

eucrim

2018 / **4**

THE EUROPEAN CRIMINAL LAW ASSOCIATIONS' FORUM



Focus: Information Exchange and Data Protection in the Area of Law Enforcement
Dossier particulier: L'échange d'informations et la protection des données dans le cadre de la poursuite pénale
Schwerpunktthema: Informationsaustausch und Datenschutz im Rahmen der Strafverfolgung

Guest Editorial
Giovanni Buttarelli

The European Commission's Proposal on Cross-Border Access to E-Evidence
Dr. Stanislaw Tosza

Unpacking the CLOUD Act
Jennifer Daskal

Classification of Electronic Data for Criminal Law Purposes
Claudia Warken

The European Commission's Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online
Dr. Gavin Robinson

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

Foundations

- 191 Fundamental Rights
- 191 Area of Freedom, Security and Justice
- 192 Schengen

Institutions

- 194 Council
- 194 OLAF
- 195 European Public Prosecutor's Office
- 195 Europol
- 196 Eurojust
- 197 Frontex

Specific Areas of Crime / Substantive Criminal Law

- 198 Protection of Financial Interests
- 198 Money Laundering
- 199 Cybercrime
- 199 Terrorism
- 199 Racism and Xenophobia

Procedural Criminal Law

- 200 Data Protection
- 201 Freezing of Assets

Cooperation

- 202 Judicial Cooperation
- 204 European Arrest Warrant
- 206 Law Enforcement Cooperation

Council of Europe

Foundations

- 207 European Court of Human Rights

Specific Areas of Crime

- 208 Corruption
- 208 Money Laundering

Articles

Information Exchange and Data Protection in the Area of Law Enforcement

- 212 The European Commission's Proposal on Cross-Border Access to E-Evidence Overview and Critical Remarks
Dr. Stanislaw Tosza
- 220 Unpacking the CLOUD Act
Jennifer Daskal
- 226 Classification of Electronic Data for Criminal Law Purposes
Claudia Warken
- 234 The European Commission's Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online
Dr. Gavin Robinson

Imprint

* The news contain Internet links referring to more detailed information. As of 2018, these links are being embedded into the news text. They can be easily accessed by clicking on the underlined text in the online version of the journal. If an external website features multiple languages, the Internet links generally refer to the English version. For other language versions, please navigate using the external website.

Guest Editorial

Dear Readers,

Police work and the administration of justice in general would be impossible without the exchange of personal information. As a member of the Italian judiciary, I can personally attest to this. At the same time, when applying and enforcing the law, judges and the police must themselves operate within the law, including the law of data protection.

Until last year, there was no general EU standard on how data should be processed for judicial and law enforcement purposes. The new “Police Directive” (Directive (EU) 2016/680) now fills that void. Though not directly applicable, like its more glamorous counterpart – the GDPR, there are no loopholes in its provisions. The choice of a directive rather than a regulation reflects the special responsibility that remains at the national level for law and order and national security. The commitment of Member States to putting these safeguards into practice is an ongoing concern. The deadline for transposition of the Directive was 9 May 2018, i.e. two years after adoption. But (at the time of writing) only 15 Member States have transposed it.

Member States tend to respond to appalling – but thankfully infrequent and isolated – incidents like the attacks in Strasbourg on December 2018 with calls for new EU-wide security measures. The 2016 PNR Directive was one such measure. Yet, as with the Police Directive, the deadline for transposition of PNR passed in May 2018, with a mere three Member States having fully transposed the Directive into national law. The Commission was obliged to reprimand 14 Member States that had failed to communicate the adoption of national legislation. It should not be necessary for the Commission to expend scarce resources in infringement proceedings. Failure to meet legislative commitments damages the credibility of those who have called so vocally for urgent EU action.

Crime is a stigma – it signifies actions that are, by their nature, intended to harm individuals or society generally. Civilised societies rightly aim to prevent crime and hold accountable those found guilty of having committed criminal acts, including the most heinous, such as terrorism. By contrast, the movement or migration of individuals and families, sometimes of entire communities, for a multitude of unique reasons, is a recurring fact and facet of human history. Migration has never been a crime in a free and democratic society.

Over the last few years, however, we have witnessed a growing tendency to conflate crime – an undisputed social ill – with the movement of people, which is innate to human freedom. This is why granting the police routine access to migration databases and creating new IT systems with dual purposes call into question the rule of law in a free and democratic society – because all of us may at some point wish or be forced to move across borders. I fear that calls for “interoperability” – while potentially justifiable – are part of this trend. New IT systems with dual purposes are under construction, and the competencies of EU agencies in the ex-third pillar sphere are being extended. Once large-scale data systems are connected, they cannot be unconnected. These are not merely technical choices; they are political choices, with ramifications for tens of thousands of people for generations to come.

Europe’s challenge today is to respond to the popular calls for stricter controls on movement across external borders without stigmatising and criminalising the people crossing those borders. Furthermore, where technology is involved – whether shared databases or the scanning of biometric information, which is among the most intimate data pertaining to an individual – the EU needs to exercise extreme vigilance to ensure that individual dignity is not degraded. This is especially true given that, in our increasingly volatile and unequal world, the most vulnerable people tend to be the ones most often subjected to monitoring and coercion enabled by digital technologies, such as big data analytics, profiling, and automated decision-making.

Now is the time for the EU to reflect on the resources needed for data protection governance of judicial and police cooperation in the coming years. In so doing, we must be guided by the ever richer and more comprehensive body of case law



Giovanni Buttarelli

from the European Court of Justice – such as *Tele2 Sverige/Watson* (Joined Cases C 203/15 and C 698/15) and *Ministerio Fiscal* (Case C 207/16), which set parameters for lawful requirements by which to retain and access subscriber, traffic, and location data.

This will shape the last chapter of the tripartite programme of data protection reform outlined by the European Commission in 2013 – first the GDPR and the Police Directive, then the EU institutions (see the recently adopted Regulation (EU) 2018/1725), and lastly the former third pillar. If we are successful, far from adding another layer of complexity to the existing and proposed new systems, we will have brought simplicity and accountability to the governance of personal data processing, fit for the purposes of the post-Lisbon Treaty Union.

In the meantime, the lawful reach of the state into the now massive quantities of personal information accumulated by the private sector continues to be debated in national and European courts. In April 2019, it will have been exactly five years since the CJEU struck down Directive 2006/24/EC, requiring the indiscriminate retention of telecommunications data. But a sustainable settlement has yet to be found, although the legality of bulk interception of communications and communications data will now be considered by Grand Chamber of the European Court of Human Rights (the cases are the *Big Brother Watch and Others v. the United Kingdom* and *Centrum för rättvisa v. Sweden*).

Police and investigating magistrates must be able to access – and require the preservation of – information relevant to investigations and prosecutions within reasonable timescales. Within the EU, it should make no difference where the data is held. The proposed e-evidence Regulation attempts to do this, although we will need explanations of how this new proposal

fits with the existing European Investigation Order, which has only recently been implemented and not yet evaluated.

The EU is attempting to set internal standards, particularly in the context of Council of Europe discussions on a Second Additional Protocol to the Convention on Cybercrime, while at the same time agreeing on norms with third countries, notably the U.S. in light of the Cloud Act. Where EU law enforcement aims to access evidence held outside the EU by non-EU service providers, third countries will expect reciprocating entitlements to access evidence held by EU companies.

Ultimately, privacy, data protection, and freedom of expression are each at stake in the proposal currently under consideration to harmonise rules for “hosting service providers” in order to prevent the dissemination of terrorist content through their services and to ensure its swift removal. Instructions from the competent public authority to the platforms should be clear and specific to avoid collateral interference with the rights of the vast majority of people who use these services and have nothing at all to do with terrorist activity.

A major challenge across the board is to ensure appropriate accountability for these actions: it should be up to the judiciary, rather than private companies, to ensure compliance of law enforcement orders with fundamental rights law. Legal certainty will require the compatibility of these rules with the data protection framework, including rules on definitions of terms like “data” and “evidence,” on the rights of data subjects, and on data security. Moreover, mutual legal assistance and prevention of terrorism should not be privatised; there needs to be democratic accountability for actions which affect the fundamental rights of individuals.

Giovanni Buttarelli, European Data Protection Supervisor



European Union*

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

Foundations

Fundamental Rights

CJEU Confirms Interim Measures Against Polish Supreme Court Reform

Also after having heard the arguments of the Polish government, the CJEU confirmed interim measures against the reform of the retirement age of Supreme Court judges under new Polish law. By [order of 17 December 2018](#), the judges in Luxembourg granted the Commission's request for interim measures and upheld a provisional order of 19 October 2018 by the Vice-President of the Court (see [eucrim 3/2018](#), 144). The full text of the order (referred to as [Case C-619/18 R](#)) is [available in French](#).

Despite taking into account the position of the Polish government, the CJEU acknowledged that the pleas raised by the Commission were justified in fact and law. All requirements for interim relief were fulfilled, in particular the urgency requirement, which presupposes that the interlocutory order avoids serious and irreparable harm to the interests of the EU.

In its reasoning, the CJEU emphasized that the application of the national legislation at issue is likely to cause serious damage to the EU legal order. The reason for this is that the independence of the Polish Supreme Court is not ensured until the delivery of the final judgments in the infringement proceedings. Failure to ensure the independency of the Supreme Court may have several consequences, e.g.:

- Preliminary ruling mechanism does not work properly;
- Lack of authority of the Supreme Court over the lower Polish courts;
- Mutual trust of the EU Member States and their courts is undermined in the Polish system, which can lead to the refusal of recognition and enforcement of judicial decisions made by Polish courts and, in the end, disturb the cooperation mechanism in the EU.

The CJEU also examined whether weighing up the interests involved support the granting of interim measures. The CJEU concluded that the EU's general interests in the proper working of its legal order predominates over Poland's interest in the proper working of the Supreme Court, given the fact that the ap-

plication of the system before the reform is only maintained for a limited period.

It should be noted that the order of 17 December 2018 did not make final judgement on the substance of the action. This will be done at a later stage. The order for interim measures is also without prejudice to the outcome of the main proceedings. (TW)

Area of Freedom, Security and Justice

CJEU Paves Way to Exit from Brexit

The United Kingdom is free to unilaterally revoke the notification of its intention to withdraw from the EU. Unanimous approval by the European Council regarding this revocation is not necessary. This was the response of the CJEU plenary to a request for a preliminary ruling by the Scottish Court of Session ([Case C-621/18](#), [Wightman and Others v. Secretary of State for Exiting the European Union](#)).

The question of whether the notification of the UK's intention to withdraw from the EU (made in accordance with Art. 50 TEU) can be revoked was posed by members of the UK Parliament, the Scottish Parliament, and the European Parliament. The intention was to provide guidance to the members of the House of Commons when exercising their vote on the withdrawal agreement.

With the [CJEU's answer of 10 December 2018](#), the UK now has three (instead of two) options since the pro-

* If not stated otherwise, the news reported in the following sections cover the period 16 November – 31 December 2018.

cedure of Art. 50 TEU was triggered by the British Prime Minister's notification to leave the EU following the Brexit referendum on 23 June 2016:

- Withdrawal from the EU without an agreement;
- Withdrawal from the EU with an agreement;
- Revocation of the notification of the intention to withdraw, with the UK remaining in the EU.

The judges in Luxembourg stressed, however, that the revocation is subject to the national constitutional requirements. Furthermore, a revocation is subject to the following:

- Only possible as long as a withdrawal agreement between the EU and the UK has not entered into force, or, if no agreement is concluded, as long as the two-year period (or any possible extension) from the date of the notification of the intention to withdraw has not expired;
- The revocation is unequivocal and unconditional;
- The revocation must be communicated in writing to the European Council.

A revocation would have the effect that the UK remains in the EU under the terms of its current status and that the withdrawal procedure is put to an end.

In its reasoning, the CJEU observed that the revocation is not expressly governed by Art. 50 TEU, but follows the same rules as the withdrawal itself. Consequently, the EU Member State that notifies its intention to withdraw can unilaterally decide not to do so, because it is the sovereign decision to retain a status as a EU Member State.

An approval of the revocation by the other EU Member States (as put forward by the Council and the Commission in the proceedings) would be counter to the principle that a Member State cannot be forced to leave the EU against its will.

The judgment of the CJEU extends the spectrum of action for UK parliamentarians and can be termed “integration-friendly.” It remains rather unlikely, however, that the option of the revocation will be heeded. First, the

UK must overcome the current political impasse. (TW)

Schengen

New Legal Framework for Schengen Information System

spot light New alerts on criminals and return decisions; greater vigilance for terrorist offences; better protection for children at risk of abduction; and enhanced data protection. These are the main features of the new legal framework for the EU's largest security database, the Schengen Information System (SIS). The new rules aim at better effectiveness and efficiency of the system's second generation (SIS II), whose legal bases stem from 2006/2007 and which became fully operational in 2013.

The reform proposal presented by the Commission on 21 December 2016 (see *eu crim* 1/2017, p. 7) was **adopted in November 2018 by the Council**. The European Parliament had already agreed to the political compromise found during the trilogue negotiations **in October 2018**.

The new legal framework was published on 7 December 2018 in the Official Journal (*O.J. L 312*). It consists of three regulations:

- **Regulation (EU) 2018/1860** on the use of the Schengen Information System for the return of illegally staying third-country nationals;
- **Regulation (EU) 2018/1861** on the establishment, operation and use of the SIS in the field of border checks;
- **Regulation (EU) 2018/1862** on the establishment, operation and use of the SIS in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.

The three legal instruments were considered necessary because of the distinct EU Member States' participation in EU

policies in the Area of Freedom, Security and Justice. The regulations emphasise, however, that this separation does not affect the principle that SIS constitutes one single information system that should operate as such.

In general, the new rules pursue the following objectives:

- Ensuring a high level of security;
- Increasing the efficiency of the SIS;
- Protecting the free movement of persons from abuse;
- Improving the exchange of information;
- Making the SIS a central tool for fighting terrorism and serious crime;
- Supporting border and migration management;
- Preparing the SIS for its interoperability with other large-scale EU information systems, such as the VIS, Eurodac, ETIAS, and EES.

The SIS continues to cover three areas of competence:

- Security cooperation, allowing police and judicial authorities to establish and consult alerts on persons or stolen objects in relation to criminal offences;
- Border and migration management, enabling border and migration authorities to control the legality of third-country nationals' stays in the Schengen area;
- Vehicle control, granting vehicle registration authorities access to information about vehicles, number plates, or vehicle registration documents in order to check the legal status of vehicles.

The following gives an overview of the new features of the legislation, in particular as regards Regulation 2018/1862 on the operation and use of the SIS for police and judicial cooperation in criminal matters:

► New Alerts:

- Introduction of a new alert category of “unknown wanted persons” connected to a serious crime, e.g., persons whose fingerprints are found on a weapon used in a crime;
- Extension of the existing category of “missing persons” to “vulnerable persons who need to be prevented from

travelling,” e.g., children at high risk of parental abduction, children at risk of becoming victims of trafficking in human beings, and children at risk of being recruited as foreign terrorist fighters;

- Creation of the new category “inquiry check” allowing national law enforcement authorities to stop and interview a person in order for the issuing Member State to obtain detailed information;
- Introduction of the category of “objects of high value,” e.g., items of information technology, which can be identified and searched with a unique identification number.

➤ *Greater Vigilance over Terrorist Offences:*

- Obligation for Member States to create SIS alerts for cases related to terrorist offences;
- Obligation to inform Europol of hits alerts linked to terrorism in order to help to “connect the dots” of terrorism at the European level.

➤ *Types of Data – Use of Biometrics:*

- New rules on more effective use of existing biometric identifiers, i.e., facial images, fingerprints, palm prints, and DNA profiles;
- Use of facial images for biometric identification;
- Use of DNA profiles when searching for missing persons who need to be placed under protection;

➤ *Law Enforcement Access:*

- Immigration authorities allowed to consult SIS in relation to irregular migrants who were not checked at a regular border control;
- SIS granted access to boat and aircraft registration authorities;
- SIS granted access to services responsible for registering firearms in order to allow them to verify whether the firearm is being sought for seizure in Member States or whether there is an alert on the person requesting the registration;
- Europol’s access rights extended to give it full access to the system, including missing persons, return alerts, and alerts in relation to third-country nationals;

■ European Borders and Coast Guard Agency and its teams granted access to all SIS categories, insofar as it is necessary for the performance of their tasks and as required by the operational plan for a specific border guard operation.

➤ *Enhanced Data Protection and Data Security:*

- Introduction of additional safeguards to ensure that the collection and processing of, and access to, data is limited to what is strictly necessary and operationally required;
- Applicability of and adaptation to the new EU data protection framework, in particular Directive 2016/680 and the GDPR;
- Coordination and end-to-end supervision by the national data protection authorities and the European Data Protection Supervisor.

Regulation 2018/1860 establishes an effective system, so that return decisions issued in respect of third-country nationals staying illegally on the territory of the Member States can be better enforced and third-country nationals subject to those decisions can be monitored.

Regulation 2018/1861 establishes the conditions and procedures for the entry and processing of SIS alerts on third-country nationals and for the exchange of supplementary information/additional data for the purpose of refusing entry into/stay on the territory of the Member States. Member States will, *inter alia*, be obliged to insert into the SIS any entry bans issued to third-country nationals preventing them from entering into the Schengen area.

The regulations contain specific rules as regards the EU Member States having a special status with Schengen and measures in the area of freedom, security and justice of the TFEU, e.g., Denmark, Ireland, Croatia, Bulgaria, Romania, and Cyprus.

As regards the entry into force of the new SIS rules, the regulations follow a step-by-step approach: Several improvements to the system apply immediately

upon entry into force of Regulations 2018/1861 and 2018/1862 (i.e., 27 December 2018), whereas others will apply either one or two years after entry into force. The said regulations should apply in their entirety within three years after entry into force – and by 28 December 2021 at the latest. Regulation 2018/1860 will apply from the date set by the Commission.

The SIS is the most widely used security database in Europe, with over 5 billion consultations in 2017 and currently contains around 79 million records. It is estimated that further enhancement of the SIS by the new legal framework will cost the EU around €65 million by 2020. Each EU Member State will reportedly receive a lump sum of €1.2 million to upgrade its national system. The EU agency eu-LISA will be responsible for technical improvements and operation of the system. (TW)

EP Wants Temporary Border Controls Kept to a Minimum

On 29 November 2018, the European Parliament (EP) [adopted its negotiating position on the revision of the Schengen Borders Code](#). MEPs backed amendments as proposed by rapporteur *Tanja Fajon* (S&D, Slovenia) by 319 to 241 votes (with 78 abstentions).

The reform was initiated by the Commission in September 2017 (see eucrim 3/2017, pp. 98–99) and aims at adapting rules on the temporary reintroduction of internal border controls in a targeted manner.

MEPs stressed that the revision must ensure the Schengen achievements and put an end to current misuse or misinterpretation when upholding internal border controls.

In particular, the EP advocated reducing the time periods by means of which internal borders controls can be upheld as follows:

- The initial period for border checks should be limited to two months;
- Border checks should not be extended beyond one year.

Furthermore, the EP's amendments to the proposal highlighted the following:

- Temporary border checks should only be used in exceptional circumstances and as a measure of last resort;
- Schengen countries should provide a detailed risk assessment if temporary border checks are extended beyond the initial two months;
- Subsequent extensions of border checks beyond six months require the Commission to state whether or not the prolongation follows the legal requirements and should be authorised by the EU Council of Ministers;
- The EP must be more informed and involved in the process.

Representatives of the EP will now enter into negotiations with the Council, which adopted its [approach to the Schengen Borders Code reform in June 2018](#).

Currently, five Schengen countries (Austria, Germany, Denmark, Sweden, and Norway) have internal border checks in place due to exceptional circumstances resulting from the migratory crisis that started in 2015. France carries out internal border checks due to a persistent terrorist threat.

The EP previously voiced criticism over the prolongation of internal border controls, which is not in line with the existing rules, unnecessary, and disproportional (see eucrim 2/2018, p. 84). (TW)

Institutions

Council

Romania Kicks off New Trio Presidency of the Council of the EU

Under the motto “Cohesion, a common European value,” [Romania](#) took over the Presidency of the Council of the EU on 1 January 2019. Priorities of the Romanian Presidency in the area of security include:

- Increasing the interoperability of EU security systems;
- Protecting the safety of citizens, com-

panies, and public institutions in the cyberspace;

- Improving the overall resilience of the Union to cyber-attacks;
- Continuing the fight against terrorism;
- Setting up the European Public Prosecutor's Office.

The Romanian Presidency is the first in a new 18-month Trio Presidency, to be followed by Finland (July–December 2019) and Croatia (January–June 2020). According to the Trio Presidency's [18-month programme](#), priorities for the EU's internal security are:

- To enhance police and judicial cooperation;
- To combat organised crime, including drug trafficking and human trafficking;
- To remove terrorist content online and to prevent radicalisation and extremism;
- To enhance the interoperability of information systems;
- To further develop the capacities needed to promote cybersecurity and to counter cyber risks;
- To advance mutual recognition and commit to promote e-Evidence and e-Justice;
- To establish the EPPO and strengthen cooperation with OLAF.

The Trio programme points out that, at the beginning of the Trio, the main priority will be the finalisation of the still outstanding files of the current Strategic Agenda and in particular those listed in the Joint Declaration on the EU's legislative priorities for 2018–19. The future work will also be inspired by the outcome of the EU summit in Sibiu, Romania, which takes place on 9 May 2019, Europe Day. It will be the first summit of the national leaders of the EU-27 after Brexit. (CR)

OLAF

ECA: Planned OLAF Reform Still Has Weaknesses

On 22 November 2018, the European Court of Auditors (ECA) issued [Opinion](#)

[No 8/2018](#) on the Commission's proposal of 23 May 2018 amending OLAF Regulation 883/2013 (for the proposal, see eucrim 1/2018, pp. 5–6). The ECA observes that the proposal pursues two objectives: (1) to adapt the functioning of OLAF to the establishment of the EPPO; (2) to enhance the effectiveness of OLAF's investigative function. The ECA Opinion welcomes certain approaches and concepts in the Commission proposal, but still sees some weaknesses preventing the two objectives from being met.

Regarding the relationship with the EPPO, the ECA points out the following:

- There is a risk that evidence collected by OLAF at the EPPO's request would not be admissible before national courts if OLAF applies its own procedural safeguards but not the ones laid down in the EPPO Regulation;
- The proposal does not address OLAF's role in criminal investigations affecting the EU's financial interests, if they concern both Member States that participate in the EPPO scheme and those that do not;
- The effectiveness of “complementary investigations” on the part of OLAF is not ensured.

