poursuit « l'objectif de valeur constitutionnelle de lutte contre la fraude et l'évasion fiscale »,[40] il estime que l'atteinte est manifestement disproportionnée.[41] En effet, le législateur n'a pas « précisé la qualité ni les motifs justifiant la consultation du registre, n'a pas limité le cercle des personnes ayant accès aux données de ce registre ».[42] On aurait pu estimer que les données disponibles, limitées aux noms de l'administrateur, du constituant, du bénéficiaire et à la date de la constitution du trust, étaient suffisamment limitées pour justifier la faible ingérence dans le droit à la vie privée. Cela étant, il est vrai que le système français allait plus loin que ce que propose la Commission. En l'espèce il s'agissait d'un trust purement privé et le Conseil d'Etat, dans sa décision de transmission de la question prioritaire de constitutionnalité, expliquait que la personne concernée faisait « valoir que la publication dans le registre litigieux de données personnelles la concernant, se rapportant notamment aux bénéficiaires des trusts qu'elle a constitués aux Etats-Unis en vue d'organiser la dévolution de ses biens après son décès, est susceptible de permettre à des personnes de son entourage d'avoir accès à des informations devant rester confidentielles jusqu'à l'ouverture de sa succession, et de les inciter à exercer sur elle des pressions en vue d'obtenir qu'elle modifie ces dispositions successorales, le cas échéant en reconsidérant la liste des bénéficiaires des trusts ainsi constitués ».[43] Cette décision du Conseil constitutionnel ne fait pas ressortir la spécificité des trusts « privés » et il est possible que la même décision serait prise dans le cas de ce que la Commission appelle les « business-type trusts » dont la transparence ne pourrait avoir de conséquences sur la vie privée. Malgré cela, il nous apparaît que le choix de la Commission est justifié et équilibré dans la mesure où il distingue les trusts qui, en raison de leur spécificité et de leur caractère privé, familial, ne peuvent être totalement transparents.[44] Plus problématique, la Commission ne s'est pas intéressée à l'encadrement de l'accès par les cellules de renseignement financier aux autres données financières collectées par les institutions financières.

IV. L'accès aux autres données financières

Selon le système actuel, les Etats membres sont libres de permettre aux cellules de renseignement financier d'accéder aux données financières détenues par les établissements financiers en l'absence de déclaration préalable par les entités assujetties.[45] En principe, les cellules policières ou judiciaires disposent de cette possibilité.[46] En effet, dans ces cas, le pouvoir d'accéder aux données financières étant déjà attribué à la police et/ou au parquet, il n'y a pas de raison pour que les cellules de renseignement financier n'en bénéficient pas. Ce pouvoir d'accès pour les cellules de renseignement financier de nature administrative est moins systématique, c'est ce qui manque dans le système actuel. Cela pose problème par exemple en matière de coopération internationale, lorsque des cellules administratives refusent d'accéder à des données dans le cadre d'une demande émanant d'une cellule judiciaire ou policière, par exemple. C'est cette situation que la Commission entend améliorer en exigeant de tout Etat membre qu'il accorde des pouvoirs d'accès plus large à sa cellule de renseignement financier, quelle que soit sa nature. La Commission entend ainsi « passer d'un système de divulgation fondé sur des suspicions

à un système de divulgation davantage basé sur le renseignement ».[47] La Commission précise que la mesure peut être justifiée par une suspicion préalable issue de la propre analyse des cellules, de renseignements fournis par les autorités compétentes ou d'informations détenues par des cellules étrangères.[48] C'est un changement significatif.[49] Notons qu'une telle extension avait été envisagée en 2014 en France, afin de transformer la cellule de renseignement financier française en « un service de renseignement financier de plein exercice».[50]