Regarding the second objective – enhancing the effectiveness of OLAF's investigative function – the ECA welcomed the targeted measures, but does not consider the overall issues surrounding the effectiveness of OLAF's administrative investigations resolved. The ECA makes specific recommendations for the legislative proposal, e.g., bringing OLAF reports under review by the CJEU.

Ultimately, the auditors stress the need to further action. In the short term, the Commission should address the overall issues of OLAF's effectiveness, and the Commission should reconsider OLAF's role in combating EU fraud. Hence, OLAF must be given a strategic and oversight role in EU anti-fraud actions.

In the medium term, the Commission should evaluate the cooperation between OLAF and the EPPO. This should cover:

- Possible restructuring of the EU bodies in charge of administrative and criminal investigations;
- Possible single legal framework to combat fraud in EU spending.

The ECA Opinion is not binding for the co-legislators (Council and EP), but is designed to support their work. (TW)

OAFCN Meeting at OLAF

In November 2018, OLAF hosted the annual meeting of the Anti-Fraud Communicators' Network (OAFCN). Communication experts working for anti-fraud public organisations discussed crisis communication, the importance of storytelling, and real-life communication scenarios.

The OAFCN is a European-wide network of communication officers and spokespersons from OLAF's operational partners in the Member States, such as customs, police, law enforcement agencies, prosecutors' offices, and Member States' Anti-Fraud Coordination Services (AFCOS). It is designed to communicate the threat of fraud and counter-measures to the public. It is also an important forum for awareness raising on fraud issues. (TW)

European Public Prosecutor's Office

Vacancy Notice for the European Chief Prosecutor

On 19 November 2018, the European Commission published a [call for application for the first ever European Chief Prosecutor](#) (ECP) to head the European Public Prosecutor's Office (EPPO) based in Luxembourg.

The European Chief Prosecutor is the Head of the EPPO, in charge of organising its work, directing its activities, and taking decisions in accordance with the EPPO Regulation and its internal rules of procedure. Furthermore, the ECP represents the EPPO towards EU institu-

tions, EU Member States, and third parties. Additionally, the ECP has various duties and responsibilities with regard to the setting up of the College, the Permanent Chambers, and the EPPO's internal rules of procedure and financial rules.

Interested applicants must be citizens of one of the EU Member States participating in the EPPO. The candidate may be no more than 63 years of age at the time of the appointment and have a minimum of fifteen years of professional experience as an active member of the public prosecution service or judiciary and at least five years of experience as a public prosecutor responsible for the investigation and prosecution of financial crimes in a Member State.

After evaluation of the selected candidates by a selection panel, the European Parliament and the Council will appoint the ECP.

The vacancy notice was open until 14 December 2018. (CR)

Europol

Cooperation Europol-Japan on New Footing

On 3 December 2018, [Europol and the National Police Agency of Japan](#) (NPA) signed a Working Arrangement with the aim of combating serious, international cross-border, and organised crime such as terrorism, drug trafficking, and cyber-crime. Under the arrangement, a secure communication line will be established between the agencies. Furthermore, the NPA may second a liaison officer to Europol. In this way, a secure, timely, and direct exchange of information between Europol and the NPA will be ensured.

The arrangement comes in addition to the cooperation offered by the existing Agreement between Japan and the European Union on Mutual Legal Assistance in Criminal Matters. It is also designed to foster cooperation between the EU and Japan in view of the upcoming Olympic Games in Tokyo in 2020. (CR)

Cooperation with Diebold Nixdorf

On 16 November 2018, [Europol and Diebold Nixdorf signed a Memorandum of Understanding \(MoU\)](#) with the aim to better prevent, prosecute, and disrupt cybercrime related to self-service ecosystems. Under the MoU, Diebold Nixdorf will be able to share threat intelligence data and best practices with Europol in a secure and trusted manner.

Diebold Nixdorf Inc is a global end-to-end provider of electronic services, software, and hardware (e.g., for self-service transaction systems such as ATMs and point-of-sale technology) for the financial and retail industries. (CR)

Second Annual Conference on Drugs in Europe

On 6–7 December 2018, Europol hosted the second annual conference on “Drugs in Europe: a bold law enforcement response.” Delegates from all over the EU, third states, and international organisations discussed the latest developments in illicit drug trafficking.

Faced with an increasing number of organised criminal groups and the supply of illegal drugs, delegates called on Member States to ensure adequate resources to combat them. Furthermore, emphasis was placed on the need for a coordinated response between the EU and Member States as well as the exchange of information, operational cooperation, and coordination of activities between Member States' law enforcement authorities and Europol. Lastly, delegates underlined the need for effective implementation of comprehensive asset recovery legislation. (CR)

Operational Network Against Mafia-Style Criminal Groups

At the end of November 2018, law enforcement authorities from Italy, Belgium, France, Germany, the Netherlands, and Spain kicked off a [new operational network \(@ON\)](#), together with Europol, to strengthen their cooperation against mafia-style criminal groups, Eurasian and Albanian criminal networks, and

Report

Conference on the Implementation of the EPPO Regulation

Bucharest, 13-14 December 2018

The Romanian National Anti-Corruption Directorate (with the assistance of the Romanian Association for the Research of EU Criminal Law) organised the conference “The impact of the EPPO Regulation at the level of the national authorities of the participating EU Member States.” The HERCULE III Programme financially supported the conference. It was part of the ongoing project “Promoting the protection of the financial interests of the EU by supporting the actions of the Member States and the European Institutions in the transition towards the EPPO.”

The event brought together representatives from the national prosecution offices, judges, academics, and members of the Associations for European Criminal Law and the Protection of Financial Interests of the European Union. It aimed to facilitate the sharing of experiences, challenges, and practices in order to prepare the EU and the national legal systems for the establishment of the EPPO.

The first part of the conference included presentations on the state of play of the implementation of the EPPO Regulation (*Péter József Csonka*, DG JUST), on OLAF support in EPPO investigation (*Luca de Matteis*, OLAF) and on the challenges of the implementation of the PIF Directive (*Christoph Burchard*, University of Frankfurt). The conference continued with presentations that focused on the study on the impact of the future EPPO on the Romanian judicial and legal system (*Gheorge Bocsan*, Prosecutor’s Office attached to the High Court of Cassation, Romania), on the relations between the national and European Prosecutors (*Alberto Perduca*, Chief Prosecutor, Italy) and on the reporting obligations and general cooperation between the national authorities and the EPPO (*Emanuelle Wachenheim*, Ministry of Justice, France).

Additional presentations addressed the issues of admissibility and freedom of circulation of evidence during the investigation and adjudication of the EPPO cases (*John Vervaele*, Utrecht University), cross-border investigations, cooperation within the EPPO and MLA in criminal matters with third countries (*Filippo Spiezia*, Vice-President of Eurojust), and the procedural guarantees and protection of human rights during EPPO investigations (*Miguel Carmona*, magistrate, Spain).

The last part of the conference was dedicated to a hypothetical case study (*Alexandra Lancranjan*, DNA, Romania), which was subsequently discussed in detail by the participants in different working groups.

Dr. András Csúri, University of Utrecht

Outlaw Motorcycle Gangs. Within the network, specialised investigative units and special investigators will offer support to the Member States involved.

The ONNET project is financially supported by the European Commission. @ON is composed of the Italian *Direzione Investigativa Antimafia* (D.I.A.) – which plays a leading role – the Belgian Federal Police, the French National Police and *Gendarmerie Nationale*, the German Federal Criminal Police Office (*Bundeskriminalamt*), the Dutch National Police, and the Spanish National Police and *Guardia Civil*. (CR)

Fourth European Money Mule Action

Europol, Eurojust, and the European Banking Federation (EBF) reported on the fourth European Money Mule Action “EMMA 4” – a global law enforcement action week tackling the issue of money muling. According to the [joint press release of 4 December 2018](#), the action led to the arrest of 140 money mule organisers and 168 persons. In addition, 1504 money mules were identified (for previous actions, see [eucrim 1/2016](#), p. 6).

Thirty states took part in the action that ran from September to November 2018, together with the European in-

stitutions. Furthermore, over 300 banks supported the action.

In addition, a money muling awareness raising campaign was kicked off on 4 December 2018. Information is provided under #DontBeAMule on how these criminals operate, how one can protect oneself, and what to do if one becomes a victim.

Money mules are persons who, often unwittingly, transfer illegally obtained money between different accounts on behalf of others. They are regularly tricked by criminal organisations that promise easy money. (CR)

Eurojust

New Eurojust Regulation

spot light On 6 November 2018, after 5 years of discussion, Eurojust’s new Regulation was adopted with the aim of strengthening its capabilities to support the national authorities in their fight against serious, cross-border crime. The Regulation ((EU) 2018/1727) was published in the [Official Journal L 295 of 21 November 2018](#), p. 138.

In the Regulation, Eurojust’s competences are now clearly set out without referring to the Europol Convention (as the previous Eurojust Decision did). The forms of serious crime for which Eurojust is competent are now listed in an Annex I to the Regulation. The Regulation also defines the categories of related offences for which Eurojust is competent. It also outlines that, in general, Eurojust shall not exercise its competence with regard to crimes for which the EPPO exercises its competence. The practical details of Eurojust’s exercise of competence, however, shall be governed by an additional working arrangement. Ultimately, when requested by a competent authority of a Member State, Eurojust may also assist with investigations and prosecutions for forms of crime other than those listed in Annex I.

While the distinction is still made as

to whether Eurojust exercises its function as a college or through its National Members, Eurojust's operational functions are now clearly set out under Art. 4.

Regarding the National Members, the Regulation now requests the Member States to grant them at least the powers referred to in this Regulation in order for them to be able to fulfil their tasks. Contrary to the former Eurojust Decision, the Regulation now limits the length of the term of office of the National Members to 5 years, renewable once. The Regulation now describes the powers of the National Members in detail as well as the types of national registers they shall have access to.

The College's voting rules for taking decisions changed from a two-thirds majority to a majority of its members. Furthermore, under the Regulation, the College has now been asked to adopt annual and multi-annual work programmes setting out objectives and strategic aims for their work. In addition, the new Regulation introduces an Executive Board to deal with administrative matters in order to allow Eurojust's College to focus on operational issues. A representative of the European Commission will be part of the Executive Board.

Contrary to the former Eurojust Decision, roles and tasks of Eurojust's National Coordination System and national correspondents are laid out in the Regulation. The exchange of information with the Member States and between national members is also set out in more detail, requiring the competent national authorities to inform their national members without undue delay under certain conditions.

More democratic oversight is foreseen by means of regular reporting to the European Parliament and national parliaments.

Finally, Eurojust's data protection rules have been aligned with the latest EU data protection rules, including supervision by the EDPS.

Eurojust's reform through the new Regulation is the last in a series of re-

forms, with new Regulations for Frontex entering into force in 2016 and Europol entering into force in 2017, and the creation of the EPPO. The Regulation replaces and repeals Council Decision 2002/187/JHA. It will be applicable by the end of 2019. (CR)

First Liaison Prosecutor for Macedonia

On 12 November 2018, Ms *Lenche Ristoska* took up her duties as the [first Liaison Prosecutor for the former Yugoslav Republic of Macedonia](#) at Eurojust. Before her secondment to Eurojust, Ms *Ristoska* served as a prosecutor at the Special Public Prosecutors' Office in Skopje. She also previously worked for the Department for International Mutual Legal Assistance in Criminal Matters of the Primary Public Prosecutor's Office of Skopje, executing incoming mutual legal assistance (MLA) requests as well as in the Department for Drugs, Sexual and Violent Crimes.

The appointment of liaison prosecutors is foreseen in the cooperation agreement between Eurojust and the former Yugoslav Republic of Macedonia, which was concluded in 2008. Liaison prosecutors play an important role in facilitating ongoing investigations of serious, cross-border, organised crime, given the increased number of cases that have connection with the Western Balkans.

The appointment of liaison prosecutors from Western Balkan states at Eurojust is also part of Eurojust's efforts to build up structural, judicial cooperation in the region in the fight against serious, cross-border crime. More information on Eurojust's cooperation with the Western Balkans is [available at the Eurojust website](#). (CR)

Frontex

FRA Opinion on Revised Frontex Regulation

At the end of November 2018, FRA published its [Opinion on the revised European Border and Coast Guard Regula-](#)

[tion and its fundamental rights implications](#).

In the Opinion, FRA focuses on four issues and makes suggestions on the following:

- How to strengthen Frontex' overall fundamental rights protection framework;
- How to address fundamental rights risks in specific aspects of Frontex operation;
- The Agency's activities in the return of third-country nationals;
- Challenges related to the enhanced role of Frontex in third countries.

The opinion does not cover issues such as the deployments of liaison officers and their role with regard to respect for fundamental rights or cover questions of criminal liability of deployed team members. (CR)

Risk Analysis Cell in Niger

In cooperation with Nigerian authorities, Frontex opened the first [Risk Analysis Cell in Niamey, Niger](#) at the end of November 2018. The cell will collect and analyse strategic data on cross-border crime such as illegal border crossings, document fraud, and trafficking in human beings. It will support relevant authorities involved in border management to produce analysis and policy recommendations. It is run by local analysts trained by Frontex.

The Risk Analysis Cell in Niger is the first of eight such cells that will be established within the framework of the Africa-Frontex Intelligence Community (AFIC). Over the next twelve months, these cells will be set up in Ghana, Gambia, Senegal, Kenya, Nigeria, Guinea, and Mali. (CR)

Eastern Partnership IBM Project Concluded

At the end of November 2018, after four years, the [Eastern Partnership Integrated Border Management \(EaP IBM\)](#) Capacity Building Project was concluded with a final meeting at Frontex premises. By offering technical as-

sistance through Frontex, the project aimed at expanding the ability of participating border agencies to effectively implement the Integrated Border Management concept. A training system on Integrated Border Management was established through the project. Countries that participated included Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine. (CR)

Specific Areas of Crime / Substantive Criminal Law

Protection of Financial Interests

New Action Plan Against Illicit Tobacco Trade

On 7 December 2018, the Commission published the 2nd Action Plan to fight the illicit tobacco trade ([Communication to the European Parliament and the Council, COM\(2018\) 846 final](#)). The action plan covers the period 2018–2020. The Commission stresses that the illicit tobacco trade can only be curbed by a combination of policy and enforcement measures.

It builds on the 1st Action Plan of 2013, its evaluation in 2017, and the WHO Protocol to Eliminate Illicit Trade in Tobacco Products (FCTC Protocol). The FCTC Protocol was actively negotiated by the European Commission and entered into force on 25 September 2018.

According to the new plan envisaged by the Commission in the years to come, the following should be pursued:

- Fully exploiting the new FCTC Protocol's potential as a global instrument and forum to curb the illicit tobacco trade;
- Engaging key source and transit countries via various frameworks for co-operation;
- Focusing on some of the key input materials going into the illicit manufacture of tobacco products, ranging from raw tobacco and cigarette filters

to manufacturing and packing equipment;

- Raising consumer awareness of the dangers of buying illicit tobacco products and of the direct links to organised crime as a means of reducing demand;
- Continuing to invest in intelligence gathering and analysis as a basis for effective targeting of policy and operational measures.

A concrete list of actions is contained in an [Annex to the Communication](#).

The illicit tobacco trade is estimated to cause an annual €10 billion loss in public revenue in the EU and its Member States. (TW)

ECA Opinion on Future Anti-Fraud Programme

On 15 November 2018, the European Court of Auditors (ECA) adopted [Opinion No 9/2018](#) on the Commission's proposal for a Regulation establishing the EU Anti-Fraud Programme for the 2021–2027 financing period (for the proposal, see [eucrim 2/2018](#), pp. 92–93). The successor to the current Hercule III-Programme, which expires in 2020, aims at protecting the EU's financial interests and supporting mutual assistance between the administrative authorities of the Member States. It also aims at cooperation between the Member States and the Commission to ensure the correct application of the law on customs and agriculture.

The ECA recommends the following:

- Better specification of the programme's concrete objectives and indicators to evaluate its results;
- Clarification of the frequency of performance and introduction of independent evaluators to carry out evaluations;
- Improved evaluations by the Commission of the programme's added value and assessment of possible overlaps with other EU actions.

If the plans of the Commission are supported by the co-legislators (Council and EP), the new programme would have €181 million at its disposal for the entire period. (TW)

Money Laundering

Council: Anti-Money Laundering Action Plan

At its meeting of 4 December 2018, the ECOFIN Council adopted [conclusions on an Anti-Money Laundering Action Plan](#). The ministers welcomed the progress made in preventing and combating money laundering in recent years, but call for further improvements, in particular as regards the (cross-border) exchange of information and collaboration between prudential and anti-money laundering supervisory authorities.

The action plan includes eight objectives that should be addressed in the short term:

- Identifying the factors that contributed to the recent money laundering cases in EU banks;
- Mapping relevant money laundering and terrorist financing risks and the best prudential supervisory practices to address them;
- Enhancing supervisory convergence;
- Ensuring effective cooperation between prudential and money laundering supervisors;
- Clarifying aspects related to the withdrawal of a bank's authorisation in case of serious breaches;
- Improving supervision and exchange of information between relevant authorities;
- Sharing best practices and identifying grounds for convergence among national authorities;
- Improving the European supervisory authorities' capacity to make better use of existing powers and tools.

The latter refers to the recent Commission proposal of 12 September 2018, which aims at amending existing EU rules on the supervision of banks and financial institutions (cf. [eucrim 2/2018](#), p. 94). This proposal is currently under discussion in the Council.

An annex lists the concrete actions planned. As from June 2019, the Commission is requested to report back on the progress made in the implementation of

the Action Plan detailed in the Annex of the Conclusions every six months. (TW)

Cybercrime

12th Referral Action Day

On 20 November 2018, Europol's EU Internet Referral Unit (EU IRU) organised a joint [Referral Action Day](#) together with national referral units from seven Member States and third parties, targeting online material linked to terrorist activities. This time, 7393 items were assessed and referred to participating online platforms, requesting their review. (CR)

First European Youth Day

Europol's European Cybercrime Centre (EC3) organised a [European Youth Day](#) for the first time, which took place on 20 November 2018. Under the slogan "Digital Rights of Youth against Violence," approx. 100 youths between 12 and 15 years of age gathered at Europol to discuss online and offline safety issues. As a result, a [call for action](#) was drafted, calling on Internet governance institutions, Internet providers, policy-makers, and all relevant stakeholders to create a safer Internet for children and adolescents. (CR)

Terrorism

EP Tables Recommendations for New EU Strategy to Combat Terrorism

On 12 December 2018, MEPs adopted a [resolution that contains over 225 recommendations for tackling the threat of terrorism](#). The resolution goes back to a report from MEPs *Monica Hohlmeier* (EPP, Germany), and *Helga Stevens* (ECR, Belgium), who compiled the findings of the Special Committee on Terrorism (TERR).

The Special Committee was established in 2017 following the persistent terrorist threats that the EU has had to face in recent years. The Committee was

mandated with examining, analysing, and assessing the extent of the terrorist threat on European soil. It carried out a thorough assessment of the existing forces on the ground in order to enable the EU and its Member States to step up their capacity to prevent, investigate, and prosecute terrorist offences.

The resolution of December 2018 makes recommendations in the following areas:

- Institutional framework;
- Terrorist threat;
- Prevention and countering of radicalisation leading to violent extremism;
- Cooperation and information exchange;
- External borders;
- Terrorist financing;
- Critical infrastructure protection;
- Explosive precursors;
- Illicit weapons;
- External dimension;
- Victims of terrorism;
- Fundamental rights.

The EP requests, *inter alia*, that the role of Europol and the EU agency for the operational management of large-scale IT systems (eu-LISA) be reinforced. Furthermore, improvements in information exchange and cooperation between intelligence services and authorities are necessary. Other proposals include:

- EU watch list for hate preachers;
- Allowing the police to cross-check persons renting cars against police databases;
- Anti-radicalisation measures, including programmes for prisons, education, and campaigns;
- Proper checks at all external borders using all relevant databases;
- Including private planes in the PNR Directive;
- European system of licences for specialised buyers of explosive precursors;
- Better protection of victims, including the creation of an EU Coordination Centre of victims of terrorism (CCVT), pre-paid medical costs after an attack, and smoother insurance procedures.

The work of TERR was finalized on 14 November 2018 by the committee's vote on the *Hohlmeier/Stevens* report. Further information on the work of this special committee during its mandate can be found on the [committee's website](#). (TW)

Racism and Xenophobia

Council Shapes Rules on Fighting Terrorist Content Online

At its [meeting of 6 December 2018](#), the JHA Council [adopted its general approach](#) to the proposed regulation on preventing the dissemination of terrorist content online. This proposal had been submitted by the European Commission on 12 September 2018, following a call by EU leaders in June. For the proposal, see *eu crim* 2/2018, pp. 97–98 and the article by *G. Robinson* in this issue.

The aim of the planned legislation is to establish binding rules for hosting service providers (HSPs) offering services in the EU (whether or not they have their main establishment in the Member States) to rapidly remove terrorist content, where necessary.

HSPs will have to remove terrorist content or disable access to it within one hour of receiving a removal order from a national authority. If HSPs do not comply with removal orders, financial penalties can be imposed on them.

Furthermore, service providers will have to apply certain duties of care to prevent the dissemination of terrorist content on their services. This may vary, depending on the risk and level of exposure of the service to terrorist content.

The establishment of points of contact to facilitate the handling of removal orders and referrals has been designed to improve cooperation between law enforcement authorities and service providers.

With the adopted general approach, the Council is ready to start negotiations. (TW)

Collection of Case Law on Hate Crime

In December 2018, FRA published a [paper looking at the evolution of the ECtHR's case law relating to hate crime](#).

The paper looks at the Court's rulings regarding the duty of state authorities to effectively investigate possible racist motivation under Article 2 ECHR and beyond. Furthermore, it analyses the Court's rulings on hate crimes committed by private persons. Lastly, the paper looks at the duty to investigate when other bias motivations besides racism come into play such as bias related to religious hatred, disability, political opinion, sexual orientation, or gender-based discrimination. (CR)

Online Tool Against Muslim Hatred

At the beginning of December 2018, FRA published a new [online tool](#) to assist Member States, policymakers, and stakeholders when confronted with anti-Muslim hatred.