Le système proposé par la Commission se rapproche dans une certaine mesure de ce qui a été mis en place aux Etats-Unis via le PATRIOT ACT. La section 314 (a) du PATRIOT Act permet à la cellule de renseignement financier américaine d'accéder aux données financières sur demande d'autres autorités enquêtant sur des faits soit de blanchiment de capitaux, soit de financement du terrorisme.[51] Cette disposition permet de contourner deux obstacles : l'absence de déclaration d'opération suspecte de la part des entités assujetties et les obstacles procéduraux à l'accès aux données financières via les voies classiques en matière de procédure pénale.[52] Avant d'en revenir à la proposition de la Commission, deux éléments du système américain méritent d'être précisés. Le premier élément est constitué par le fait que les Etats-Unis appliquent un système de protection de la vie privée en matière d'enquête qui est très différent du système européen. Les données financières ne bénéficient pas d'une protection constitutionnelle sur le fondement du quatrième amendement de la Constitution américaine.[53] De ce fait, le Congrès est absolument libre de permettre un accès à ces données qui ne soit pas enserrés dans des conditions strictes. Le deuxième élément important est que la section 314 (a) ne permet qu'un accès limité aux données financières. La cellule de renseignement financier américaine ne peut que demander aux établissements financiers de lui signaler si une certaine personne, celle qui fait l'objet de l'enquête, détient des comptes auprès de cet établissement, et si ces comptes ont permis d'effectuer des transactions dans les six derniers mois avec d'autres comptes dont l'identité sera, elle aussi, divulguée. Autrement dit, il ne s'agit d'accéder qu'à des « lead information » qui ne font qu'indiquer dans quelle direction les enquêteurs doivent diriger leur attention. Pour accéder aux informations relatives à toutes les transactions, en particulier aux relevés de compte enregistrés par les banques, il faudra alors passer par les procédures normales qui, elles, sont plus encadrées.[54]

La proposition de la Commission ne s'embarrasse pas de limiter les pouvoirs qu'elle attribue aux cellules de renseignement financier. Elle renvoie purement et simplement au droit national qui doit encadrer ces mesures et se contente de rappeler les exigences très générales qui devront être respectées au niveau national, en particulier que l'ingérence doit être prévue par la loi[55]. Aurait-elle pu faire autrement ? Le problème vient du fait que les pouvoirs d'enquête tant des autorités compétentes en matière pénale que des cellules de renseignement financier dans le champ du renseignement relèvent en principe des prérogatives des Etats membres. Cependant, la Commission entend étendre les pouvoirs des cellules de renseignement financier via une Directive et doit en tirer les conséquences. De plus, comme l'a affirmé récemment l'avocat général Henrik Saugmandsgaard Øe « la raison d'être d'une obligation de conservation de données est de permettre aux autorités répressives d'accéder aux données conservées, de sorte que les problématiques de la conservation et de l'accès ne sauraient être complètement dissociées ».[56] En matière de données financières, l'obligation de rétention étant organisée dans une large mesure par la quatrième directive anti-blanchiment, n'aurait-il pas été pertinent d'accompagner la nouvelle proposition de lignes directrices en matière de garanties devant encadrer les pouvoirs des cellules de renseignement financier ?[57]

En guise de conclusion, une première garantie pourrait être proposée. Les nouveaux pouvoirs des cellules s'appliqueraient tant en matière de blanchiment de capitaux qu'en matière de financement du terrorisme,[58] autrement dit il n'y aurait pas de limitation quant aux raisons qui peuvent justifier l'accès aux données. Or, cette nouvelle mesure étant justifiée par le besoin de coopération accru entre les cellules de renseignement financier en matière de lutte contre le financement du terrorisme, n'aurait-il pas été préférable de la limiter aux cas de financement du terrorisme, en écartant le blanchiment de capitaux ? Il est en effet peu discutable qu'en matière de financement du terrorisme, les entités assujetties soient bien moins à même de détecter des faits suspects dans la mesure où les capitaux utilisés sont généralement d'origine légale, alors qu'un tel problème ne se pose pas en matière de blanchiment de capitaux.[59]

Plutôt que d'ignorer le problème en renvoyant à la responsabilité des Etats membres dans la transposition de la Directive, n'aurait-il pas été préférable de « rouvrir des débats fondamentaux »[60] en matière de lutte contre le financement du terrorisme afin de proposer un nouveau système ambitieux mais précisément encadré ? Cela aurait aussi permis de ne pas assimiler lutte contre le financement du terrorisme et lutte contre l'évasion fiscale, des objectifs différents qui appellent des réponses adaptées et donc vraisemblablement différenciées.

1 Directive 2015/849/EU relative à la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux et du financement du terrorisme (« la quatrième directive anti-blanchiment »), J.O. L 141/73, 5.6.2015.