The database offers information on international, European, national, regional, and local-level case law and rulings relating to hate crime, hate speech, and discrimination against Muslims. It includes the courts' reasoning, findings, and considerations as well as key facts for each case. In addition, the database contains relevant national, European, and international human rights organisation decisions, and reports as well as findings by human rights and equality bodies and organisations.

Users can access research, reports, studies, data, and statistics on these issues. As an online tool, it offers a unique street-level view of victim support services in all 28 EU Member States. It also provides guidance on where to find appropriate information, support, and protection. (CR)

New Structures at FRA


With the aim of responding better to its strategic priorities, FRA started working in a [new configuration](#) on 16 November 2018. The agency created a new Institutional Cooperation and Networks Unit

as well as a new Technical Assistance and Capacity Building Unit next to the existing Research and Data, Communications and Events, and Corporate Services Units. The Institutional Cooperation and Networks Unit shall work closely with FRA's EU, international, and national partners to reinforce human rights systems and frameworks. The Technical Assistance and Capacity Building Unit shall help improve FRA's realtime assistance and expertise. (CR)

Procedural Criminal Law

Data Protection

New Data Protection Framework for EU Institutions

 The European Union has a new legal framework for the protection of personal data processed by Union institutions, bodies, offices, and agencies. The underlying Regulation (EU) 2018/1725 was [published in the Official Journal of 21 November 2018 \(L 235/39\)](#). It repeals Regulation (EC) No 45/2001 and Decision No 1247/2002/EC which date back to the pre-Lisbon era and did not cover the processing of personal data within all Union institutions and bodies.

The main aim of the new Regulation is to adapt its rules to the modern General Data Protection Regulation (Regulation (EU) 2016/679), which has been fully applicable since May 2018. Hence, Regulation 2018/1725 establishes a coherent framework, while guaranteeing the free flow of personal data within the Union. It also sets out provisions on the European Data Protection Supervisor (EDPS). The EDPS is entitled to monitor the application of the provisions of this Regulation to all processing operations carried out by a Union institution or body. He is also the first port of call if complaints are lodged against infringements of an individual's data protection rights.

The Regulation is divided into 12 chapters, including the following:

- General provisions, including scope and definitions;
- General data protection principles;
- Rights of the data subject;
- Controller and processor, including provisions on security of personal data;
- Transfers of personal data to third countries or international organisations;
- EDPS;
- Remedies, liabilities and penalties;
- Review.

Chapter IX contains specific rules on “the processing of operational personal data by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU.” In other words, this concerns activities of Union bodies/offices/agencies (as their main or ancillary tasks) exercised for the purposes of the prevention, detection, investigation, and prosecution of criminal offences. In this event, the tailor-made rules of Chapter IX apply as a *lex specialis*.

It must be noted, however, that the Regulation does not apply to Europol or to the European Public Prosecutor's Office until the legal acts establishing Europol and the European Public Prosecutor's Office (i.e., Regulations No 2016/794 and No 2017/1939) are amended with a view to rendering this chapter (on the processing of operational personal data) applicable to them as adapted. Whether the legal basis of these institutions must be adapted to the Regulation will be assessed in a review process in 2022.

The rules of the Regulation apply from 12 December 2018, with an exception for Eurojust: the Regulation applies to the processing of personal data by Eurojust from 12 December 2019.

In the aftermath of the adoption, the EDPS *Giovanni Buttarelli* welcomed the new data protection rules for EU institutions (see [press release of 11 December 2018](#)). He pointed out:

“The new Regulation, which applies

from today, brings the data protection rules for the EU institutions and bodies (EUI) in line with the standards imposed on other organisations and businesses by the [General Data Protection Regulation](#) (GDPR). Under the new rules, which we may refer to as the EUI-GDPR, the EDPS remains responsible for ensuring the effective protection of individuals' fundamental rights and freedoms whenever their personal data is processed by the EU institutions or on their behalf, whether this is to ensure EU markets work better, to evaluate and supervise medicines in the EU or to fight against terrorism and organised crime."

He also added that the EU institutions should take the lead by example in ensuring the individual's protection of personal data. (TW) ■

The Awakening of EU Data Retention Rules

At the Council meeting of 6–7 December 2018, the JHA ministers of the EU Member States reiterated their [support for EU-wide legislation on data retention](#). They encouraged the continuation of work at the expert level to develop a new concept after the 2006 Directive "on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks" was declared void by the CJEU in 2014 (*"Digital Rights Ireland"*, see eucrim 1/2014, p. 12). In *"Tele2 Sverige"*, the CJEU further prohibited Member States from maintaining national data retention regimes if they entail a general and indiscriminate retention of data (see eucrim 4/2016, p. 164).

After these judgements, an expert group was established in 2017 with the task of exploring avenues to reconcile the demand for effective law enforcement access to retained data (stored for commercial purposes by telecommunication service providers) with the requirements of necessity and proportionality set by the CJEU. (TW)

FRA Handbook on Profiling

In December 2018, FRA published a [handbook aiming to contribute to the prevention of unlawful profiling](#).

The handbook explains what profiling is, when it is unlawful, and what the potential negative impacts of unlawful profiling for law enforcement and border management could be. Furthermore, it explains the principle and practice of lawful profiling and looks at algorithmic profiling and its data protection framework.

The handbook is primarily designed for those responsible for training law enforcement and border management officials. Nevertheless, it may also help officers in mid-level positions to implement profiling techniques lawfully. (CR)

Freezing of Assets

Regulation on Freezing and Confiscation Orders



The European Parliament and the Council adopted a regulation on the mutual recognition of freezing orders and confiscation orders. The new legal framework ([Regulation \(EU\) 2018/1805](#)) was published in the Official Journal of the EU of 28 November 2018 (O.J. L 303/1).

The Regulation replaces the provisions of Framework Decision 2003/577/JHA as regards the freezing of property and Framework Decision 2006/783/JHA as of 19 December 2020. It should be noted, however, that the existing framework continues to apply to Denmark and Ireland, which are not bound by the new Regulation.

The Regulation aims at making the freezing and confiscation of criminal assets across the EU quicker and simpler. The reform was considered necessary because the existing pre-Lisbon legal framework was underused and complex. Depriving criminals of their assets is an important tool in fighting organised crime and terrorism. According to a 2016 Europol study, however, only an

estimated 1.1% of criminal profits are currently confiscated in the EU.

The legislative proposal was controversially discussed; eucrim closely monitored the development of the legislation. See: eucrim 4/2016, p. 165 (Commission proposal), and eucrim 2/2017, p. 73; eucrim 3/2017, p. 117; eucrim 4/2017, p. 176; eucrim 1/2018, p. 27; and eucrim 2/2018, p. 102.

The major "innovation" is that, for the first time, the EU legislator chose a Regulation and not a Directive to govern future cooperation in an area mutually enforcing Member States' orders. Against the opposition of several Member States (including Germany), which favoured a Directive, the provisions of the Regulation will be directly applicable, thus hindering Member States from implementing the EU instrument into their national legal orders. Recital 53 concedes, however, that "(t)he legal form of this act should not constitute a precedent for future legal acts of the Union in the field of mutual recognition of judgments and judicial decisions in criminal matters."

The key features of the new Regulation are as follows:

- The scope has been formulated broadly. According to recital 14, "(t)his Regulation should cover freezing orders and confiscation orders related to criminal offences covered by Directive 2014/42/EU, as well as freezing orders and confiscation orders related to other criminal offences." Thus, the Regulation is not limited to particularly serious crimes with a cross-border dimension.

- It is only decisive that the issuing State issue a freezing or confiscation order "within the framework of proceedings in criminal matters." On the one hand, orders issued within the framework of proceedings in civil and administrative matters have been excluded from the scope of the Regulation. On the other hand, so-called "non-conviction based orders" must be recognised even if such orders might not exist in the legal system of the executing State (cf. recital 13).

■ Grounds for non-recognition and non-execution are provided for in Art. 8 (for freezing orders) and Art. 19 (for confiscation orders). The most hotly debated issue during the negotiations was whether the Regulation should include a (more or less general) refusal ground if fundamental rights were infringed in the issuing state. Germany (in the Council) and the EP favoured the introduction of such a refusal ground; however, the final text was a compromise: Art. 8(1)(f) and Art. 19(1)(h) formulate a refusal ground in the style of the recent CJEU case law in *Arranyosi & Căldăraru* containing a similar refusal ground in cases of European Arrest Warrants. As a result, non-recognition because of fundamental rights infringements will only be possible in exceptional situations.

■ The Regulation foresees several time limits for the recognition and execution of the freezing and confiscation orders respectively. They have been designed to ensure quick and efficient cooperation. As regards freezing orders, for instance, the executing authority should start taking concrete measures necessary to execute such orders no later than 48 hours after the decision on the recognition and execution thereof has been taken. The text of the Regulation does not, however, mention any legal consequences in case of delay.

■ The Regulation contains only a few rules on legal remedies. In essence, reference is made to national law. According to Art. 33, “affected persons” have the right to effective legal remedies in the executing State against the decision on the recognition and execution of freezing orders pursuant to Art. 7 and confiscation orders pursuant to Art. 18. The right to a legal remedy must be invoked before a court in the executing State in accordance with its law. This also includes challenges against measures during the process of execution of the orders (Art. 23(1)). However, the substantive reasons for issuing the freezing order or confiscation order

must be challenged before a court in the issuing State (Art. 33(2)).

■ The Regulation pays special attention to the restitution of frozen property to victims. Accordingly, the compensation and restitution of property to victims should have priority over the disposal of frozen or confiscated property (recital 45). The notion of “victim” is to be interpreted in accordance with the law of the issuing State, which should also be able to provide that a legal person could be a victim for the purpose of this Regulation.

■ Property claims must be demanded in the issuing State (Art. 29(1)). If there is a decision to restitute frozen property to the victim, the issuing authority must inform the executing authority. The executing authority must then take the necessary measures to ensure that the frozen property is restituted to the victim as soon as possible, in accordance with the procedural rules of that State. However, this obligation is subject to three conditions: (1) the victim’s title to the property is not contested; (2) the property is not required as evidence in criminal proceedings in the executing State; and (3) the rights of affected persons are not prejudiced (Art. 29(2)).

■ In order for the affected person to assert his/her claims, he/she must be informed by the executing authority on the execution of a freezing or confiscation order (Art. 32). “Affected person” is defined in Art. 2(10) as “the natural or legal person against whom a freezing order or confiscation order is issued, or the natural or legal person that owns the property that is covered by that order, as well as any third parties whose rights in relation to that property are directly prejudiced by that order under the law of the executing State.”

The annexes of the Regulation contain standardized forms for freezing and confiscation certificates. As other standard forms in EU’s judicial cooperation instruments they are designed to ensure that EU states act faster and communicate more efficiently. (TW)

Cooperation

Judicial Cooperation

Council Conclusions on Mutual Recognition

At their meeting of 7 December 2018, the EU Member States’ Ministers for Justice adopted [Council conclusions on mutual recognition in criminal matters](#). The conclusions contain several calls on the Member States, including the following:

- To implement the procedural rights Directives in a timely and correct manner and to ensure independence and impartiality of the courts and judges;
- To restrictively apply the fundamental rights exception for non-execution of requests in accordance with CJEU case law;
- To make use of alternative measures to detention in order to reduce the population in detention facilities;
- To promote training of practitioners (e.g., judges, prosecutors) and exchanges between practitioners from different Member States;
- To establish (non-binding) guidelines on the application of the EU mutual recognition instruments;
- To make better use of the EJP’s possibilities and platforms;
- To encourage executing authorities to enter into dialogue and direct consultations with the issuing authorities, in particular before considering the non-execution of a decision or judgement;
- To consider the withdrawal of reservations on MLA instruments;
- To set up, as a matter of priority, the e-Evidence Digital Exchange System to ensure the effective exchange of European Investigation Orders and MLA requests.

The Commission has, *inter alia*, been invited to provide practical guidance on the recent CJEU case law, notably regarding the *Aranyosi* case (see eucrim 1/2016, p. 16, and 2/2018, pp. 103 et seq.) and to give reliable and updated in-

formation on penitentiary establishments and prison conditions in the Member States. The latter includes translations of the CoE's fact sheets on detention conditions and treatment of prisoners.

Furthermore, the Commission has been invited to further develop the handbook on the European arrest warrant (see eucrim 4/2017, p. 177) and to communicate notifications by Member States on EU mutual recognition instruments to the EJNI, so that they can be published on the EJNI website. (TW)

CJEU: Obligations of MS if Extradition Sought to Enforce Custodial Sentence for Union Citizens

On 6 September 2016, the CJEU rendered an important judgment in the *Petruhhin* case, giving guidance on whether the extradition of Union citizens from an EU country to non-EU countries is in line with the Union's prohibition of discrimination (see eucrim 3/2016, p. 131). This decision triggered several follow-up references for preliminary rulings, e.g., the *Pisciotti* case (eucrim 1/2018, p. 29) and the *Adelsmayr* case (eucrim 3/2017, pp. 116–117).

Another reference was brought to Luxembourg by the *Korkein oikeus* (Finnish Supreme Court), which essentially wanted to know whether (and, if yes, how) the concept established in *Petruhhin* not only applies to extraditions for the purpose of prosecution but also to those for the purpose of enforcing custodial sentences. The Grand Chamber of the CJEU delivered its judgment in this case (*C-247/17 – Denis Raugevicius*) on 13 November 2018.

►Facts of the Case and Questions Referred

In the case at issue, the Russian authorities requested extradition of Mr. Denis Raugevicius, a Lithuanian and Russian national, from Finland for the purpose of enforcing a custodial sentence of four years' imprisonment for drug possession. Mr. Raugevicius challenged his extradition, arguing that he had lived in Finland for a considerable length of time

and that he is the father of two children residing in Finland and having the Finnish nationality. The *Korkein oikeus* was unsure whether the CJEU's *Petruhhin* judgment posed legal barriers to extradition. On the one hand, Finnish law prohibits the extradition of own nationals to countries outside the EU, but not of citizens having the nationality of another EU Member State (here: Lithuania). On the other hand, international agreements and Finnish law make provision for the possibility that a custodial sentence imposed by a third country on a Finnish national may be served on Finnish territory.

Therefore, the Finnish court, in essence, posed the question of whether Union law also requires extradition alternatives to be applied to Union citizens, so that the effects are less prejudicial to the exercise of the right to free movement.

►The CJEU's Answer

First, the CJEU posits its main findings in the *Petruhhin* judgment:

- A national of an EU Member State (here: Lithuania) who moved to another EU Member State (here: Finland) exercised his right to free movement; therefore this situation falls within the scope of Art. 18 TFEU, which lays down the principle of non-discrimination on grounds of nationality;

- The national rule that prohibits only own nationals from being extradited, and not nationals from other EU Member States, gives rise to unequal treatment;

- This is a restriction on the freedom of movement, within the meaning of Art. 21 TFEU;

- This restriction can be justified only where it is based on objective considerations and is proportionate to the legitimate objective of the national provisions.

Second, the CJEU reiterated that extradition is a legitimate means to avoid the risk of impunity. In the *Petruhhin* case, however, it was possible to settle the conflict with the Union's non-

discrimination rule by giving the EU country of nationality the opportunity to exercise jurisdiction first.

Although this avenue is barred if extradition (by a third country) is sought for the purpose of enforcing a sentence, the requested EU Member State must consider mechanisms that are consistent with the objective of non-impunity, but are less prejudicial to the person's status as Union citizen.

In this context, the CJEU observed that Art. 3 of the Finnish Law on International Cooperation provides foreigners who permanently reside in Finland with the possibility to serve criminal law sanctions imposed abroad in Finland. In fact, Finnish law already provides for comparable situations in which permanent residents who demonstrate a certain degree of integration into the State's society can be treated as Finnish nationals (provided the person concerned as well as the requesting State consent).

The CJEU therefore concluded that Arts. 18 and 21 TFEU require that nationals of other Member States who reside permanently in Finland and whose extradition is requested by a third country for the purpose of enforcing a custodial sentence should benefit from the provision preventing extradition from being applied to Finnish nationals and may, under the same conditions as Finnish nationals, serve their sentences on Finnish territory.

►Put in Focus

In further development of the *Petruhhin* doctrine, the CJEU's judgment first means that, in situations in which extradition requests from third countries collide with issues of enforcing custodial sentences, EU Member States must also pay attention to the rights of nationals of other EU Member States. The CJEU made clear that alternative, mechanisms less prejudicial to extradition, which apply to own nationals, must also be extended to Union citizens.

In a second line of reasoning, however, the CJEU established an important restriction: Member States may apply

this equal treatment on the condition that the Union citizen is a permanent resident and has demonstrated its integration into the Member State's society. In this context, previous CJEU case law on who can be considered a "permanent resident" must be recalled. The CJEU also emphasised that the person concerned may face extradition "on the basis of applicable national or international law" if the courts of the requested Member State cannot establish a "permanent residence."

This ruling and the exception to it may trigger further references for preliminary rulings. The present ruling seems fitting for the Finnish case, specifically the situation of the person sought (Mr. Raugevicius) and the particular circumstances of Finnish law that include foreigners in the cross-border enforcement of custodial sentences.

Several questions remain:

- What if national law only confers the possibility to serve foreign custodial sentences to its own nationals?
- Which degree of integration must a Union citizen have in the requested EU Member State?
- To what extent does the State's obligations go under the traditional principle of "*aut dedere aut iudicare*"? (TW)

European Arrest Warrant

CJEU: Surrender of Resident if Executing State Unable to Enforce Custodial Sentence

On 13 December 2018, the CJEU decided on a request for a preliminary ruling that concerned the interpretation of Art. 4 No. 6 FD EAW in conjunction with the divergent levels of sanctioning among the EU Member States.

►Facts of the Case

In the case at issue (C-514/17 – *Sut*), Belgium was requested to execute a one-year-and-two-month custodial sentence against *Marin-Simion Sut* for having driven a vehicle without valid licence plates and without, for not having a valid

driving licence, and for having caused an accident. Mr. Sut is a Romanian national, but has lived in Belgium since 2015 where he is working with his spouse. In the proceedings on the execution of the Romanian arrest warrant, the Belgian Public Prosecutor argued that the Belgian provision implementing Art. 4 No. 6 FD EAW cannot be applied. According to Art. 4 No. 6 FD EAW, the execution of an EAW may be refused "if the EAW has been issued for the purposes of execution of a custodial sentence, where the requested person is staying in, or is a national or a resident of the executing Member State and that State undertakes to execute the sentence in accordance with its domestic law."

►The Legal Question

The Belgian Public Prosecutor affirmed that Mr. Sut is a "resident staying in the executing Member State" within the meaning of Art. 4 No. 6 FD EAW. According to Belgian law, however, the offenses at issue can be punished by fines only, but conversion of a custodial sentence into a fine is expressly prohibited. Therefore, the Romanian sentence cannot be enforced in Belgium and the EAW must be executed, hence Mr. Sut surrendered.

The referring *Cour d'appel de Liège* (Court of Appeal, Liège) had doubts on this interpretation with regard to previous CJEU case law, which stresses the importance of the requested person's reintegration into society when the sentence imposed on him expires.

►Decision and Reasoning of the CJEU

The CJEU pointed out that the optional ground for non-execution according to Art. 4 No. 6 FD EAW requires two conditions to be satisfied in the case at issue:

- The person requested must be a "resident" of the executing Member State;
- The custodial sentence passed in the issuing state against that person can actually be enforced in the executing state (while the latter can consider that there is a legitimate interest which would justify the execution of the sentence).

The CJEU further noted that Union law allows a certain margin of discretion when implementing Art. 4 No. 6 FD EAW. In addition, the more the national legislator limits the situations in which its national authorities may refuse surrender, the more they reinforce the surrender system in favour of building up an area of freedom, security and justice.

Against this background, the CJEU recognised the importance of potentially increasing the requested person's chances of reintegrating into society when the sentence imposed on him expires, but this cannot prevent a Member State from limiting the refusal grounds such to give effect to the fundamental principle of mutual recognition enshrined in Art. 1(2) FD EAW. Therefore, the executing authority may give effect to an EAW if the executing state is not able to actually enforce the custodial sentence.

This is a rather unfavourable result for the requested person. The CJEU, however, left one back door open: the Belgian courts must ascertain whether the consequence in the case at issue (i.e., Belgium not being in the position of enforcing the custodial sentence) is really indispensable under Belgian law. In this context, two issues must be considered:

- Art. 4 No. 6 FD EAW does not give any indication that the executing authority is precluded from refusing the execution of a EAW if the law of this state provides only for a fine in response of the offence to which the EAW relates;
- The margin of discretion for the national legislator when implementing Art. 4 No. 6 FD should be taken into account.

As a result, it is ultimately up to the referring court whether the Romanian EAW must be executed, even though the defendant has economic and family ties in Belgium and enforcement is only be hindered because Belgium foresees a lighter penalty for the offense at issue. The case shows the repercussions of the different levels of sanctioning in the EU. (TW)

CJEU: Consequences of Failure to Refer to Additional Sentence in EAW

On 6 December 2018, the CJEU delivered its judgment in [Case C-551/18 PPU](#), which concerns the execution of a European Arrest Warrant (EAW) issued against IK. The judgment mainly concerns the interpretation of Art. 8 FD EAW (entitled “content and form of an EAW”), but also Art. 15 (communication of supplementary information) and Art. 27 (rule on speciality).

►Facts of the Case

In the case at issue, IK was sentenced to a primary custodial sentence of three years for sexual assault (main sentence). In the same judgment, the court ordered an “additional sentence of release conditional to placement at the disposal of the *strafuitvoeringsrechtbank* (Court for the enforcement of custodial sentences) for a 10-year period.” Under Belgian law, this additional sentence takes effect after the expiry of the main sentence and, for the purpose of its enforcement, the Court responsible for the enforcement of custodial sentences is to decide whether the convicted person must be deprived of liberty or whether he can be released conditionally. Accordingly, the person “shall be deprived of his liberty if there is a risk of him committing serious offences that undermine the physical or psychological integrity of third parties which, in the context of release under supervision, cannot be offset through the imposition of special conditions.”

Since IK had left Belgium, the Belgian judicial authorities issued a EAW against him for the enforcement of the sentence. They indicated the main sentence, the nature and legal classification of the offences and the relevant legal provisions, and outlined the facts, but did not mention the additional sentence imposed on IK. The *Rechtbank* Amsterdam/the Netherlands, ordered the surrender of IK to Belgium for the purposes of serving the custodial sentence in Belgium for the offense of sexual assault.

IK was surrendered and put in custody for the main sentence. In the subse-

quent proceedings before the Court for the enforcement of custodial sentences in Antwerp/Belgium, which decided on the additional sentence, IK claimed that the court cannot take this decision because the additional sentence was not subject to the surrender by the Dutch authorities.