2 Proposition de Directive modifiant la directive 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme et la directive 2009/101/CE (la "proposition de directive"), COM (2016) 450 final.

Maxime Lassalle

Doctorant, Faculté de Droit, d'Économie et de Finance, Université du Luxembourg et Faculté de Droit et de Science Politique, Université Paris Ouest Nanterre La Défense

3 Communication de la Commission relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme, COM (2016) 50 final.
4 Plutôt que de parler d'entités assujetties, nous limiterons nos propos aux établissements financiers.
5 Commission Staff Working Document, Impact Assessment accompanying the Proposal for a Directive of the European Parliament and the Council amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC (« l'analyse d'impact »), SWD(2016) 224 final, publié en anglais, p. 53; proposition de directive, p. 11.
6 Analyse d'impact, p. 60; proposition de directive, p. 11.
7 Analyse d'impact, pp. 69–96.
8 Analyse d'impact, pp. 46–47.
9 Ce chapitre est intitulé « Protection des données, conservation des documents et pièces et données statistiques ».
10 G. Butterelli, Opinion off the European Data Protection Supervisor on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds, Bruxelles, 4 juillet 2013, p. 13, para. 65.
11 S. De Vido, « Anti-money laundering measures versus European Union fundamental freedoms and human rights in the recent jurisprudence of the European Court of Human Rights and the European Court of Justice », *German Law Journal*, nº 5, vol. 16, 2015, p. 1271–1291; J. Böszörmenyi et E. Schweighofer, "A review of tools to comply with the Fourth EU anti-money laundering directive", *International Review of Law, Computers and Technology*, nº 1, vol. 29, 2015, pp. 63–77.
12 C'est le cas par exemple en France avec le fichier FICOBA.
13 C'est le cas par exemple en Allemagne : Voir l'analyse d'impact, p. 38.
14 Analyse d'impact, p. 22–24.
15 Proposition de directive, p. 14–15.
16 Analyse d'impact, p. 103.
17 CJUE, C-293/12 et C-594/12, *Digital Rights Ireland Ltd*, 8 avril 2014.
18 *Digital Rights Ireland Ltd*, para. 57.
19 *Digital Rights Ireland Ltd*, para. 58.
20 *Digital Rights Ireland Ltd*, para. 58.
21 Conclusions de l'avocat général Henrik Saugmandsgaard Øe, présentées le 19 juillet 2016, C-203/15 et C-698/15, *Tele2 Sverige AB*, para. 195.
22 *Digital Rights Ireland Ltd*, para. 60.
23 *Digital Rights Ireland Ltd*, para. 61.
24 *Digital Rights Ireland Ltd*, para. 62.
25 Ou éventuellement de transférer les informations à une autre autorité compétente.
26 J. Tricot et A. Nieto Martin, "Monitoring of Banking Transactions and Traffic Data", in: K: Ligeti (ed.), *Toward a Prosecutor for the European Union*, Vol. II, Hart Publishing, 2016 (à paraître); M. Simonato et M. Lassalle, "A Fragmented Approach to Asset Recovery and Financial Investigations: a Threat to Effective International Judicial Cooperation", in: Z. Durdević, E. Ivičević Karas (eds.), *European Criminal Procedure Law in Service of Protection of European Union Financial Interests: State of Play and Challenges*, Croatian Association of European Criminal Law, 2016.
27 CEDH, *Brito Ferrinho Bexiga Villa-Nova c. Portugal*, 1er décembre 2015, n°69436/10.
28 Article 30 (3) de la quatrième directive.
29 Article 31 (3) de la quatrième directive.
30 Money Laundering Using Trust and Company Service Providers, FATF, 2010.
31 Article 30 (5) c) de la quatrième directive.
32 Proposition de directive, p. 17.
33 Proposition de directive, p. 16.
34 Le système proposé est assez complexe et passe par une modification de l'article 31 de la quatrième directive et par une modification de la directive 2009/101/CE.
35 Considérant 22 de la proposition de directive.
36 Considérant 23 de la proposition de directive.
37 Fifty shades of tax dodging, Eurodad, 2015, p. 38.
38 Analyse d'impact, p. 103.
39 Conseil constitutionnel français, *Mme Helen S.*, Décision n°2016-591 QPC, 21 octobre 2016, para. 6.
40 Conseil constitutionnel français, *Mme Helen S.*, Décision n°2016-591 QPC, 21 octobre 2016, para 5.