In the following, the Dutch authorities denied a request by the Belgium authorities, which sought additional authorisation in respect of the additional sentence pursuant to Art. 27 FD EAW. The Dutch authorities argued that Art. 27 concerns the sentencing or prosecution of an offence other than the one for which surrender was authorized, which did not apply to the present case.

The Antwerp court then rejected IK’s arguments and ordered the maintenance of his deprivation of liberty.

►Reference for the Preliminary Ruling

Upon appeal, the *Hof van Cassatie* (Court of Cassation) decided to refer the case to the CJEU, asking about the impact of the failure to mention the additional sentence in the EAW on the further proceedings regarding this sentence in Belgium.

The main question was, in essence, whether non-compliance with Art. 8(1) (f) of the FD EAW, which provides for the necessity to include in the EAW request the penalty imposed, precludes the enforcement of the additional sentence.

►Decision and Reasoning of the CJEU

At first, the CJEU reiterated the main principles of the EAW scheme that had already been mentioned in previous judgments:

- The EAW is based on mutual trust that requires each of the EU Member States, save in exceptional circumstances, to consider all the other Member States to be in compliance with EU law and particularly with the fundamental rights recognised by EU law;

- Based on the principle of mutual recognition, the EU system of surrender replaces the conventional multilateral system of extradition;

- The FD EAW seeks to facilitate and accelerate judicial cooperation by contributing to the attainment of the Union’s objective of becoming an area of freedom, security and justice;

- The FD EAW pursues the policy that the crime committed does not go unpunished;

- Refusal to execute a EAW is only possible on the grounds for non-execution exhaustively listed in the FD EAW (Arts. 3–5); accordingly, execution of the EAW is the rule, whereas refusal is the exception.

Although the CJEU decided that failure to comply with the formal requirements of Art. 8(1) FD EAW can result in the executing authority not giving effect to a EAW (cf. Case C-241/15, *Bob-Dogi*, eucrim 2/2016, p. 80), the CJEU observes that it must be examined to what extent failure to indicate an additional sentence in a EAW affects the exercise of jurisdiction that the executing authority derives from Arts. 3–5 FD EAW.

The CJEU put forth that the purpose of Art. 8(1)(f) is to give information, so that the executing authority can decide whether it has to refuse the EAW because the thresholds of Art. 2(1) FD EAW for the execution of a custodial sentence (min. four months) have not been ascertained. In the present case, this threshold was unproblematic (the main sentence against IK was three years’ imprisonment). Hence, the executing authority could do nothing but grant the surrender.

As a result, the CJEU ruled that, in circumstances such as those at issue in the main proceedings, the fact that the European arrest warrant did not indicate the additional sentence cannot affect the execution of that sentence in the issuing Member State following surrender.

Subsequently, the CJEU dealt with several counterarguments and dismissed them. In particular, it reasoned as follows:

- The rule of speciality, as referred to in Art. 27 FD EAW, does not apply in the present case, because it only concerns

offences other than those on which the surrender was based;

- Failure to indicate the additional sentence does not trigger the reporting mechanism of Art. 15(3) FD EAW; therefore, the executing judicial authority need not be informed of the additional sentence in advance.

Ultimately, the CJEU pointed out that the rights of the person concerned were guaranteed. He can challenge the maintenance of the deprivation of liberty before the Belgian courts.

► *Put in Focus*

After the *Bob-Dogi* judgment, the CJEU delivered another judgment on the consequences of failure to comply with the formal requirements of an EAW. In essence, it links the requirements of Art. 8 FD EAW with the substantial refusal grounds in Art. 3 et seq. FD. If the failure to comply formally has no effect on the jurisdiction of the executing authority, enabling it to apply one of the listed refusal grounds, the formal failure is negligible. The person concerned is referred to the legal remedies as provided for in the legal order of the issuing state.

The judgement also clarifies the applicability of the rule on speciality (Art. 27 FD EAW) and the scope of the reporting mechanism of Art. 15(3) FD EAW. (TW)

Law Enforcement Cooperation

Council Pushes for E-Evidence Law, EP Applies the Brakes

On 7 December 2018, under the Austrian Presidency, the JHA Council [agreed on its position](#) on a proposal for a regulation on European production and preservation orders for e-evidence in criminal matters (for the proposal, see [eucrim 1/2018](#), pp. 35–36 and the article by *S. Tosza* in this issue). The new legal framework foresees that judicial and law enforcement authorities can quickly obtain and efficiently secure evidence stored electronically by directly sending

respective orders to service providers. If service providers do not comply with the orders, they can be sanctioned. The location of the data should no longer play a role.

Debate in the Council was controversial, however, with seven Member States, including Germany, disagreeing with the [general approach of the Council](#). The countries particularly raised concerns about overly harsh infringements of the fundamental rights to privacy and the protection of personal data.

The major amendment proposed by the Council in comparison to the Commission is the establishment of a – limited – notification system: if content data are concerned and if the issuing authority believes the person whose data are sought is not residing on its own territory, the issuing authority must inform the enforcing state and give it an opportunity to flag whether the data requested may fall under the following categories:

- Data protected by immunities and privileges;
- Data subject to rules on determination and limitation of criminal liability related to freedom of expression/the press;
- Data whose disclosure may impact fundamental interests of the state.

The issuing authority shall take these circumstances into account, and it shall not issue or adapt the order. The notification does not entail a suspensive effect. Such notification procedure was requested from several parties, since it follows similar rules in international cooperation in criminal matters, e.g., the interception of telecommunication data without the need for technical assistance of a requested state.

Meanwhile, the European Parliament dampened expectations that it will finalise the legislation by the end of the parliamentary term in May 2019. During a [hearing organised by the \(mainly responsible\) LIBE Committee](#), MEPs voiced critical concerns over the Commission proposal. In a [working document](#), the main rapporteur, *Birgit Sippel*

(S&D, Germany), took up the criticism already put forward by legal experts, practitioners, and NGOs (also see in this regard [eucrim 1/2018](#), p. 36; [2/2018](#), pp. 107–108, and [3/2018](#), pp. 162–163). She pointed out that the serious legal questions must be addressed in a comprehensive manner and concluded:

“With regards to the numerous consultations conducted so far (in shadows’ meetings, the LIBE hearing, as well as in bilateral meetings with involved parties), but also publications received (in particular an assessment of the Commission’s proposals on electronic evidence, commissioned by the EP Policy Department for Citizens’ Rights and Constitutional Affairs at the request of the LIBE Committee), the Rapporteur together with the shadows has identified several legal areas that will need further clarification, in order to guarantee the drafting of a legally sound legal instrument regarding the production and preservation of e-evidence.” (TW)

Civil Society Organisations Voice Concerns over Council Plans on E-Evidence

Eighteen civil society organisations urged Member States to seriously reconsider its draft position on law enforcement access to “e-evidence” on the eve of the vote on the general approach in the Council. In a [letter of 5 December 2018](#), the organisations point out that the draft presented by the Austrian Presidency fails to solve the fundamental concerns of the e-evidence proposal (for the proposal, see [eucrim 1/2018](#), pp. 35–36 and the article by *S. Tosza* in this issue; for other critical reactions, see [eucrim 2/2018](#), pp. 107–108, and [3/2018](#), pp. 162–163). In particular, the following issues have been raised:

- Considerable reduction in the possibility for enforcing authorities to refuse recognition and enforcement of an order on the basis of a violation of the Charter of Fundamental Rights;
- Erroneous assumption that non-content data is less sensitive than content

data, contrary to CJEU and ECtHR case law;

- Contemplation of the possibility to issue orders without court validation, disregarding CJEU case law (e.g., in *Tele 2 Sverige*);
- Failure to provide legal certainty;
- Undermining of the role of executing states, thereby undermining judicial co-operation.

In sum, the concerns over fundamental rights already raised have grown even more with the new text. (TW)

US CLOUD Act: EU Wants Executive Agreement with the U.S.

With the “CLOUD Act” of March 2018, the U.S. rushed ahead in facilitating law enforcement access to data held by U.S. service providers, such as Microsoft, Facebook, and Google. It also gave foreign law enforcement authorities the possibility to bypass existing MLA procedures and to directly request communication content of “non-U.S. persons” located outside the U.S. from U.S.-based providers, subject to specified requirements (see *eu crim* 1/2018, p. 36).

One pre-condition is the conclusion of an “executive agreement” with the “foreign government,” which must meet a number of criteria (e.g., adequate substantive and procedural laws on cybercrime and e-evidence, respect for the rule of law, non-discrimination and respect for human rights, accountability and transparency mechanisms, etc.). Requests must be limited to “serious crimes.” For the U.S. CLOUD Act and the executive agreements, see the article by *J. Daskal* in this issue.

The conclusion of an executive agreement is subject to a positive determination by the U.S. Attorney General before it is submitted to the US Congress. The EU and the U.S. agreed that the U.S. will negotiate one agreement with the EU instead of bilateral agreements with individual Member States. The [Commission and the Council are preparing the mandate](#) in order to start the negotiations. (TW)

New Measures to Disrupt Migrant Smuggling Networks

With the aim of disrupting migrant smuggling networks, both inside and outside the EU, the Council approved a [set of measures with a law enforcement focus](#) on 6 December 2018. These new measures shall enhance the inter-agency approach, both at EU and national levels, make the best use of synergies among the operational tools available, and maximise the use of the external assets of the EU.

Hence, the operational and analytical capacities of the European Migrant Smuggling Center (EMSC) at Europol shall be increased and a stronger link between frontline information and information analysis capacities established. Furthermore, a joint liaison task force on migrant smuggling shall be set up within the EMSC. In order to better disrupt online communications, Europol’s EU Internet Referral Unit shall be strengthened. (CR)



Council of Europe*
Reported by Dr. András Csúri

Foundations

European Court of Human Rights

20th Anniversary of European Court of Human Rights

On 1 November 2018, it was the [twentieth anniversary of the entry into force of Protocol No. 11](#) and the setting up of a single, full-time ECtHR. The protocol also established the right of individual petition to over 800 million Europeans. Following the entry into force of Protocol No. 11 on 1 November 1998, the new, permanent Court replaced the existing European Commission and Court of Human Rights in order to strengthen the efficiency of the protection of human rights and fundamental freedoms. In the last 20 years, the new Court has dealt with more than 800,000 applications, delivering nearly 21,000 judgments.

Speaking at a [seminar](#) organized during the Finnish presidency of the CoE on 26 November 2018, ECtHR President *Raimondi* hailed the establishment

of the new Court as a landmark in the development of international human rights protection. He further noted that only a little over 58,000 applications are currently pending before the Court, which is down from the high number of 160,000 applications pending in 2011.

First Case for Advisory Opinion under Protocol No. 16

On 3 December 2018, the Grand Chamber panel of five judges accepted a request for an advisory opinion under Protocol No. 16. This is the [first case \(received on 16 October 2018 from the French Court of Cassation\)](#) since the entry into force of Protocol No. 16 to the ECHR on 1 August 2018 (see *eu crim* 2/2018, p. 109). The case raises questions on legal mother-child relationship and compliance with the requirements of Article 8 of the Convention when regis-

* If not stated otherwise, the news reported in the following sections cover the period 16 November – 31 December 2018.

tering the birth of a child born abroad to a surrogate mother.

Protocol No 16 allows the highest courts and tribunals to request the ECtHR to give advisory opinions on questions of principle relating to the interpretation or application of the rights and freedoms defined in the Convention or its protocols. An advisory opinion may be requested only in the context of a case pending before a domestic court. A panel of five judges decides whether to accept or reject the request. The advisory opinions given by the Grand Chamber provide reasons and are not binding.

Specific Areas of Crime

Corruption

GRECO: Fifth Round Evaluation Report on Estonia

On 7 December 2018, GRECO published its [fifth round evaluation report on Estonia](#). The main focus of this evaluation round is on preventing corruption and promoting integrity in central governments (top executive functions) and law enforcement agencies. The evaluation sets particular focus on issues such as conflicts of interest, the declaration of assets, and accountability mechanisms (for the fifth evaluation round, see eucrim 2/2017, p. 76; for more recent reports, see eucrim 1/2018, pp. 38–39 and 2/2018, pp. 109–110).

In general, GRECO observed that the comprehensive legislative framework and online tools in place in Estonia provide a sound basis for preventing corruption amongst all officials. There are, however, a number of areas in which improvements are necessary and recommended. Currently, a code of conduct is lacking that would cover all relevant government actors (ministers, senior civil servants, and political advisers). GRECO recommends laying down clear standards, illustrated by concrete examples of the risk of conflicts of in-

terest. These standards should be made clear to anyone taking up a government position from the outset. In addition, political advisers, like ministers and senior civil servants, should also submit declarations of interest as part of their recruitment process, so as to identify any conflicts of interest. While acknowledging the good level of transparency of the legislative process in Estonia, GRECO sees room for further improvement by clear rules on reporting as well as disclosure by ministers, senior civil servants, and political advisers of contact to lobbyists/third parties that seek to influence the public decision-making process. The report further recommends the adoption of rules to prevent the risks of revolving doors – when government officials shift to the private sector – with a view to preventing lobbying of the government or the immediate acceptance of employment in a sector that was previously within the remit of their government duties.

The report acknowledges that, over the last several years, the Police and Border Guard Board has built up a strong practice to prevent corruption within its own ranks, which has also led to an increased level of public trust. GRECO further welcomes that the Estonian police service reportedly has the highest percentage of women in Europe, yet recommends improving gender representation at higher management levels within the police.

The report recommends focusing on two particular issues in order to prevent conflicts of interest in the police service: the increasing number of police officers taking up secondary employment in addition to their regular police work, on the one hand, and the type of employment they take after they leave the Police and Border Guard Board, on the other. The report also recommends reviewing the safeguards in place when it comes to internal police investigations. In addition, GRECO calls for improvements regarding the process of appointing the Director General of the Police and Border

Guard Board, the rotation of police staff working in areas exposed to particular risks of corruption, and the protection of whistleblowers.

Money Laundering

MONEYVAL: Fifth Round Evaluation Report on Albania

On 17 December 2018, MONEYVAL published its [fifth-round evaluation report on Albania](#). The fifth evaluation round builds on previous MONEYVAL assessments by strengthening the examination of how effectively Member States prevent and combat ML and terrorism financing (TF). See also eucrim 1/2018, pp. 40–41 and 2/2018, p. 111 with further references. The report calls on the Albanian authorities to step up their efforts in pursuing launderers, when confiscating assets connected to significant proceeds-generating offences and in tackling terrorist financing risks.

Corruption poses major money laundering risks in Albania. Often linked to organised crime activities, it generates substantial amounts of criminal proceeds and seriously undermines the effective functioning of the criminal justice system. The authorities are aware of the risks from corruption, but law enforcement has paid limited attention to targeting corruption-related ML so far. A significant judicial reform is currently being implemented to better address the corruption risks prevalent in the country.

MONEYVAL acknowledges that the Albanian authorities have a reasonably good understanding of the country's ML risks and have at their disposal national coordination mechanisms for policy-making to address risks. However, these mechanisms have not proven fully effective. Therefore, the report recommends enhancing the analysis of ML and TF risks to implement appropriate mitigation measures, most notably by way of:

- Conducting a more in-depth TF risk assessment;
- Understanding the impact of the in-

formal economy and of corruption (including its nexus with organised crime) on ML/TF risks;

■ Assessing the risk posed by legal persons (including through ownership/control by foreign legal arrangements).

The competent authorities systematically use wide-ranging sources of information to initiate and facilitate investigations of ML, associated predicate offences, and terrorist financing. However, these investigations rarely result in indictments. ML proceedings connected to significant parallel proceeds-generating offences are usually suspended or dismissed by the prosecution. Therefore, MONEYVAL recommends reviewing the reasons behind the low performance of the prosecution in ML investigations and pursuing more indictments in ML cases involving foreign proceeds. To this end, better use could be made of circumstantial evidence concerning the predicate crimes committed abroad if such evidence is available.

Though Albania has a robust legal framework for confiscation of criminal proceeds, the number and value of seized and confiscated assets is not commensurate with the level of criminality in the country. MONEYVAL recommends ensuring that adequate efforts are made to identify criminal proceeds located abroad and take appropriate actions for their confiscation.

With regard to terrorist financing, MONEYVAL notes that the perception and understanding of the related risks does not seem to adequately address the characteristics of potential TF activities in the country and the Western Balkan region. There is no systematic approach towards identifying and investigating financing aspects of terrorism-related offences.

MONEYVAL acknowledges that the Bank of Albania has a good understanding of ML and TF risks, recently enhancing its offsite reporting system to support its assessment of risks of individual entities. However, inspections by the Financial Supervisory Authority (FSA) have

Council of Europe Treaty	State	Date of ratification (r) signature (s) of accession (a) entry into force (e)
Protocol amending the Additional Protocol to the Convention on the Transfer of Sentenced Persons (ETS No. 222)	Holy See Ukraine Turkey Italy Lithuania	15. January 2019 (a) 12. April 2018 (s) 6. March 2018 (s) 20. February 2018 (s) 12. January 2018 (s)
Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (ETS No. 217)	Lithuania Sweden Hungary European Union Turkey Portugal France Montenegro Armenia Czech Republic	1. January 2019 (e) 1. January 2019 (e) 1. December 2018 (e) 1. October 2018 (e) 1. June 2018 (e) 13. March 2018 (r) 1. February 2018 (e) 1. February 2018 (e) 24. January 2018 (s) 1. January 2018 (e)
Council of Europe Convention against Trafficking in Human Organs (ETS No. 216)	Slovenia Croatia Portugal Costa Rica Albania Czech Republic Malta Moldova Norway Montenegro Armenia	6. December 2018 (s) 29. November 2018 (s) 8. November 2018 (r) 16. April 2018 (s) 1. March 2018 (e) 1. March 2018 (e) 1. March 2018 (e) 1. March 2018 (e) 1. March 2018 (e) 16. February 2018 (s) 24. January 2018 (s)
Protocol No. 16 to the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 214)	Belgium Luxembourg Armenia Ukraine Estonia Finland France San Marino Slovenia Lithuania Georgia Albania Bosnia and Herzegovina Andorra	8. November 2018 (s) 6. September 2018 (s) 1. August 2018 (e) 1. August 2018 (e) 1. August 2018 (e) 1. August 2018 (e) 1. August 2018 (e) 1. August 2018 (e) 1. August 2018 (e) 1. August 2018 (e) 1. August 2018 (e) 11. May 2018 (s) 12. April 2018 (s)
Protocol No. 15 amending the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 213)	Greece Spain Bosnia and Herzegovina Belgium Ukraine Malta Croatia	5. October 2018 (r) 20. September 2018 (r) 11. May 2018 (s) 4. April 2018 (r) 22. March 2018 (r) 16. January 2018 (r) 9. January 2018 (r)
Fourth Additional Protocol to the European Convention on Extradition (ETS No. 212)	Ukraine France Russia	1. March 2019 (e) 2. October 2018 (s) 1. September 2017 (e)

Council of Europe Treaty	State	Date of ratification (r) signature (s) of accession (a) entry into force (e)
Convention on the counterfeiting of medical products and similar crimes involving threats to public health (ETS No. 211)	Portugal Switzerland Benin Russia Turkey	1. April 2019 (e) 1. February 2019 (e) 1. September 2018 (e) 1. July 2018 (e) 1. January 2018 (e)
Third Additional Protocol to the European Convention on Extradition (ETS No. 209)	Ukraine France Moldova Romania Lithuania Switzerland Turkey	1. March 2019 (e) 2. October 2018 (s) 1. May 2018 (e) 1. January 2018 (e) 1. May 2017 (e) 1. November 2016 (e) 1. November 2016 (e)
Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (ETS No. 201)	United Kingdom Norway	1. October 2018 (e) 1. October 2018 (e)
Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (ETS No. 198)	Liechtenstein Denmark Greece Russia	26. November 2018 (s) 1. June 2018 (e) 1. March 2018 (e) 1. January 2018 (e)
Council of Europe Convention on the Prevention of Terrorism (ETS No. 196)	European Union Czech Republic	1. October 2018 (e) 1. January 2018 (e)
Additional Protocol to the Criminal Law Convention on Corruption (ETS No. 191)	Czech Republic	1. January 2019 (e)
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)	Paraguay Morocco	1. November 2018 (e) 1. October 2018 (e)
Convention on Cybercrime (ETS No. 185)	Ghana Paraguay Cabo Verde Argentina Morocco Philippines Costa Rica	1. April 2019 (e) 1. November 2018 (e) 1. October 2018 (e) 1. October 2018 (e) 1. October 2018 (e) 1. July 2018 (e) 1. January 2018 (e)
Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182)	Spain Hungary Austria	1. July 2018 (e) 1. May 2018 (e) 1. March 2018 (e)
Additional Protocol to the Convention on the Transfer of Sentenced Persons (ETS No. 167)	Holy See Spain Turkey	1. May 2019 (e) 1. November 2017 (e) 1. September 2016 (e)
Convention on the Transfer of Sentenced Persons (ETS No. 112)	Holy See India	15. January 2019 (a) 1. May 2018 (e)
Second Additional Protocol to the European Convention on Extradition (ETS No. 098)	France	2. October 2018 (s)

Latest Update: 4 February 2019 (by Thomas Wahl). The complete table is available at: <https://eucrim.eu/ratifications/>

been very limited so far, even though the authority is in the process of transitioning to a risk-based approach in supervision. Despite important efforts, neither the Bank of Albania nor the FSA consistently apply a risk-based perspective when reviewing applications for licences by financial institutions or take a systematic approach to monitoring them in order to fully mitigate the risk of criminal infiltration. Therefore, MONEYVAL recommends:

- Ensuring the implementation of high standards (which should include a comprehensive framework of screening applicants/indirect shareholders);
- Assessing criminal records beyond criminal convictions, current proceedings, and potential links to criminal associates;
- Obtaining international cooperation whenever appropriate;
- Implementing ongoing mechanisms to check the integrity status of exiting licences.

Albania has reportedly provided mutual legal assistance with an appropriate level of cooperation, but the general legal mechanism for executing foreign mutual legal assistance requests shows deficiencies. Therefore, the report recommends taking legislative steps to simplify the existing legal framework for executing MLA requests and introducing a case management system (CMS), which also allows for the systemic prioritisation of MLA cases for all authorities involved. Furthermore, direct cooperation between counterpart judicial authorities should be encouraged.

Based on the results of its evaluation, MONEYVAL decided to apply its enhanced follow-up procedure to Albania.

MONEYVAL: AML/CFT Report on Israel Triggers the Country's Membership to the FATF

On 10 December 2018, FATF and MONEYVAL published a [mutual assessment report on Israel's](#) anti-money laundering and counter-terrorist financing (AML/CFT) system, the effectiveness of

measures in place, and their level of compliance with FATF Recommendations.

Israel became an observer to the FATF in February 2016. Until then it had already been closely involved in the work of the FATF through its participation in MONEYVAL. Since the start of its observer status in February 2016, Israel has worked to meet the requirements for full membership of the FATF, which include undergoing a successful mutual evaluation. With publication of the assessment report, Israel met FATF's membership requirements and became an official member of FATF with immediate effect.

The report underlines that Israel's geographic location means it faces a particularly high terrorist financing (TF) risk from external sources. Specific TF sources and channels identified by the report are:

- Funding from other jurisdictions;
- Supposedly legitimate business activities;
- Donations;
- Foreign non-profit organisations (NPOs);
- Smuggling of goods, valuables, and funds through border crossings, including through trade; and the use of money transfer mechanisms.

Fraud, tax offences, organised crime and public sector corruption are among the ML risks.

As regards risk assessment and policy setting, the report states that Israel has a good understanding of the risks it is exposed to, has developed a sound and effective AML/CFT system, demonstrates an effective policy of timely prevention,

and achieves good results in investigating, prosecuting, and convicting ML and TF. Great emphasis is also placed on depriving criminals of the illicit gains, assets, and instruments of crime at an average of over €24 million per year in confiscations.

However, the report identified areas requiring major improvement:

- Introducing and strengthening the supervision and implementation of preventive measures;
- Coordination in preventing the misuse of non-profit organisations for TF, in particular by increasing Israel's resources to register and supervise these organisations.

Financial institutions and their supervisors have a good understanding of the ML and TF risks they face. This understanding is weaker in the money service sector, though there has been a significant increase in this sector's reporting of unusual activities recently. Financial supervisors generally have not yet developed a full, risk-based AML/CFT-specific supervision. Israel has not included real estate agents, dealers in precious metals, and trust and company service providers in its AML/CFT system. Lawyers and accountants are not required to report suspicious transactions. Among the recommendations related to financial institutions, the report suggests ensuring that all financial institutions, especially smaller firms, apply adequate background checks when hiring new employees, instead of just relying on applicants' self-assessment. Furthermore, it calls on financial institutions to continue providing up-to-date

and AML/CFT-specific training to staff.

The supervisors of designated non-financial businesses and professions (DNFBPs) have a reasonable understanding of ML/TF risks and obligations, but are at an early stage in the development of a risk-based model for supervision. The report recommends the following in this regard:

- Extending AML/CFT obligations to all DNFBPs that are currently not covered by the national AML/CFT regime;
- Developing and enhancing their understanding of ML/TF risks and obligations;
- Updating supervised entities and self-regulatory bodies on how their sectors could be misused for ML/TF purposes;
- Verification of customer and transaction information in a timely manner and on a regular basis by DNFBPs.

Furthermore, diamond dealers should apply adequate background checks when hiring new employees.

Authorities must make effective use of financial intelligence and other information and co-operate well with international counterparts. That said, some issues have arisen with delays in executing requests for international cooperation. In this regard, the report recommends continuing with the planned increase in human resources to assist in the timely execution of MLA requests, to improve the response time for incoming extradition requests (whether through additional resources or dedicated staff to handle such requests or through enhanced interaction with foreign counterparts), and to streamline the process for handling incoming MLAs requiring investigative action.

Fil Rouge

The European Union already has an impressive track record when it comes to the protection of its citizens' data. Yet the challenges posed by the digital revolution are not limited to protecting people's privacy, but also require finding effective ways to access data when need be, including for criminal investigations. The lack of a comprehensive framework in that respect currently results in more informal solutions based on the voluntary cooperation of service providers, not necessarily with due regard to the protection of fundamental rights. This problem is also a good example of a broader phenomenon linked with the technological revolution: the role of service providers as partners in law enforcement. Their role is not only instrumental in the gathering of e-evidence, but also, for instance, in the fight against the dissemination of illicit content online.

The contributions in this issue of *eu crim* touch upon all these difficulties. The first two articles – by *S. Tosza* and by *J. Daskal* – deal with the same problem: law enforcement access to data held by service providers for the purpose of criminal investigation. As data is very often held in a different country than the place of criminal investigation, the complexity of instruments necessary to obtain such data is

out of proportion. *S. Tosza* presents the EU initiative aimed at creating a legal framework for direct requests for electronic evidence sent by law enforcement authorities in the EU to service providers in another EU Member State (the “e-evidence initiative”). *J. Daskal* discusses the recent changes in U.S. law, which should facilitate the transfer of data from U.S. service providers to authorities in the EU.

The immense growth in data-analysing capacities has thrown into question the traditional classification of data, as even non-content data may be extremely revealing when gathered in sufficient quantity and properly analysed. *C. Warken* critically analyses the current approach to classifying data and proposes a new take on the matter.

G. Robinson examines the European Commission's proposal for a Regulation on preventing the dissemination of terrorist content online. This highly relevant initiative largely relies on the good cooperation of service providers, including their proactive role.

Katalin Ligeti, University of Luxembourg and *eu crim* Editorial Board Member & *Stanislaw Tosza*, University of Utrecht

The European Commission's Proposal on Cross-Border Access to E-Evidence

Overview and Critical Remarks

Dr. Stanislaw Tosza

With human activity becoming more and more dependent on digital technologies, criminal investigations increasingly depend on digital evidence. Yet the gathering of this type of evidence is far from straightforward. Besides technological challenges, one of the major obstacles that law enforcement authorities encounter is the fact that the data they need is often stored abroad or by a foreign service provider. At the international level, this results in the need to resort to mutual legal assistance and, at

the EU level, to the European Investigation Order. Even the length of the procedure when resorting to the EIO is far too slow, because relevant data can be lost in the meantime. This article discusses the initiative of the European Commission to establish a European legal framework regarding direct requests for electronic evidence sent by law enforcement authorities in the EU to service providers in another EU Member State (the “e-evidence initiative”). The initiative, which is currently under debate in the EU Parliament after the Council agreed on proposed amendments, is not without controversy. The article analyses its overall structure and the most important aspects of its design, and it offers critical remarks on several major elements of the initiative.

I. Introduction

A large number of criminal offences, not only cybercrime, is currently committed in a way that leaves digital traces that can serve as evidence. In order to effectively investigate and prosecute these offences, law enforcement must have access to digital data, which is mostly in the possession of service providers, often located abroad. The law of criminal procedure allows the authorities to access this data, while protecting suspects’ procedural safeguards. However, when the service provider is located in another country or the data is stored abroad, law enforcement should in principle resort to mutual legal assistance (MLA) because their coercive powers are limited to their national territory.

As the significance of digital or electronic evidence has grown, so has the frustration of law enforcement with the cumbersome procedure to acquire this data in combination with the number of cases when digital evidence is needed and the relevant data is held abroad. This has stimulated attempts to find unilateral solutions forcing providers to deliver data not stored in the territory of the requesting state circumventing the MLA procedure, which resulted in significant litigation,¹ and calls for reform of the framework. The latter is not an easy undertaking, as the complexity of the issue is composed of problems linking criminal procedure, international law, in particular questions of jurisdiction and sovereignty in the context of criminal investigations, EU law as well as the impact of fast developing technology, in particular cloud computing or encryption.²

With the Conclusions of 9 June 2016 the JHA Council requested the Commission to develop a legal framework that would allow law enforcement to obtain relevant data.³ This request led to the proposal of the Commission of 17 April 2018 that is composed of two instruments: a regulation and a directive.⁴ The aim of this contribution is to provide an overview of and a few critical remarks on the Commission’s proposal, in particular focusing on the draft regulation, which is the main component of the legislative initiative.

At the same time, legislative work has also progressed in the U.S., with the ultimate adoption of the CLOUD Act in March 2018, which is meant to facilitate access to data held by U.S.

companies by non-U.S. law enforcement authorities. This act is the subject of the contribution by *Jennifer Daskal* in this issue of *eu crim*.

II. Commission’s Proposal

The envisaged regulation would create two new instruments: a European Production Order (EPdO) and a European Preservation Order (EPsO).⁵ An EPdO is defined as “a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence” (Art. 2(1) of the draft regulation⁶). An EPsO is “a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to preserve electronic evidence in view of a subsequent request for production” (Art. 2(2)). It is interesting to note that an EPsO may result not only in an EPdO, but also for instance in a mutual legal assistance request or a European Investigation Order (Art. 6(2)).

The crucial characteristic of the Commission’s proposal is that the orders go from the issuing authority in one Member State directly to the service provider in another Member State and the data should go back the same way. The involvement of an authority in the executing state is, in principle, avoided and the basic check of the order is done by the service provider. In order to guarantee the effectiveness of the regulation, the second piece of the Commission’s proposal, i.e. the directive, obliges the Member States to provide for a framework assuring that there is a known and empowered legal representative of a service provider to whom the order may be addressed. The choice both of the legal basis and of the legal instrument is noteworthy: The directive, which must be transposed by the EU Member States, has an internal market legal basis (see also 2. below), whereas the – binding and directly applicable – regulation is based on Art. 82(1) TFEU, which provides for judicial cooperation in criminal matters on the basis of the mutual recognition principle. While being a regulation, a number of issues will have to be clarified by national law, most notably sanctions and remedies (see below).

1. Draft Regulation

a) What may an order be issued for?

The EPdO and the EPsO have the same objective: they oblige the service provider to respectively produce or preserve electronic evidence. The term “electronic evidence” is explained in Art. 2(6). This definition is characterised by three elements: Firstly, evidence must be stored in an electronic form either by the service provider or on its behalf. Secondly, it has to be stored at the time of receipt of the EPdO or EPsO. This means that the order concerns the data that is already in the possession of the service provider and not any data to be obtained in the future, thus excluding any future surveillance. Thirdly, the term evidence is not defined as such, but the definition provides for four types of data of which that evidence might consist: subscriber data, access data, transactional data and content data.

These four categories of data are further defined in the draft regulation in Art. 2(7)–(10). The spectrum includes content and non-content data, with the latter being divided into three categories (subscriber data, access data, transactional data). In terms of infringement of fundamental rights, the regulation provides two groups of categories of data: subscriber and access data on the one hand, which are considered less intrusive, and transactional and content data, where the intrusiveness is deemed more significant. The differentiation particularly affects the possibility of using the order, which is limited to some categories of offences for the second group, whereas it is open to all offences for subscriber and access data. Furthermore, the differentiation has an impact on the radius of the action of the prosecutor’s, who is excluded from the list of competent issuing authorities when it comes to transactional and content data. As per the Explanatory Memorandum to the proposal, the differentiation between the two categories is made according to the following philosophy: data related only to the identification of the user is less intrusive and can be made more accessible, whereas data involving predominantly the content of a person’s activity should be more protected.⁷ The Explanatory Memorandum considers that the starting point of an investigation is often the subscriber data or access data in order to reveal the identity of the suspect, before data about the content is sought.

b) Who may issue the order?

While the Member States may differ as to which authorities they give the right to ask for data from service providers in the national context, the draft proposes a quasi-harmonised approach in that regard. It should be borne in mind, that no margin of discretion is allowed, because no implementation of

the provisions of a regulation is needed (see above). The Commission singled out three categories of authorities that can be entitled to issue an EPdO or EPsO (Art. 4).

The first group contains authorities that are entitled to issue both types of orders and for all types of data: judges, courts and investigative judges. The second group is composed of prosecutors whose authority is limited to what the draft considers to be less sensitive measures (cf. recital 30 of the preamble). Prosecutors may issue an EPsO for any type of data, but an EPdO only for subscriber and access data. Given the fact that a regulation (and not a directive) will be enacted, it does not seem to be possible for the Member States to restrict the circle of authorities entitled to issue the orders, e.g. by further limiting the power of the prosecutor. As a result, it may happen that a prosecutor might be in the position to issue an EPsO for content data at the European level, while he or she would not be able to do so in a purely domestic context.

The third group is defined as follows: “any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law.” Such orders will need to be examined for their conformity with the conditions set out for the validity of the orders. The authorities entitled to validate the order are the same two (aforementioned) groups as those for issuing the orders, according to the same range of competences (with the prosecutor’s competence limited to the less intrusive types of data). In other words, the third category would include authorities that are equipped with the necessary power to gather electronic evidence according to the national laws of the Member States. Thus, prosecutors can also be entitled to ask for transactional and content data, but with the necessary authorisation and conferral of powers is at the discretion of the national legislator. The language of the draft indicates that a piece of national legislation would be necessary in this respect because, contrary to other instances (e.g. Art. 5(2)), the draft regulation does not refer to similarities with national rules or comparable domestic situations.

c) Who is the recipient of the order?

The recipient of the order is a service provider offering services in the Union and established or represented in another Member State. A service provider can be a natural or a legal person and is otherwise defined by the services it offers, which, according to Art. 2 (3), can be:

- Electronic communication services;
- Information society services;
- Internet domain name and IP numbering services.

These categories are explained in more detail in the Explanatory

tory Memorandum and use also references to other acts. In practice, the first two categories (electronic communication services and information society services) comprise such services as Skype, WhatsApp, Amazon, Dropbox and mailing services.⁸ As to the last category of the definition of service providers (Internet domain name and IP numbering services), the Explanatory Memorandum makes reference to the providers of Internet infrastructure services that hold data potentially of high relevance in identifying the suspect.⁹

Another requirement is that providers of the services described above fall within the scope only if they are offering services in the Union and are established or represented in another Member State. These terms are further explained in the Directive itself (Art. 2(4)) and in the Explanatory Memorandum.¹⁰ Mere accessibility of the service from the territory of the European Union cannot be a sufficient criterion, as this would cause every provider in the world to fall within the scope. Furthermore, the service provider has to be established or represented in *another* EU Member State, since otherwise there would be a purely domestic situation, which is excluded from the scope.

An EPdO or an EPSO should be addressed directly to a legal representative that the service provider shall designate for the purpose of gathering evidence in criminal proceedings (Art. 7(1)). The efficiency of this approach is supported by the proposed Directive (see below 2.) and alternative addressees if such a representative is not designated (cf. Art. 7(2)–(4)).

d) Under what conditions may the order be issued?

The draft regulation provides for a set of common conditions for issuing EPdOs and EPSOs as well as specific conditions for each of them. The first common condition is that the order may be issued only for criminal proceedings, which includes the pre-trial and the trial phase (Art. 3(2)). According to Art. 3(2), the order may also be issued in proceedings against legal persons, where these persons may be held liable or punished. This formulation excludes any sort of double criminality requirement in this respect: even if the executing Member State does not provide for criminal liability of legal persons, the order still needs to be executed.

The second condition applicable to both orders refers to necessity and proportionality. The draft regulation distinguishes, however, between the two types of orders if it comes to the reference point of the evaluative criteria, which is founded in the different objectives of these instruments. The EPdO must be necessary and proportionate for the purpose of the criminal proceedings in question (Art. 5(2)). By contrast, the EPSO must be necessary and proportionate to prevent the removal,

deletion or alteration of data in view of a subsequent mutual legal assistance request, a European Investigation Order or an EPdO (Art. 6 (2)).

Two additional conditions limit the issuing of an EPdO, both referring to the national law of the issuing Member State. First, a similar measure must be available for the same criminal offence in a comparable domestic situation. This excludes the use of the EPdO in an issuing Member State that does not provide for such a measure in this context, thus limiting the harmonising effect of the regulation and positioning the applicability of the EPdO within the realm of national law. This limiting effect must, however, be relativized: firstly, the limitation affects the power of the national authority, but not the foreign one. Secondly, the formulation does not state that the condition of application must be identical.

A second additional condition foresees that the application of the EPdO is also limited depending on the type of data and the type of offence in question. In case of subscriber or access data, the issuance of an EPdO is allowed for any criminal offence, whereas the issuing of an EPdO for transactional or content data is limited to two groups of offences. The first group refers to the national law: the EPdO may be issued for “offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years.” The second one makes reference to framework decisions and directives (which harmonised substantive criminal law in specific fields) and allow national authorities to issue an EPdO regardless of the severity of punishment on the national level in the following cases:

- Fraud and counterfeiting of non-cash means of payment;
- Sexual abuse and sexual exploitation of children and child pornography;
- Attacks against information systems;
- Terrorism.

e) Execution

The EPdO or EPSO will be transmitted to the recipient through certificates.¹¹ The certificates are to be issued according to the models annexed to the draft regulation (Annex I and II). Some flexibility is granted as far as the transmission of the certificate is concerned. Any means are acceptable provided that they are capable of producing a written record and allow to establish the authenticity of the certificate (Art. 8).

Tight deadlines are foreseen for the execution of the orders (Art. 9). As far as the EPdO is concerned, the draft distinguishes as follows: in regular cases, the service provider should transmit the data to the issuing authority at the latest within 10 days from the moment of receiving the certificate. In emergen-

cy cases, which are defined as an “imminent threat to life or physical integrity of a person or to a critical infrastructure,”¹² this deadline is brought down to 6 hours. An EPsO has to be executed without “undue delay”.

f) Enforcement

In order to guarantee the practical effectiveness of the instrument, while taking into account potential reservations and constraints on the side of the service provider or other affected persons, the regulation provides for a set of procedures and tools, some of which are prescribed by the regulation itself, and some of which require intervention on the part of the national legislator. On the one hand, in order to accommodate the interests of the service providers, the regulation provides for instruments of dialogue¹³ between law enforcement and service providers in addition to remedies for the latter, the suspects and accused persons as well as for other persons whose data were obtained. On the other hand, in order to guarantee effectiveness of the measures, there are procedures for enforcement which engage authorities in the executing Member State and eventually pecuniary sanctions.

After receiving the order, the service provider would have to perform a check of the order. The draft regulation provides this as a right, but on many occasions the check will instead be a duty because of the contractual relationship with the user or data protection rules. According to the draft, there are three groups of reasons which may create difficulties for the service provider to comply with the order and for which the regulation provides ways of remedying the situation. The objections shall be transmitted to the issuing authority by using a standard form (annexed to the draft regulation).

The first group of reasons concerns the situation when the order is incomplete, contains manifest errors or does not contain sufficient information to execute. In this case, the service provider may ask for clarification. The reasons of the second group arise if the service provider is unable to execute the order because of *force majeure* or *de facto* impossibility, e.g. either because the order does not concern their customer or because the data has been deleted already. If the issuing authority confirms the objection, it shall withdraw the order. The third group of reasons is described as “other”. So, for any other reason that the service provider does not provide the requested data within the deadline or does not provide it exhaustively, it shall also send the annex to the issuing authority explaining the reasons for failing to provide the data. The only potential consequence of this action is that the issuing authority shall review the order and, if necessary, set a new deadline. This does not seem to oblige the authority to withdraw the order even if there is good reason to do so.

If the addressee does not comply with the order and the above dialogue procedure does not cause the issuing authority to accept the reasons provided, the issuing authority may transfer the order to the competent authority in the executing Member State. This transforms the procedure into a more traditional mutual recognition process: the enforcing authority should recognise the order, except if there are grounds to oppose, which are enumerated in Art. 14(4) or (5), immunity or privilege under national law, or if its disclosure may impact its fundamental interests such as national security and defence.

So far, the above rules apply to both types of orders (EPdO and EPsO). The draft regulation provides, however, an additional reason for the service provider not to provide information if it comes to the EPdO. This reason is an example of the above-mentioned “other” reasons and refers to an EPdO that “cannot be executed because based on the sole information contained in the [order] it is apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive.” In this case, the service provider must send the respective annex to the enforcement authority in the Member State of the addressee. The latter authority may then seek clarification from the issuing authority, including through Eurojust or the European Judicial Network.

The impact of this rule is problematic. While it seemingly concerns a fundamental question – a significant abuse – it seems only procedural in nature: it requests that another authority be informed, an authority which may be potentially involved if the enforcement is needed. How should this fundamental rights clause be construed? Should it be read as if the violation or abuse is not manifest, it is not a ground to object? Or should it merely be read as saying, that if the violation or abuse is not manifest, the other authority should not receive the annex at this stage? If this provision is read together with the enforcement part, one notices that the executing state authority cannot oppose the execution of the order if it finds that it violates the Charter or that it is abusive, unless the violation/abuse is manifest. It results from this interpretation that, without the fulfilment of this adverbial condition (“manifestly”), the abuse or violation have no relevance and the execution of the EPdO would be obligatory. This is a highly questionable outcome. In addition, the Explanatory Memorandum does not explain how to interpret the word “manifest,” which usually means “obvious” or “clearly apparent.” Yet, an abuse is an abuse irrespective of whether it is visible *prima facie* or not. If the court in the executing member state reveals its abusiveness, why should it not be allowed to oppose the order just because it was not possible to spot it *prima facie*?

g) Sanctions and remedies

The draft regulation contains provisions on sanctions (Art. 13) and remedies (Arts. 15–17), although these are relatively restrained, making mostly reference to national law. The Member States are also obliged to put in place provisions on pecuniary sanctions applicable to service providers in the event of infringements of their duties (as described above). While the sanctions do not need to be of a criminal nature, they have to be effective, proportionate and dissuasive. The proposal does not clarify who shall impose a sanction and who should enforce it. It is also not clear whether good reasons to refuse providing information on the part of the service provider, such as a (non-manifest) violation of the Charter or a (non-manifest) abuse of the order (see f) above), may be taken into account in the process of imposing such sanctions.

The draft regulation further contains a chapter entitled “Remedies”, which complements the measures described above and grants rights not only to the service providers, but also to suspects and accused persons as well as other persons whose data were obtained. Except for the service providers, the remedies concerning all the other persons are to be provided by national law. Such right to an effective remedy shall be exercised before a court in the issuing state and must offer the possibility to challenge the legality of the measure, including its necessity and proportionality. The issuing authority is also responsible for informing the interested persons about that right (Art. 17). Within this framework these persons should be able to address issues of violation of the Charter or the abuse of the order.

It should also be underlined, that Art. 1(2) of the draft regulation contains the same clause as Art. 1(3) of the Framework Decision on the European Arrest Warrant, which has recently resulted in cases where the execution of the EAW was put under question or refused because of fundamental rights concerns.¹⁴ It cannot be excluded that the clause could result in similar questioning of the orders based on the same or similar concerns.