41 Conseil constitutionnel français, *Mme Helen S.*, Décision n°2016-591 QPC, 21 octobre 2016, para. 6.
42 Conseil constitutionnel français, *Mme Helen S.*, Décision n°2016-591 QPC, 21 octobre 2016, para. 6.
43 Décision de renvoi du Conseil d'Etat, para. 9.
44 La dernière version du texte, négociée au Conseil, semble toutefois revenir sur l'aspect public au profit d'un accès limité aux personnes prouvant un intérêt légitime. La dernière version est accessible en ligne http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_14884_2016_INIT&from=EN.
45 Voir à ce sujet : MONEYVAL, *The postponement of financial transactions and the monitoring of bank accounts*, Research report of the Council of Europe, April 2013.
46 Sur la typologie des cellules de renseignement financier, voir par exemple V. Mitsilegas, "New Forms of Transnational Policing: The Emergence of Financial Intelligence Units in the European Union and the Challenges for Human Rights", *Journal of Money Laundering Control*, vol. 3, no. 2, 1999, pp. 147–160 and vol. 3, no. 3, 2000, pp. 250–259.
47 Communication de la Commission relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme, COM (2016) 50 final, p. 8.
48 Considérant 4 de la directive proposée.
49 V. Mitsilegas et N. Vavoula, "The evolving EU anti-money laundering regime: challenges for fundamental rights and the rule of law", *Maastricht journal of European and comparative law*, no. 2, 2016, p. 292.
50 Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014 de la délégation parlementaire au renseignement, Assemblée Nationale, 2014, p. 49.
51 E.J. Gouvin, "Are There Any Checks And Balances On The Government's Power to Check Our Balances? The Fate Of Financial Privacy In The War On Terrorism", *Temple Political & Civil Rights Law Review*, Vol. 14, 2005, p. 517; E.J. Gouvin, "Bringing Out the Big Guns: The USA PATRIOT Act, Money Laundering, and the War on Terrorism", *Baylor Law Review*, Vol. 55, no. 3, 2003, p. 955.
52 En matière de procédure pénale, la protection des données bancaires est très importante aux Etats-Unis. Voir le Right to Financial Privacy Act, Titre XI du Financial Institutions Regulatory and Interest Rate Control Act adopté le 10 novembre 1978. Le Right to Financial Privacy Act est codifié au 12 U.S. Code chapitre 35, para. 3401 et s.
53 *Miller v. United States*, 425 U.S. 435 (1976).
54 E. J. Gouvin, "Are There Any Checks And Balances On The Government's Power to Check Our Balances? The Fate Of Financial Privacy In The War On Terrorism", *Temple Political & Civil Rights Law Review*, Vol. 14, 2005, p. 535–537.
55 Analyse d'impact, p. 53; proposition de directive, p. 63.
56 Conclusions de l'avocat général Henrik Saugmandsgaard Øe, présentées le 19 juillet 2016, C-203/15 et C-698/15, *Tele2 Sverige AB*, para. 125.
57 CCBE comments on the proposal of 5 July 2016 to amend Directive 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, Conseil des barreaux européens, 2016, p. 3.
58 La version issue des négociations au Conseil permet de confirmer cela, alors que la proposition de la Commission ne visait que le blanchiment de capitaux. La dernière version est accessible en ligne http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_14884_2016_INIT&from=EN.
59 T. Krieger et D. Meirrieks, "Terrorism: causes, effects and the role of money laundering", in: B. Ungeret et D. van der Linde (eds.), *Research Handbook in Money Laundering, Cheltenham*, Northampton, Edward Elgar, 2013, p. 78; GAFI, Directives à l'attention des institutions financières pour la détection des activités de financement du terrorisme, 24 avril 2002, p. 3, point 9.
60 M. Wesseling, *Evaluation of EU measures to combat terrorism finance, In-depth analysis for the LIBE Committee*, Parlement européen, Bruxelles, p. 32.

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:

Thomas Wahl
Max Planck Institute for Foreign and International Criminal Law
Guenterstalstrasse 73,
79100 Freiburg i.Br./Germany

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

Max-Planck-Institut
für ausländisches und
internationales Strafrecht