The service providers' right to remedy is limited to conflicts of laws and affects only the EPdO. This remedy is meant to take into account situations in which the service provider would find itself in a situation where the order obliges it to provide information although the applicable law of a third country prohibits it. According to the Explanatory Memorandum, this approach should also encourage non-EU countries to respect the limitations that the providers falling into the scope of this regulation face, in particular as regards fundamental rights concerns, including data protection.¹⁵ The remedy applies if compliance with the EPdO would result in a conflict with the applicable law of a third country prohibiting disclosure of the data concerned:

- On the grounds that this is necessary to either protect the fundamental rights of the individuals concerned or the fundamental interests of the third country in relation to national security or defence (Art. 15);
- On other grounds (Art. 16).

It is expressly stated that the conflict cannot be based just on the lack of a similar procedure in the third country or on the fact that the data is stored in that country. The service provider shall inform the issuing authority about the existence of the conflict. If the issuing authority intends to uphold the EPdO, it shall request a review by the competent court in the issuing Member State. The court shall verify if the law of the third country applies and if it is so, whether the service provider is prohibited from disclosing the information. The verification can have several consequences:

- If the court finds no relevant conflicts of law, it shall uphold the order;
- If the court finds that there is a conflict because of “other grounds,” the court lifting of the order is not mandatory. The court must (only) consider the conflict when evaluating a number of criteria specified in Art. 16(5) that are based on the requirements of data protection, investigation and the addressee's interests;
- If the conflict is grounded in the protection of the fundamental rights of the individuals concerned or of the fundamental interests of the third country in relation to its national security or defence, a central authority of the third state is engaged. This authority shall respond within 15 days (a deadline that may be extended upon request from that authority), whether it objects to the execution of the EPdO. Such an objection obliges the court in the issuing state to lift the order. Lack of response of the authority results in a reminder with a five days deadline and if that brings no reaction, the order shall be upheld. It is worth noticing that the authority in the third state is not obliged to comply with the deadlines. While questions of national security or defence may be a sufficient motivation for the authority to comply with the deadline, the protection of fundamental rights may not in all cases. Then, such an authority in the third country may only be motivated by comity or by the will to protect the service provider because of its connection with the third state.

2. Draft Directive

The draft directive obliges the Member States to set up rules ensuring that service providers offering services in the European Union designate at least one legal representative in the Union empowered to receive and respond to the orders described in the regulation. In order for the regulation to be effective, it is crucial that the name of such representative is

made known, also in view of relatively short deadlines that the regulation imposes for the execution of the orders.

Some Member States have already created such obligations – at the national level – to nominate a service provider’s representative. This action is, however, in conflict with the internal market logic: imposing mandatory legal representation within the territory of a Member State is in conflict with the freedom of services within the internal market.¹⁶ Therefore, the directive aims not only to assure the possibility of an effective enforcement of the EPdO and EPsO, but also to avoid the risk that other Member States launch further unilateral initiatives in this regard, creating divergent legal frameworks and further obstacles to the internal market. Hence, the directive is issued on an internal market legal basis, which is explained by its aim. While the problem described affects the service providers that are not established in a Member State in question, it does not exist if they have already been established. As a consequence, and similarly to the draft regulation, the directive does not affect service providers offering services exclusively in the territory of one EU Member State.

The obligation to “designate at least one legal representative in the Union for the receipt of, compliance with and enforcement of decision and order issued by competent authorities of Member States for the purpose of gathering evidence in criminal proceedings” concerns service providers established in the European Union as well as those that are not established in the Union, but offering services in the territory of the Member States concerned (Art. 3 (1) and (2) of the draft Directive). The latter means that such a service provider should have a substantial connection to the Member State. The meaning of substantial connection is the same as for the draft regulation (see above 1c).¹⁷ In order to guarantee the fulfilment of these duties, the Member States should also provide for effective, proportionate and dissuasive sanctions applicable for infringements of these duties and make sure that they are implemented (Art. 5).

III. Next Steps

The Commission’s proposal has already been subject to some analysis at the request of the European Parliament¹⁸ as well as by the academic community,¹⁹ civil society²⁰ and industry.²¹ The Council as well as the European Parliament have been discussing the proposal for the regulation. The Council reached an agreement on 7 December 2018 proposing a number of amendments to the Commission’s draft.²² The following are among the most important amendments:

- Including into the scope of application of the regulation that an order may also be issued for the purpose of the execution

of custodial sentences or detention orders (with exceptions) (Art. 3);

- Deleting the subsection on orders being manifestly abusive or manifestly violating fundamental rights (Art. 9(5));
- Adding to the provision on sanctions that pecuniary sanctions – of up to 2% of the total worldwide annual turnover of the service provider’s preceding financial year – can be imposed (Art. 13);
- Abolishing the differentiation between the two remedies for service providers regarding a conflict of law; according to the new design, the mandatory opinion of the authority of the third country is abolished, and only seeking information from that authority is allowed; it is not obligatory to lift the order, regardless of the conflict of law (Arts. 15 and 16);
- Adding for the EPdOs concerning content data a procedure requesting notification of the authority of the enforcing Member State if there are reasonable grounds to believe that the person whose data is sought is not residing in the territory of the issuing Member State; this procedure, which was one of the major issues discussed in the Council, is meant to safeguard rights stemming from immunities and privileges (new Art. 7a);²³
- Including the speciality principle providing limitations on the use of electronic evidence other than for the purpose of the proceedings for which it was obtained and its transmission to another Member State, third country or international organisation (new Art. 12b).

Following these conclusions, the Council is ready to start the trilogue negotiations with the European Parliament. Yet, work on the Directive is still ongoing within the Council, which hopes to reach an agreement under the Romanian Presidency.²⁴ As to the regulation, the Parliament still has to agree on its position, which is being prepared first and foremost by the LIBE Committee. The committee requested two reports²⁵ and held a public hearing on 27 November 2018, while the designated rapporteur issued a working document, which should help steer further discussion.²⁶ It is difficult to predict whether the agreement can be achieved before the end of the parliamentary term, given the number of critical voices within the Parliament and also the fair number of reservations on the part of Member States that were expressed during the discussions in the Council.²⁷

1 On the *Microsoft Corp. v. United States* known as Microsoft Ireland case, see J. Daskal, “Microsoft Ireland, The CLOUD Act, and International Lawmaking 2.0”, (2018) 71 *Stan. L. Rev. Online*, 9. For a description and critical analysis of the cases against Yahoo and Skype in Belgium, see V. Franssen, “The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?”, (2017) 3 *Eur. Data Prot. L. Rev.*, 534, 538 et seqq.

2 For a complex analysis of legal and technical challenges see K. Ligeti and G. Robinson, "Cross-Border Access to Electronic Evidence: Policy and Legislative Challenges", in: S. Carrera, and V. Mitsilegas (eds.), *Constitutionalising the Security Union: Effectiveness, rule of law and rights in countering terrorism and crime*, 2017, pp. 99–111, as well as K. Ligeti and G. Robinson, "Transnational Enforcement of Production Orders for Electronic Evidence. Beyond Mutual Recognition?", in: R. Kertand A. Lehner (eds.), *Vielfalt des Strafrechts im internationalen Kontext: Festschrift für Frank Höpfel zum 65. Geburtstag*, 2018, pp. 625–644. See also: S. Carrera, G. González Fuster, E. Guild, and V. Mitsilegas, *Access to Electronic Data by Third-Country Law Enforcement Authorities*, Centre for European Policy Studies, Brussels 2015.

3 <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/council_conclusions_on_improving_criminal_justice_in_cyberspace_en.pdf> accessed on 29.01.2019.

4 The Commission issued in 2017 a non-paper: "Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward" and conducted public consultation. Furthermore, it issued an impact assessment. All documents can be found here: <<http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-cross-border-access-to-e-evidence>> accessed 21 December 2018. For the legislative proposals themselves, see COM (2018) 225 final [draft Regulation] and COM (2018) 226 final (draft Directive). See also T. Wahl, "Commission Proposes Legislative Framework for E-Evidence", *eurim* 1/2018, 35–36.

5 The abbreviations proposed by the Regulation are rather unfortunate, i.e. "EPOC" for the production order and "EPOC-PR" for the preservation order. This is confusing because both words – production and preservation – start with the letters "PR". The author suggests and uses the abbreviations "EPdO" and "EPsO". These abbreviations are much easier for an immediate recognition which instrument is being referred to. They would also be much easier for the respective certificates, hereinafter: "EPdOC" and "EPsOC".

6 If not stated otherwise, references to Articles in the following refer to the draft regulation.

7 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Explanatory Memorandum, pp. 14–15. For an alternative proposal regarding a new categorization of data in the context of fundamental rights interferences, see the article of C. Warlen in this issue.

8 V. Franssen, "The European Commission's E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement?", *European Law Blog* (12 October 2018), <<https://european-lawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/>> accessed on 29.01.2019.

9 Explanatory Memorandum, p. 14.

10 Explanatory Memorandum, p. 15.

11 Again, the regulation uses confusing abbreviations: EPOC and EPOC-PR. This article proposes to use EPdOC and EPsOC instead (see note 5).

12 Art. 2(15) of the draft regulation. Critical infrastructure is defined by reference to the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection – Art. 2(a).

13 As the Explanatory Memorandum puts it: Explanatory Memorandum, p. 19.

14 ECJ, 5 April 2016, Joined Cases C404/15 and C659/15 PPU, *Aranyosi and Căldăraru*; ECJ, 25 July 2018, Case C-216/18 PPU, *LM*.

Dr. Stanislaw Tosza

Assistant Professor at Willem Pompe Institute for Criminal Law and Criminology; Researcher at Utrecht Centre for Regulation and Enforcement in Europe (RENFORCE). Faculty of Law, Economics and Governance, Utrecht University



15 Explanatory Memorandum, p. 21.

16 Recital 3 of the Directive.

17 Recital 13 of the Directive.

18 See E. Sellier and A. Weyembergh *Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation*. The study is of a more general nature, but touches upon the e-evidence proposals well. It can be retrieved from the Internet via the following link: <http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/10-10/IPOL_STU2018604977_EN.pdf> accessed on 29.01.2019. See further M. Böse, *An assessment of the Commission's proposals on electronic evidence*: <[http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU\(2018\)604989_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf)> accessed on 29.01.2019.

19 Inter alia: V. Franssen, *op. cit.* (n. 8); G. Robinson, "The European Commission's e-Evidence Proposals", (2018) 3 *European Data Protection Law Review*, 347; T. Christakis, "E-Evidence in the EU Council: The Key Issue of When One Member State Can Review the Requests from Another", posted on October 1, 2018 at the *Cross Border Data Forum* <<https://www.crossborderdataforum.org/e-evidence-in-the-eu-council-the-key-issue-of-when-one-member-state-can-review-the-requests-from-another/>> accessed on 29.01.2019.

20 <<https://cdt.org/insight/cdt-recommendations-for-improving-the-european-commissions-e-evidence-proposals/>> accessed on 29.01.2019.

21 <<http://www.euroispa.org/e-evidence-euroispa-adopts-position-paper/>> accessed on 29.01.2019; <<https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/>> accessed on 29.01.2019.

22 Council Interinstitutional File: 2018/0108(COD).

23 The future of this provision will be particularly interesting because a large number of Member States made reservations to this provision. See also T. Christakis "'Big Divergence Of Opinions' On E-Evidence In The EU Council: A Proposal In Order To Disentangle The Notification Knot", posted on 22 October 2018, <<https://www.crossborderdataforum.org/big-divergence-of-opinions-on-e-evidence-in-the-eu-council-a-proposal-in-order-to-disentangle-the-notification-knot/>> accessed on 29.01.2019.

24 Council of the European Union, "Regulation on cross border access to e-evidence: Council agrees its position", *Press Release of 7 December 2018*.

25 See note 18.

26 <<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NON SGML+COMPARL+PE-631.925+02+DOC+PDF+V0//EN&language=EN>> accessed on 29.01.2019.

27 S. Stolton, "Council makes half-hearted agreement on e-Evidence", *euractiv* (7 December 2018), <<https://www.euractiv.com/section/digital/news/council-makes-half-hearted-agreement-on-e-evidence/>> accessed on 29.01.2019.

Unpacking the CLOUD Act

Jennifer Daskal

This article seeks to demystify the recently enacted Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted in March 2018 by the U.S. government in an effort to address challenges faced by law enforcement in accessing data located across borders. It explains the two parts of the act, dealing with: (i) U.S. access to data located outside the United States; and (ii) foreign government access to data held by U.S. companies within the United States. As the article highlights, the CLOUD Act offers a model for both responding to law enforcement needs and setting – and raising – baseline privacy protections. In that regard, it is a step in the right direction, although there is much more work to be done.

I. Introduction

In March 2018, the United States enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act, mooted a pending Supreme Court case, detailing the reach of U.S. law enforcement authority over extraterritorially located data, and setting out a mechanism for foreign governments to gain expedited access to U.S.-held data in specified circumstances.¹

The Act has generated controversy both within and outside the United States. Critics described it as having been “rushed” through Congress at the expense of privacy and civil liberties.² Others decried the “expansion of US enforcement power.”³ But, as this article explains, the rhetoric does not match the reality.

That said, there remain key, unresolved issues that need to be worked out, both by U.S. courts and in coordination with foreign partners in Europe and elsewhere; how these issues are resolved will go a long way towards determining the effectiveness of the Act as well as its effect on both privacy and security.

It is true that the legislation was tacked onto an omnibus spending bill at the 11th hour. But it was not the surprise that some have suggested. On the contrary, key elements had been the subject of hearings in both the House and Senate judiciary committees and in multiple other open, informal congressional briefings.⁴ What ultimately became Part II of the Act was something that had been actively pursued by the Obama administration and ultimately also supported by the Trump administration. Tech companies, law enforcement officials, academic experts, and members of civil society were involved in a multi-year discussion of the issues; many representatives actively lobbied members of Congress both for and against key provisions.⁵ An earlier version of the CLOUD Act had been previously proposed as a stand-alone bill.⁶

Moreover, whereas much of civil society argued – both before and after – the Act’s passage that the baseline protections included in the second part of the Act do not sufficiently protect privacy and civil liberties, those baseline requirements are a *floor* – not a ceiling. Specifically, the Act authorizes the executive branch of the United States to enter into agreements with foreign governments, pursuant to which foreign governments can gain expedited access to U.S.-held data. In so doing, it sets out the *minimal* requirements that each and every agreement must meet. The envisioned agreements also impose a number of use-based limitations, mandating, for example, the secure storage of any disclosed data, deletion or segregation of non-relevant information, and limits on when the data can be shared. They also require that foreign partners agree to periodic reviews to ensure that the requirements are met.

In many areas, even these minimal requirements are more robust than what would be required if governments were able to compel the production of sought-after communications content pursuant to their existing domestic rules; this provides an incentive for governments to raise standards to meet the minimal requirements – an incentive that will ultimately enhance privacy protections above and beyond the status quo.

In addition, the first part of the Act, which clarifies the reach of US law enforcement over extraterritorially held data, is neither the kind of sea change nor the enforcement grab that some have suggested.⁷ Prior to December 2013, when Microsoft first challenged a U.S.-issued warrant based on the fact that the sought-after data was located outside the territorial borders of the United States, providers regularly responded to U.S.-issued disclosure orders without regard to the location of the data being sought. A company like Google operates what has been called by a “data shard” model,⁸ referring to the fact which the data of even a single account is sometimes broken up and moved from place to place, in many cases across inter-

national borders, for reasons of performance and efficiency. As of 2017, Google did not have a mechanism in place to ascertain where all of its data was located at any given point in time.⁹ It only developed the tools to ascertain data location when, as a result of court rulings, it was required to do so.

As with all legislation, the CLOUD Act was the product of negotiated compromise; it is, as a result, inherently imperfect. Among other flaws, it does not contemplate the possibility of multilateral agreements, thereby leaving unresolved key questions about the possibility and contours of a potential US-EU agreement;¹⁰ adopts a new conflict-of-law provision yet only applies it in very limited circumstances; fails to tackle the critically important issue of user notice; and neglects to provide explicit protection for companies that seek to provide transparency over foreign government requests for data. But it also reflects a much-needed attempt to respond to the changing needs of law enforcement, establish new mechanisms to address these needs, and lay out minimal substantive and procedural standards to govern law enforcement in the process. In so doing, it responds to three emerging realities:

- The increased digitalization of information;
- The power of third-party private companies that manage and control so much of that data;
- The increased internationalization of investigations, with either the data of interest or the provider that controls that data located across an international border.

As just one measure of these developments, a recent European Commission report found that law enforcement sought data held by extraterritorially-located service providers in over 55% of EU law enforcement investigations.¹¹ In many cases, that jurisdiction is the United States – a reality that the CLOUD Act tries, in part, to deal with. The first section of this article seeks to move past the rhetoric and demystify the CLOUD Act by explaining and analysing its two key parts. The second section highlights some of the key issues left to be resolved.

II. Unpacking the CLOUD Act

The CLOUD Act contains two key parts. Part I clarifies the reach of US law enforcement to access data held extraterritorially by US-based providers. Part II authorizes the executive to enter into agreements with foreign governments, pursuant to which foreign governments can bypass the otherwise applicable mutual legal assistance requirements in specified circumstances and according to baseline substantive and procedural requirements. The next two subsections provide details on each of these two parts.

1. The reach of US law enforcement

Just one month before the CLOUD Act's enactment, the Supreme Court heard oral arguments in what is often referred to as the *Microsoft Ireland* case. The case dates back to December 2013, when Microsoft was served with a warrant for emails, pursuant to the Stored Communications Act (SCA), as part of a drug-related criminal investigation. The sought-after emails were stored in Dublin, Ireland, and Microsoft refused to comply with the warrant as a result. According to Microsoft, warrants issued pursuant to the SCA are territorially limited and thus only could compel the production of data that was stored within the territorial jurisdiction of the United States.

The U.S. government acknowledged that the warrants authorized by the SCA do not have extraterritorial effect. But it emphasized that Microsoft was a U.S.-based company that could access and control the data from within the United States. According to the U.S. government, the fact that the particular 0s and 1s were located outside the United States did not matter. What mattered was the location of access and disclosure – all within the territory of the United States.

In sum, both parties agreed that warrants issued under the SCA are territorially limited. But they strongly disagreed as to whether or a warrant issued on a U.S.-located company for data located outside the United States was a territorial or extraterritorial exercise of the warrant authority. To resolve this dispute, the justices needed to identify the intent behind, and thus focus of, the SCA – a 30-plus-year-old statute that did not directly address the question posed. At the oral argument, several justices suggested that this was an issue better dealt with by Congress than the courts.¹²

And in fact, Congress stepped in just one month later, passed the CLOUD Act and answered the key unresolved question, and thereby mooted the Supreme Court case.

Consistent with the government's position in the case, the CLOUD Act specifies that providers are, in response to lawful process, required to disclose responsive communications content within their possession, custody, or control, regardless of the location of that data.¹³ But Congress also recognized the risk of conflicts with foreign law, particularly in situations in which the request seeks extraterritorially held data of a foreign national. It thus created a new statutory basis for providers to move to quash based on a conflict with foreign law, albeit only in those limited circumstances in which the conflict is with a "qualifying foreign government" and the United States seeks the data of a non-U.S. person located outside the United States.¹⁴ To become a qualifying foreign government, the government must have entered into an executive agreement with

the United States as authorized pursuant to Part II of the Act. To date, there are *zero* such qualifying governments although that is likely to change over time as will be described below.¹⁵

Congress further noted the possibility that separate comity claims could be considered under “common law” standards in those circumstance in which statutory provision does not apply.¹⁶ This would arise if, for example, a provider alleged that a compelled disclosure order conflicted with foreign law prohibiting such disclosure. Courts would then be in a position of weighing the relevant equities in deciding whether to continue to compel disclosure of the sought-after data. Notably, these kinds of claims could be made before and after the CLOUD Act’s enactment; the CLOUD Act merely notes a continuation of the status quo. That said, Congress’s explicit recognition of the need for courts to address legal conflicts gives credibility to such claims if and when they do arise.

As far as is known, no such claims of conflict in response to the issuance of U.S. warrants have yet been raised.¹⁷ Even in the *Microsoft Ireland* case, neither Microsoft nor Ireland asserted a direct conflict of law. In its amicus brief to the Supreme Court, Ireland emphasized that it was willing and ready to respond to a mutual legal assistance request for the sought-after data. But it never actually asserted that Microsoft would violate Irish law if it were compelled to disclose the data.¹⁸ That said, such conflicts are likely to emerge over time, given, in particular, transfer restrictions included in the EU’s General Data Protection Regulation and as discussed below.¹⁹

2. Foreign law enforcement to U.S.-held data

Part II of the CLOUD Act responds to the converse problem foreign governments face with respect to their ability to access communications content held by U.S. service providers. The same statute at issue in *Microsoft Ireland*, namely the SCA, blocks US-based providers from disclosing communications content to foreign law enforcement. Instead, foreign law enforcement authorities are required to make a government-to-government mutual legal assistance request for such data, even if they are seeking the data of one of their own citizens or residents in connection with a local crime. This is a time-consuming process involving a Department of Justice review of the request, a U.S. attorney’s office going to court to obtain a warrant on behalf of the foreign government, and a subsequent review by the Department of Justice before the data is ultimately disclosed.²⁰ A 2013 report found that it took an average of ten months for the U.S. government to respond, even in those situations in which it agreed to turn over the data.²¹

Foreign governments are increasingly frustrated by this reality, given, in particular, the fact that US-based companies control such a significant quantity of the world’s data and given the ways in which these requirements thwart the efforts to swiftly and efficiently investigate crime. Paddy McGuinness, the UK’s former Deputy National Security Advisor, twice testified before the U.S. Congress about the ways in which the provisions blocking direct disclosures to foreign law enforcement were hampering the U.K.’s ability to investigate and prevent crime.²²

To address these concerns, Congress authorized the executive branch to enter into agreements with foreign governments, pursuant to which the partner government could directly request communications content from U.S.-based providers, subject to specified requirements, without having to employ the mutual legal assistance process. In order to be eligible, the foreign government must first be certified by the Attorney General, in conjunction with the Secretary of State, as “afford[ing] robust substantive and procedural protections for privacy and civil liberties.”²³ Each individual request must also meet specified requirements, including those that the requests be particularized, in compliance with the foreign government’s domestic law, based on “articulable and credible facts” and subject to review or oversight by a court, judge, or magistrate or other independent authority of the requesting foreign government.²⁴ Requests must be limited to “serious crimes.”²⁵

Congress also anticipated the possibility that, pursuant to such agreements, foreign governments could seek live intercepts – and not just stored communications. For live intercepts, the legislation includes the additional requirements that the orders be time-limited, lasting no longer than is needed to accomplish the approved objectives, and subject to a finding that the same information “could not reasonably be obtained by another less intrusive method.”²⁶

The agreements also include a number of requirements as to use of collected data. The data must be stored on a “secure system” accessible only to those “trained in applicable procedures.”²⁷ The foreign government is required to segregate, seal, or delete non-relevant information.²⁸ In addition, the foreign government must agree to periodic reviews by the United States government to ensure that the provisions of the executive agreement are being followed.²⁹ Whereas some such use-based limitations and accountability provisions were already included in the EU-US Umbrella Agreement, which covers law enforcement sharing across the Atlantic, these provisions include additional specifics that will help to protect the security and privacy of shared data.³⁰ Further-

more, for countries outside the EU that are not subject to the Umbrella Agreement, they represent a significant increase in protection compared to the status quo under the current mutual legal assistance process, where the U.S. government has minimal say as to how data is handled once it is provided to a foreign government.

Notably, the agreements also only permit foreign government direct access to the data of non-U.S. persons located outside the United States. Thus, even with an executive agreement in place, partner governments cannot directly compel the production of a U.S. person's (defined to include U.S. citizens and legal permanent residents)³¹ communications content or the communications content of non-U.S. citizens physically located in the United States; these requests still need to go through the mutual legal assistance system.³² In other words, partner foreign governments can directly access foreigners' data and hence set the rules, albeit with a number of baseline requirements in place, concerning access to that data. But if they want access to U.S. citizen and resident data, they still need to get U.S. court approval based on the U.S. standard of probable cause.

Finally, the foreign government must provide "reciprocal rights of data access." This means that the foreign government must permit its own locally based providers to respond directly to U.S. requests for data if and when the United States is seeking the data of a non-national of the partner government, has issued valid legal process to the provider, and has jurisdiction to compel such production.³³

III. Open Questions

The CLOUD Act is still new, leaving key questions as to implementation and interpretation to be worked out. Despite the warnings that Part I would lead to widespread conflicts of law, no such claims have yet been raised, although some may emerge in the near future. Of particular relevance, the EU's newly implemented General Data Protection Regulation includes key limitations on when EU-held data can be transferred out of the EU.³⁴ Some have argued that, in the absence of a new international agreement explicitly providing for transfers in these situations, no currently applicable exception would permit transfers of EU residents' data to the United States outside of the mutual legal assistance process, even in response to a validly U.S.-issued warrant.³⁵ The European Commission's amicus brief to the Supreme Court was non-committal on this point.³⁶ In the absence of an explicit EU-US agreement providing the basis for such transfers, conflicts may very well occur, with litigation to ensue.³⁷

Meanwhile, no executive agreements have yet been entered into (and hence there are no "qualifying countries" for purposes of Part I of the CLOUD Act), although there are expectations that a U.S.-UK agreement will be forthcoming. Either a U.S.-EU framework agreement or agreements with specific EU countries may be next. These initial agreements are likely to become a model for those that follow.

Importantly, and as noted in the Introduction of this article, the statutorily specified requirements for executive agreements merely set a floor not a ceiling. Additional protections can, and in some cases should, be added to any agreements that are ultimately adopted. Among the key additional provisions to be included:³⁸

- An agreed-upon mechanism for providers to initiate a U.S.-government review mechanism if and when they have concerns about a foreign government request;
- Protections for providers that produce transparency reports with details about foreign government requests for data;
- Clear rules on whether, when, and in what circumstances notification to the target of the collection is required and when and for what reasons it can be delayed.

Use-based requirements also provide an opportunity to incorporate protections in new and innovative ways. The required limitations on access, dissemination, and retention should be robustly implemented and followed. Periodic reviews should be regular and meaningful to ensure effective prevention and rapid correction of any errors or abuse.

A range of other details still needs to be worked out, including the scope of free speech protections and the set of "serious crimes" to be covered by the agreements. Each and every agreement also will need to address issues of scope. The CLOUD Act, for example, authorizes agreements that cover both stored communications and live intercepts. But there is no requirement that agreements do, in fact, encompass both. In fact, there is no basis in U.S. law to issue a wiretap order with extraterritorial reach.³⁹ It is thus possible to design agreements that allow for direct production of stored communications but do not include wiretaps.

In order to facilitate both compliance and oversight, partner countries might consider channelling all applicable cross-border requests through specified points of contact to ensure that specified protections are met. This is also something that the United States might require in certain circumstances. It also would help facilitate the periodic reviews and accountability that the agreements require. Each of these determinations can and should be worked out as part of an ongoing dialogue with the United States and key stakeholders from both industry and civil society. The considerations outlined here are just some of many.

IV. Conclusion

The CLOUD Act represents the opening salvo in a much-needed dialogue about the substantive and procedural rules governing law enforcement access to digital evidence and the shifting relationship between territorial boundaries and evidentiary needs. It is just one of many initiatives being pursued because of shifting trends in the ways key evidence is managed and stored. The European Union's draft e-Evidence proposals, unveiled in April 2018,⁴⁰ represent Europe's contribution to this discussion and bear remarkable similarities to the CLOUD Act.

Akin to Part II of the CLOUD Act, the draft E-Evidence Regulation provides a mechanism for law enforcement in an investigating country to bypass the mutual legal assistance process and issue a disclosure order directly to a private company that holds evidence of interest, even if that private company is located outside the investigating country's territorial jurisdiction.

Other unilateral initiatives abound. As a result of recent legislative changes, the UK now authorizes the issuance of extraterritorial warrants. Australia recently enacted legislation that would authorize the issuance of technical assistance orders on extraterritorially-located providers that have one or more end users in Australia.⁴¹ In specific court cases, Belgian authorities have maintained their authority to compel the production of data held by foreign-based providers offering services within Belgium, even if they are not located there.⁴²

These initiatives seek to respond to the increasing digitalization of information, the role of third-party providers in controlling this information, and the fact that providers and data of interest are increasingly held across borders. These shifts provide opportunities as much as they create challenges. The U.S. CLOUD Act is an important contribution to these efforts – one that can and should be built on via the construction of robust bilateral agreements that protect and elevate privacy and civil liberties while at the same time facilitating lawful access in ways that help protect and promote security.



Jennifer Daskal

Associate Professor at American University
Washington College of Law

1 Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115–141, 132 Stat. 348 (2018).

2 See N. Nielsen, "Rushed US Cloud Act Triggers EU Backlash", *euobserver* (26 March 2018), <<https://euobserver.com/justice/141446>> accessed 12 December 2018; D. Heide et al., "European Criticism of New US Cloud Act Mounts", *Handelsblatt Global* (24 April 2018), <<https://global.handelsblatt.com/politics/with-new-us-law-how-safe-is-online-data-in-europe-914956>> accessed 12 December 2018.

3 S. Richmond, "US CLOUD Act Raises New Data Privacy Issues", *Verneglobal* (12 July 2018), <<https://verneglobal.com/blog/us-cloud-act-raises-new-data-privacy-issues>> accessed 12 December 2018.

4 See, e.g., *Subcommittee on Crime and Terrorism*, "Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights", Hearing Before the S. Judiciary, 115th Cong. (2017), <<https://www.judiciary.senate.gov/meetings/law-enforcement-access-to-data-stored-across-borders-facilitating-cooperation-and-protecting-rights>> accessed 12 December 2018; *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. (2017), <<https://judiciary.house.gov/legislation/hearings/data-stored-abroad-ensuring-lawful-access-and-privacy-protection-digital-era>> accessed 12 January 2019; *International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. (2016).

5 See, e.g., J. Daskal and A. K. Woods, "Cross-Border Requests: A Proposed Framework", *Just Security* (24 November 2015), <<https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/>> accessed 12 December 2018 (proposing in 2015 a framework very similar to that enacted in 2018 as part of the CLOUD Act).

6 See S.2383 (115th Cong.); H.R. 4943 (115th Cong.).

7 See E. Wenger, "Does the CLOUD Act Really Grant DOJ Sweeping New Powers?", *Cross-Border Data Forum* (27 August 2018), <<https://www.crossborderdataforum.org/does-the-cloud-act-really-grant-doj-sweeping-new-powers/>> accessed 12 December 2018 (making a similar point).

8 P. M. Schwartz, "Legal Access to the Global Cloud", (2018) 118 *Colum. L. Rev.*, 1681, 1695.

9 *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d 708, 723 (E.D. Pa. 2017).

10 J. Daskal and P. Swire, "A Possible EU-US Agreement on Law Enforcement Access to Data?", *Lawfare* (21 May 2018), <<https://www.lawfare-blog.com/possible-eu-us-agreement-law-enforcement-access-data>> accessed 12 December 2018.

11 European Commission, "Commission Staff Working Document Impact Assessment, Accompanying the Document, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings", SWD(2018) 118 final, p. 14.

12 See J. Ginsburg, Transcript of Oral Argument, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2)(), <https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/17-2_j4ek.pdf> accessed 12 December 2018, p. 6: "So wouldn't it be wiser just to say let's leave things as they are; if – if Congress wants to regulate in this brave new world, it should do it?"; J. Sotomayor, *ibid.*, p. 12: ("Why shouldn't we leave the status quo as it is and let Congress pass a bill in this new age?"; J. Alito, J., *ibid.*, p. 36: "It would be good if Congress enacted legislation that modernized this"

- 13 Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018), § 103(a), (to be codified at 18 U.S.C. § 2713). If, however, the data is not within the company's possession, custody, or control there is no obligation to disclose.
- 14 CLOUD Act § 103(b) (codified at 18 U.S.C. § 2703(h)). If and when applicable, reviewing courts are instructed to consider the location and nationality of the investigative target whose data is being sought, the importance of the data to the investigation, and the relative interests of the United States and relevant foreign government, among other facts.
- 15 That said, the entire point of the executive agreements is, in significant part, to eliminate such conflict, meaning that, even when the set of qualifying governments increases, this statutory mechanism will rarely be invoked if the agreements work as intended.
- 16 CLOUD Act § 103(c).
- 17 The absence of any such conflicts to date undercuts the description of the CLOUD Act as representing a massive expansion of U.S. law enforcement reach and the prediction of increased legal conflict that some suggested would result from allowing U.S. access to data located abroad. See, e.g., Brief for Microsoft Corp. at 13, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2), <https://www.supremecourt.gov/DocketPDF/17/17-2/27619/20180111205746909_Brief%20for%20Respondent%202018.01.11.pdf> accessed 12 December 2018 (warning of "direct conflicts with foreign laws that govern emails stored in foreign lands"); *id.* at 41 (same).
- 18 Brief for Ireland as Amicus Curiae in Support of Neither Party, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2), <https://www.supremecourt.gov/DocketPDF/17/17-2/23732/20171213152516784_17-2%20ac%20Ireland%20supporting%20neither%20party.pdf> accessed 12 December 2018.
- 19 See Regulation (EU) 2016/679 of the European Parliament and of the Council, *O.J. L* 119, 4.5.2016, 1 [hereinafter GDPR], Arts. 48–49 (laying out transfer restrictions plus exceptions). Whether, to what extent, and in what situations the exceptions to the otherwise applicable transfer restrictions will permit a provider to transfer EU-held data to U.S. law enforcement remains an open question. See *infra* notes 35–38 and accompanying text. That said, the absence of any such conflicts to data undercuts the description of the CLOUD Act as representing a massive expansion of U.S. law enforcement reach and the prediction of increased legal conflict that some suggested would result from allowing U.S. access to data located abroad. See, e.g., Brief for Microsoft Corp. at 13, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2), <https://www.supremecourt.gov/DocketPDF/17/17-2/27619/20180111205746909_Brief%20for%20Respondent%202018.01.11.pdf> accessed 12 December 2018 (warning of "direct conflicts with foreign laws that govern emails stored in foreign lands"); *id.* at 41 (same).
- 20 See G. Kent, "The Mutual Legal Assistance Problem Explained", *CIS Blog* (23 February 2015), <<http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained>> (describing the process).
- 21 See R. A. Clarke et al., *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, 2013, <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> accessed 12 December 2018, pp. 227–28 (noting that it takes an average of ten months to process these MLAT requests).
- 22 See *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. (2017) (written statement of Paddy McGuinness, Deputy National Security Adviser, U.K.), <<https://docs.house.gov/meetings/JU/JU00/20170615/106117/HHRG-115-JU00-Wstate-McGuinnessP-20170615.pdf>> accessed 12 December 2018; *Hearing Before the S. Judiciary Subcomm. on Crime and Terrorism*, 115th Cong. (2017) (written testimony of Paddy McGuinness, Deputy National Security Adviser, U.K.), <<https://www.judiciary.senate.gov/imo/media/doc/05-10-17%20McGuinness%20Testimony.pdf>> accessed 12 December 2018; see also J. Daskal, "Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues", (2016) 8 *J. Nat'l Sec. L. & Pol'y*, 473, <http://jnsnl.com/wp-content/uploads/2017/10/Law-Enforcement-Access-to-Data-Across-Borders_2.pdf> accessed 12 December 2018.
- 23 CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523 (b)(1)).
- 24 *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(D)(ii)–(v)).
- 25 For a further elaboration of these protections, see J. Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, (2018) 71 *Stan. L. Rev. Online* 9, 13–15, <<https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/>>; J. Daskal & P. Swire, "Why the CLOUD Act is Good for Privacy and Human Rights", *Just Security* (Mar. 14, 2018), <<https://www.justsecurity.org/53847/cloud-act-good-privacy-human-rights/>> all accessed 12 December 2018.
- 26 CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523 (b)(4)(D)(vi)).
- 27 *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(F)).
- 28 *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(G)).
- 29 *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(J)).
- 30 See Council of the European Union, "Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses", Council doc. 8557/16 of 18 May 2016.
- 31 CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523 (a)(2)); 18 U.S.C. § 2523(a)(2) (defining U.S. person).
- 32 *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(A–C)).
- 33 CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523 (b)(4)(I)).
- 34 Arts. 48–49 GDPR.
- 35 See, e.g., European Data Protection Board, Guidelines 2/2018 on Article 49 under Regulation 2016/679 (adopted on 25 May 2018), <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf> accessed 12 December 2018.
- 36 See Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2), <https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf> accessed 12 December 2018, pp. 12–16 (noting the data transfer restrictions included in the GDPR, highlighting the possibility that transfers could be justified under Art. 49 of the Regulation, but also emphasizing that Art. 49 grounds for transfer are to be "interpreted strictly").
- 37 For a further discussion of this issue, see J. Daskal, "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0", (2018) 71 *Stan. Online Rev.*, 9, 12–13.
- 38 See also P. Swire and J. Hemmings, "Recommendations for the Potential US-UK Executive Agreement Under the CLOUD Act", *Lawfare* (13 September 2018), <<https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act>> accessed 12 December 2018 (suggesting additional provisions).
- 39 See J. Daskal, "Setting the Record Straight: The CLOUD Act & The Reach of Wiretapping Authority Under US Law", *CBDF Forum* (15 October 2017), <<https://www.crossborderdataforum.org/setting-the-record-straight-the-cloud-act-and-the-reach-of-wiretapping-authority-under-us-law/>> accessed 12 December 2018.
- 40 See also T. Wahl, "Commission Proposes Legislative Framework for E-Evidence", *eu crim* 1/2018, 35–36; For a detailed analysis, see the article of S. Tosza, in this issue.
- 41 See Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) (Austl.), Sch. 1 § 317C (defining scope of coverage), <https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_aspassed/toc_pdf/18204b01.pdf;fileType=application/pdf> accessed 17 January 2019.
- 42 Hof van Cassatie [Cass.] [Court of Cassation], 18 January 2011, *Procureur-Général v. Yahoo! Inc.*, Nr. P.10.1347.N (Belg.), translated in: (2011) 8 *Digital Evidence & Electronic Signature L. Rev.* 216, 216–18, <<http://journals.sas.ac.uk/deeslr/article/view/1978/1915>> accessed 12 December 2018; see Hof van Beroep [HvB] [Court of Appeal] Antwerp, Nov. 15, 2017, *Openbaar Ministerie v. Skype Commc'ns SARL*, 2016/CO/1006 (Belg.), 5.1.1.4., 5.1.2.2. For a further discussion of these cases and related issues, see J. Daskal, "Borders and Bits", (2017) 71 *Vand. L. Rev.*, 101, 114–118.

Classification of Electronic Data for Criminal Law Purposes

Claudia Warken

Although the significance of electronic evidence for criminal investigations of any type of criminal offence has been steadily growing for years, respective legal frameworks in all EU Member States are only fragmented – if they exist at all. There is an urgent need for comprehensive legislation that takes into account the various grades of data sensitivity. For various reasons, the common distinction between subscriber data, traffic data, and content data is not suitable for this purpose. Instead, a new classification is necessary. The article analyzes the relevant backgrounds and provides an overview of the current issues. More importantly, it proposes a new classification with five categories of electronic data. The key criterion for determining the sensitivity of a dataset – the data subject's reasonable expectation of confidentiality – allows a distinction as follows: (1) data of core significance for private life, (2) secret data, (3) shared confidential data, (4) data of limited accessibility, and (5) data of unlimited accessibility. The article further shows that the newly proposed classification is comprehensive and technically neutral – thus, future-proof. In addition, it explains why the approach presented is solidly based and most suitable for legislative purposes, since it derives solely from the specifically affected fundamental rights.

I. Theses¹

Electronic data have become increasingly relevant as evidence in criminal investigations. Yet, there are – if any – only fragmented legal frameworks on European or national levels in the Member States of the European Union targeting the specific challenges posed by this unique type of evidence. Thus, there is a need for comprehensive and coherent legislative solutions on different levels.

The conditions and safeguards of different investigation measures depend on the intrusiveness of the respective measure. In the context of electronic data, the intrusiveness of a measure can vary widely. This has to be taken into account in the development of any legislative approach by means of an appropriate classification of the data. The common distinction of communication data, generally resulting in a classification of content data and non-content data or content data, traffic data and user data, does not meet the requirements of modern logistics.² The required classification has to reflect the sensitivity of specific types of electronic data. Thus, it should solely be based on the affected data subject's fundamental rights. The key criterion for determining the sensitivity of a dataset is the data subject's reasonable expectation of confidentiality.

It allows a classification as follows (in order of decreasing sensitivity): data of core significance for private life, secret data, shared confidential data, data of limited accessibility, and data of unlimited accessibility. The following sections further discuss this statement.

II. Relevance of Electronic Data as Evidence – Specific Characteristics

Electronic data are increasingly relevant as evidence in criminal investigations. According to the common understanding, the term refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system.³ These data play a significant role, e.g. where perpetrators communicate electronically or where the mere possession of an electronic device can provide location data for exact and specific times. In addition, it has been observed over the last few years that electronic data are not only relevant in the context of classical cybercrimes such as DDoS hits or ransomware attacks but also in the context of traditional offenses, such as fraud or child sexual abuse, which are more and more frequently committed through the internet.

Furthermore, the rapidly expanding use of electronic devices, e.g. for work-related and private purposes, for mobile communication, or in the Internet of Things, where devices exchange information through the internet directly, has led to the phenomena of Big Data – large amounts of information stored in electronic form and potentially relevant as evidence.

Electronic data for use as evidence in a criminal investigation can be obtained from the victim, the suspect, or any third party who, in most cases, is a service provider whose service refers to the creation, transmission, and/or storage of the data. Law enforcement can obtain the data through open or covert measures: A house search, including the seizure of electronic de-

vices, such as a mobile phone or a laptop, is an example of an open investigation measure, while the interception of a mobile communication, for instance, is usually conducted in a covert way.

Because electronic data are intangible – they are nothing more than a processable sequence of zeros and ones –, they show characteristics that are not comparable to those of other, tangible evidence.⁴ In contrast to physical things, the handover of electronic data usually does not imply a loss of control; on the contrary, the data possessor usually keeps the original dataset and only transfers a copy of it – either electronically, on a data storage device, or as a printout on paper. From a technical point of view, electronic data can generally be accessed (and thus be obtained) from anywhere in the world as long as they are accessible through the internet; the necessary act for their seizure does not have to take place at the concrete data location. Concerning the acquisition of electronic data, time is a crucial factor, not only because this evidence can be transmitted with literally nearly speed of light, but also because such transmission can be carried out irrespective of any national borders. Last but not least, compared to physical things, it is much easier to create and process electronic data anonymously; traces in the virtual cyberspace can be hidden much better.⁵ Once law enforcement has obtained electronic data that are potential evidence, they usually have to be converted into a compatible, readable format for further processing. This implies the risk of intentional, unintentional, and even unnoticed manipulation of the original information.

III. Existing Legal Frameworks (Criminal Law)

Even though electronic data show unique characteristics that have a significant impact on their availability and admissibility as evidence, only a few legal frameworks exist and they take only some of the specifics into account. Even where specific legal provisions of criminal procedure exist, the legal landscape on European level as much as on national levels in the European Union, the USA, and other “Western” countries is fragmented. There is no comprehensive set of rules addressing these specific issues. Like in other EU countries, the German Code of Criminal Procedure,⁶ lacks explicit regulations, e.g. on the acquisition of electronic data from any third party who is not a telecommunication service provider,⁷ on the acquisition of machine-to-machine information, on preliminary measures for data preservation (“quick freeze”), on the handling of large amounts of Big Data, and on procedures to guarantee and confirm the integrity and authenticity of a dataset. As in other jurisdictions, existing provisions referring to tangible pieces of evidence are applied in order to fill gaps – a questionable approach in the sensitive area of criminal law.

Although there is a cross-border aspect in many cases referring to electronic evidence, it is often unclear how a provider who offers service in a country without having any physical assets there should be dealt with.⁸ It is also unclear whether a request for data disclosure should be served in the country where the service provider has its headquarters or, if different, rather in the country where the data are stored.⁹ Unsolved issues of jurisdiction arise, e.g. if a multi-national botnet is used to commit a DDoS attack in one country, if several perpetrators who are located in different jurisdictions act together, or if a number of victims in different countries are affected through one offense.¹⁰ In addition, the problem of “loss of location” – electronic data stored abroad and, at the same time, accessible from home – is being discussed controversially.

The current general opinion seems to favor prohibiting the domestic investigator from processing such data, due to the assumed violation of the other state’s sovereignty that such an act would cause. The same seems to apply to the situation involving “loss of knowledge of location,” where it is not even clear where the data are located. Thus, they could well be stored domestically so that there would be no cross-border situation at all; still, the potential risk of violation of another country’s sovereignty would prevent the investigator from using these data.¹¹ Preliminary cross-border data retention is regulated only between EU Member States,¹² and there are no comparable instruments concerning other countries. Last but not least, open questions remain when service providers who operate internationally find themselves in situations of conflicting law, e.g. when the disclosure of certain data is requested by one country and a compliant disclosure would violate another country’s data protection laws.

In a nutshell, there is a lack of legislation – both quantitatively and qualitatively. Only recently, legislators have begun to tackle the issues, leading, for example, to the European Commission’s proposal on access to electronic evidence in criminal investigations of April 2018¹³ or to the Council of Europe’s current discussion on an additional protocol to the Convention on Cybercrime. On the national level, provisions allowing remote evidence gathering through the internet have been introduced lately e.g. in Belgium, Germany and Austria while the US CLOUD Act of March 2018 specifically aims at data “in the cloud”. Still, these approaches cover only some of the problems. The lack of clear and reliable normative concepts in criminal investigations endanger legal certainty and jeopardize the fundamental rights of affected persons.

IV. General Logistic Requirements

The right of equal treatment is a fundamental right generally accepted in all modern “Western” legal frameworks. In the sim-

plified words of the German Constitutional Court, it calls on the legislator and law enforcement to treat equal cases equally and unequal cases unequally unless there are reasonable grounds to deviate from this rule. Accordingly, deriving from the fundamental right of equal treatment and depending on the object of a concrete investigation measure, there is a general understanding that different conditions and safeguards may apply. Thus, the search of a home follows different rules than one for a bag on the street, even though both objects are physical things that belong to an individual. Obviously, the search of a home and that of a bag on the street are considered unequal cases because the intrusiveness, e.g. regarding the fundamental right of privacy, is higher in the first scenario than in the second one. This example indicates that the level of interference with the respective fundamental right(s) is an appropriate criterion by which to group and to distinguish cases or, in other words, to determine whether cases are equal or unequal.

That is nicely said, yet it provokes the next question of how the level of interference with fundamental rights is determined or, in other words, what the appropriate criteria for the differentiation are. Why exactly is a home considered more private than a bag on the street? What is the concrete reason for this legal distinction? Many national constitutions even ban certain aspects as distinguishing features at all.¹⁴ Outside this banned scope, there are many possible options at the discretion of the legislator.

V. Classifying Electronic Data – Traditional Approach

Consensus exists that there is a wide range of potential interference with fundamental rights through the acquisition and the use of electronic data in a criminal investigation. It is further commonly agreed that this broad range of potential intrusiveness calls for a set of possible measures with different conditions and safeguards. As referred to above, for instance, acquiring the content of the mobile communication of a lawyer and his/her client is legally not equal to acquiring the content of a communication in an open internet chat; the first example is considered much more sensitive than the second one. There are many more examples which reflect the general assumption that the sensitivity of one dataset is not always identical to the one of another dataset – even if both could be grouped, for example, as personal communication content information. Cases differ; they may be unequal.

In addition, there are apparently no reasonable grounds for treating the unequal cases equally. The general sense of justice requires communication with a lawyer and communication in an open chat to be treated differently. Thus, for constitutional reasons and based on the fundamental right of equal

treatment, a differentiation of electronic data is an indispensable requirement for any comprehensive legal framework tackling the issue. There is currently no structural approach of how to differentiate electronic data comprehensively. Only regarding communication data different levels of sensitivity are assumed, leading to a distinction between content data and non-content data (or metadata), while non-content data are sometimes further broken down into user data (or subscriber data) and traffic data.¹⁵

This differentiation is widely acknowledged. It derives from the transition of classical telecommunication providers from analogue to digital networks in the early 1990s. For billing purposes, the companies had to rely on the data provided in the service contract, such as the name of the subscriber and his/her address, and the monthly bill was invoiced in paper form. In addition, the details of the concrete service, such as the destination and duration of a call (today's traffic data), had to be documented in order to provide proof in case of disagreement about the billing. Lastly, and different than today, the content of a communication was of no relevance for the involved service provider. Having its origin in the practical needs of service providers, the traditional differentiation subsequently found its way into legal frameworks concerning data protection and criminal procedural law.

Irrespective of whether it was compliant with legal requirements in the past, the traditional differentiation used today is no longer suitable anymore with regard to modern communications. Especially in the context of social media and open chat fora, the content of a communication can no longer automatically be assumed more sensitive than non-content data that the user does not want to share publicly. In addition, the needs of the service providers involved have changed significantly. They no longer need to possess the traditional user data, e.g. when pre-paid services are offered, and often, parameters like the duration of a call via an internet application, such as Skype or WhatsApp, are of no relevance for billing. In fact, the user increasingly does not have to pay for a service with an amount of money based on the amount of service delivered. Instead, the user agrees (with more or less awareness) that his/her personal data will be given in exchange for the service. These data might include the content of a communication which is of high economic value because it can be sold, analyzed, and ultimately used e.g. for tailored advertising.

To add to the complexity of the problem, the common distinction of communication data refers to the same wording internationally; yet, due to the technical expansion of communication means, the terms are often used with slightly different but relevant different meanings.¹⁶ Apart from concerns emerging from the traditional distinction of communication data, major

classification gaps remain regarding all non-communication data. This affects not only the machine-to-machine exchange of information, which is increasing significantly with the growth of the Internet of Things and which covers everything from most sensitive to most trivial data and also any data that are not shared but only stored on the user's device or "in the cloud."

Thus, the traditional model of classifying electronic data has served its time. A new approach must be taken.

VI. Classifying Electronic Data – Current Discussion

The required re-classification of electronic data for criminal purposes should ideally fulfil several conditions in order to allow "good" legislation: Firstly, it should aim at covering all potential electronic evidence. The classification should be comprehensive in order to avoid legislative gaps. Secondly, the classification should be technically neutral. Only then can the solution be future-proof. That is especially true in the rapidly developing cyber area, where specific technical issues may have become irrelevant by the time a referring legislation is finally adopted and implemented. Ultimately, the classification should follow an abstract structure and avoid any catalogue listing. Even if a list of detailed types of data seems to facilitate their handling at first glance, such a list would be likely to miss one or the other type – if not from the outset, then possibly after a short time, as no legal amendment procedure can keep up with the rapid technical developments in IT. In addition, a catalogue listing would likely blur the actual differentiator – if there is an appropriate one, it should simply be named.

Taking these premises into account, it needs to be determined what exactly constitutes the sensitivity of electronic data. Aspects which, generally have an impact on the intrusiveness of any investigation action – namely whether the measure is open or covert, its duration, or the number of people affected – should be considered when it comes to the proportionality test of the measure. However, they do not play a role for the classification as such.

Various approaches are currently discussed about how to determine the sensitivity of electronic data best. The main problem is the identification of the criteria which determine their sensitivity. In short, the following criteria are under discussion, both separately and in combination with one another:

1. The content of the data

This criterion is reflected in the traditional distinction of communication data, where the content of a set of data refers either

to the content of the communication itself or to metadata that is created through the processing of the data. The flaws of this approach are described above. In particular, it can no longer be assumed that the content of a publicly shared communication is more sensitive *per se* than, for example, location data that the user wishes to hide. It depends on the individual circumstances – therefore, referring to the content of a set of data is not a suitable criterion for a general classification. In addition, referral to the content of a set of data would cause practical problems at the very least when intercepted or retrieved stored data are concerned: determining the content would first require obtaining and inspecting the data, which might only be allowed for certain types of content.

2. The amount of data collected

This aspect raises not only technical issues: What amount of data is considered appropriate for differentiation? How to deal with situations where the data to be obtained are unknown in advance? It also rules out the premise of technical neutrality that the classification should follow. In addition, it cannot be assumed that a small amount of data is generally less sensitive than a larger amount. Thus, the amount of data is not an appropriate criterion for classification purposes. Nevertheless, it is of significant relevance for the proportionality test of any concrete measure that is applied.

3. The technical origin of the data

In order to determine the sensitivity of a set of data, one could refer to its technical origin (e.g. an electronic document or a digital picture) or the underlying service (e.g. a mobile call, a video stream, or a mere storage in the cloud). Besides the fact that such an approach would not respect the condition of technical neutrality, there is no comprehensible reason why, for instance, a document should legally be treated differently than a picture. Thus, the technical origin of the data can be discarded as a criterion.

4. The processing state of the data

It is generally assumed that data in rest are more sensitive than data in transit. Although this assumption is not based on obvious legal reasons (there are strong arguments in favor of the opposite conclusion), there are legal provisions which are based on this differentiation and, accordingly, establish different investigation measures like real-time communication interception, on the one hand, and the seizure of a data storage device, on the other. Like the data volume criterion, the state

of the data is not technically neutral. Current problems in this context occur concretely regarding cloud storage: from the user's point of view, his/her data are stored and "laid to rest" in the cloud while, in fact, the data are frequently processed (split, re-merged, duplicated, transferred from one server to another one, etc.) for security reasons. In practice, this makes it almost impossible to determine the state of a set of data at the exact time when an investigation measure is to be applied. Furthermore, the applied differentiation is very broad because it provides only two groups. That is not sufficient for legal purposes, since there is no doubt that the sensitivity of stored data, e.g. on an USB-stick, can vary widely. Thus, referring to the state of the data is of little help for the required data classification.

5. Data protection law approach

Data protection law concerns personal data as opposed to non-personal data and differentiates further within the first category between sensitive and less sensitive data. The top-level differentiation between personal and non-personal data obviously applies to criminal investigation measures as well, as there is no need to legislate measures that do not affect a person (or even a large number of persons). However, this broad differentiation does not really help. The additional distinction division of personal data into sensitive and less sensitive data only targets data *about* a person and does not provide a classification of data *from* a person. Furthermore, the relevant criterion derives from the societal mainstream and is therefore not necessarily compatible with criminal law aspects.¹⁷ Last but not least, such a distinction assumes that the content of a set of data is known before a measure is taken, which is not the case in many investigation measures. For these reasons, the approach of data protection law does not support a data classification for criminal law purposes.

6. Significance of the data for the investigation

Focusing on the significance of the data for the concrete investigation causes an unsolvable problem: in order to determine the significance of data, one can refer to the individual case or to comparable cases in general. Under the first option, the significance could only be determined once the investigation has progressed, thus, once the data have been obtained and used. At this point in time, the classification would not matter anymore. Under the second option, the statistical analysis would itself rely on a classification (or else the analysis would not make any sense), so the question of the appropriate criterion would remain unsolved. In addition to the practical issues, the data's significance for an investigation does not reflect the somehow person-related link to the sensitivity of a set of data;

most useful data can be of marginal sensitivity and vice versa. Thus, this criterion should only be considered for the test of proportionality and, specifically, of the necessity of a concrete measure.

7. Offense concerned/applicable investigation measure

One could apply a scheme by which the seriousness of the offense concerned or the applicable investigation measure would determine the type of data that would be accessible. Thus, the more serious the offense or the less intrusive the applicable investigation measure (in general terms, i.e. an open measure, e.g., would have to be considered less intrusive than a covert one), the less strict the conditions and safeguards. However, that would not allow an originary classification of data and instead turn the logistic approach upside down: the classification is a pre-condition to determining conditions and safeguards and not the other way around.

Taking into account the flaws of each of the discussed approaches, there does not seem to be a feasible solution based on a combination of several of the criteria; all of them exhibit major problems. Thus, the current discussions do not provide a solid solution.

VII. Classifying Electronic Data – A New Approach

What is instead needed in order to determine the criteria for a dataset's sensitivity, is a new line of thinking that takes into account the premises mentioned above – being comprehensive, technically neutral, and abstract as opposed to detail-listing – and focuses on legal aspects, namely on the fundamental rights of the data subject.

Looking at other provisions that deal with evidence in criminal procedural law, the focus on legal aspects is very common, e.g. information that can be obtained through physical interference or contact with a person. Here, the fundamental right of physical integrity is affected and, depending on how much it is affected, different investigation measures with different safeguards and conditions apply. The extent of physical interference is the key criterion for classifying the body-related evidence. It can range from minor (e.g. taking a person's picture or fingerprint) to more severe (e.g. taking a blood sample). Even beyond that, the grade of intrusiveness provides different categories of body-related information such as appearance, fingerprint, and blood count. The same applies to documents for which legal provisions have established the assumption of different levels of sensitivity that are derived from the affected fundamental rights.

In the context of electronic evidence, it is therefore necessary in a first step to determine the fundamental rights that are specifically affected, then to extract their key content, and thirdly to filter out the aspect that allows for a differentiation between minor and more serious interferences. Once that aspect has been carved out, it can be applied.

1. Relevant fundamental rights

There is a general understanding that the specific fundamental rights which concern electronic data encompass the right of respect for private life, the right of self-determination, and the right of secrecy of correspondence. Although the concrete interpretations may slightly differ (especially when they refer to very similar, yet not identical legal frameworks like the European Convention on Human Rights, the European Charter of Fundamental Rights, or national constitutions), there is still an overall agreement that the principles of the above-mentioned fundamental rights are the relevant ones.

2. Key content of the relevant fundamental rights

Concisely, the key content of the relevant fundamental rights regarding electronic data is the data subject's possibility to freely and independently decide what happens to his/her data – who should have access to them, with whom they are shared, etc. Electronic data might, for example, not be shared at all, be shared only with most trusted persons, or be shared publicly with an uncontrolled number of persons. Thus, the core issue of data-related fundamental rights relates to the confidentiality of the data.

3. Key criterion for differentiating the grade of interference

The grade of interference with the confidentiality of data depends on how much the free will of the data subject is respected: the more it is respected, the less interference. In other words, the more the data subject can reasonably expect that a set of data will remain confident, the more sensitive the data are. It needs to be stressed that, because of its derivation from individual fundamental rights, the sensitivity of electronic data depends only on the data subject; there is no room for allowing e.g. the legislator or society to decide what is sensitive for a specific individual.

These findings allow the following conclusions: First, whether a set of data is sensitive or not does not depend on the status of the data subject in the investigation; it is the same for the suspect, the

victim, and the witness alike. Thus, the role of the data subject in the investigation is irrelevant for the classification of electronic data; it only requires consideration when it comes to the proportionality test of a concrete investigation measure.

Second, the coincidental *processing state* of the data (whether it is currently being processed or not) does not matter for the classification of electronic data. The sensitivity, e.g. of the content of an electronic diary, does not depend on whether it is still on the laptop at home, in the process of being transmitted to the storage place in the cloud, or already stored there.

Third, the level of *confidentiality* that can be reasonably expected depends on the circumstances of the specific case. There are two crucial aspects for its determination: the data subject's behavior (i.e. to what extent he/she shares the respective data) and his/her bond of trust with the person who receives the data. This bond of trust can be based on both actual and/or legal grounds, e.g. on the personal relationship between close friends or on a contractual agreement with a service provider. On the contrary, the content of the information does not play a key role for the confidentiality assessment; it may be an indicator, but nothing more.

VIII. Applying the New Criterion of Reasonable Expectation of Confidentiality

The finding that the classification of electronic data has to rely only on the criterion of the data subject's reasonable expectation of confidentiality allows classifications of different granularities. In order to find a workable balance between the wide range of potential data sensitivity and the number of data categories, a classification with five categories is proposed. These are, in order of decreasing sensitivity: (1) data of core significance for private life, (2) secret data, (3) shared confidential data, (4) data of limited accessibility, and (5) data of unlimited accessibility.

1. Data of core significance for private life

The first category – the data of core significance for private life – refers to the *most private, inviolable data*; the reasonable expectation of confidentiality extends to the level of knowledge that the information will not be used as evidence in a criminal investigation.

2. Secret data

The category of secret data refers to additional electronic information that the data subject has not shared with anyone else or, alternatively, to data that have been transferred to a reli-

able, usually non-natural third party with the only intention that this party stores the data without gaining knowledge of its actual content, e.g. where a provider offers the automated service of cloud storage without any additional services. In both cases, the reasonable *expectation of confidentiality is very high*.

3. Shared confidential data

Shared confidential data has been shared with specifically trusted persons under the data subject's reasonable expectation that the information will not be distributed any further, e.g. with a spouse, a very close friend, a lawyer or a doctor. Compared to secret data, however, there is an *increased risk that the information will be leaked*.

4. Data of limited accessibility

Data of limited accessibility is data that have been shared with one or a limited number of individuals who are not specifically trusted. This category takes into account that a controlled distribution of the data still indicates a certain will to maintain at least some confidentiality, while at the same time acknowledging that *the reasonable expectation that the data will not be shared further is rather limited*. It covers all communication metadata in the sense of the traditional classification, because the use of electronic means for communication inevitably depends on information like the recipient's contact data or the radio cell used. This information is available to the involved service provider(s) who generally cannot claim specific personal trustworthiness.

5. Data of unlimited accessibility

For information distributed publicly – or data of unlimited accessibility (e.g. on an open social media platform) –, there is *no reasonable expectation of confidentiality*. The same applies to data voluntarily shared with law enforcement authorities with the knowledge that the information might serve as evidence in a criminal investigation. Furthermore, it covers data that voluntarily and legally disclosed to law enforcement by a third party, at least if the third party has obtained the data in a legal way. The reason for including the last-mentioned alternative is the consideration that the confidentiality was breached through the act of a third party without pro-active support from any authority, and the materialized risk of voluntary disclosure by the informed third party is fully on the data subject's side.

IX. Résumé

The newly introduced approach allows a comprehensive data classification for criminal law purposes, which is urgently needed. It avoids the problem of defining communication data and closes current gaps.¹⁸ The comprehensive classification facilitates an all-encompassing regulation that embraces all criminal investigation measures related to electronic data.¹⁹ Since it is solely based on the affected fundamental rights of the data subject and not dependent on, e.g. billing purposes of telecommunication service providers in the past, it is solidly based for legal purposes. For the same reason, the new classification of electronic data is also coherent with the existing classifications of other types of criminal evidence, e.g. documents or body-related information, both of which are also categorized according to the level of interference with the affected fundamental rights.

In addition, because of its technical neutrality, the new model is decoupled from future technical developments; it is future-proof. Furthermore, the questionable legislative differentiation between telecommunication service providers and over-the-top service providers becomes obsolete; when offering services that are identical from the user's perspective, they have to be treated equally.

The referral to abstract terms for the different categories avoids the flaws inherent to a detail-listing catalogue. One can assume that, with the knowledge of its logistic derivation, the courts would substantiate the various categories – as it has happened in the context of other abstract terms in criminal law.

X. Outlook

This article focuses on criminal law, yet its derivation from the affected fundamental rights might allow further potential applications, e.g. regarding data retention or civil law. In practice, the approach can be directly applied where existing legal provisions do not address the issue of the required level of proof concerning the integrity and authenticity of electronic data that are to serve as evidence. The lower the level of sensitivity, the more easily a court could, in general, assume the integrity and authenticity of the data. In other words, the more confidential the data, the higher the required level of proof of their integrity and authenticity. Furthermore, until a comprehensive legal framework enters into force, the new model can serve the test of proportionality for any investigative measure that refers to electronic data.

Due to the comparable protection of fundamental rights in the “Western” world and specifically the European Union,

the model could subsequently be applied in these countries as well. This would significantly improve the more and more frequently required international cooperation regarding the acquisition and exchange of electronic data as well as their admissibility in court.

While the new classification provides solutions, new questions also emerge. As mentioned earlier, the courts would have to substantiate some abstract legal terms, such as the “reasonable expectation” of confidentiality. However, this would only be a matter of time and is no issue of principle concern. Within the context of determining the reasonable expectation of confidentiality, the use of encryption could be considered an additional indicator, possibly depending on whether it is applied intentionally or by default through the service provider. Fur-

ther issues arise in cases in which the data subject’s behavior does not correspond to his/her expectation of confidentiality, e.g. where data are shared unknowingly or where a third party distributes the information without being allowed to do so.

Finally, it has to be clarified who the data subject is, e.g. in cases of machine-to-machine communication (any non-public information exchange eventually refers to at least one person), or when the data relate to a group of natural persons or a legal person.

These questions are not exclusive. Finding appropriate solutions requires a rethinking of how to approach potential electronic evidence. This article is meant as a first impulse to start the discussion.

1 The content of this article was extensively elaborated in German in the doctoral thesis submitted by the author to the Law Faculty of the University of Heidelberg, Germany in May 2018 under the original title “Klassifikation elektronischer Beweismittel für strafprozessuale Zwecke”. The dissertation will be published in 2019.

2 The term „legistics” refers to the sum of all aspects that have to be considered by any law maker in order to create „good” laws – such as the principles of necessity and proportionality. It seems that the seldomly used term has been introduced by U. Karpen, *Gesetzgebungslehre – neu evaluiert – Legistics – freshly evaluated*, Baden-Baden 2008. Accordingly, references are made to „legistic requirements” in this article, meaning those that should ideally be considered in any law making process.

3 See, e.g., Art. 2(b) of the Directive 2013/40/EU on attacks against information systems (O.J. L 218, 14.8.2013, 8) and Art. 1(b) of the Council of Europe’s Convention on Cybercrime (ETS 185).

4 Traditional evidence includes persons (witnesses and experts) and physical things (objects for legal inspection such as documents, pictures, or real estate).

5 E.g., the use of proxy servers can hide concrete data transfers while user names, e-mail addresses, and other identifiers do not have to reveal any information about the persons behind them. Another major challenge for law enforcement in this context is the simultaneous distribution of identical dynamic IP addresses to up to several thousand users at one time.

6 Strafprozessordnung, StPO.

7 In most countries, the term “telecommunication service provider” refers to the traditional provider who is usually legally obliged to cooperate with law enforcement, whereas the new over-the-top service providers generally do not have to disclose available electronic data. This distinction is made even where identical data is available (e.g., when it comes to the IP address used for a concrete communication) or where, from the user’s point of view, identical services are delivered (e.g., a mobile phone call without an additional user’s application or via WhatsApp for instance). In Germany, the differentiating definitions of the respective service providers are found in the Telekommunikationsgesetz (TKG) and the Telemediengesetz (TMG).

8 This was one of the main legal questions in the *YAHOO! Inc. v Belgium* case (Hof van Cassatie of Belgium, 1 December 2015, case P.13.2082.N).

9 That was the key question in the so-called *Microsoft Ireland case* (Supreme Court of the United States, No. 17-2, 584 U.S. (2018)) in the USA, which was rendered moot by the US Supreme Court after the Clarifying Lawful Overseas Use of Data Act (CLOUD Act; H.R. 4943) was enacted in March 2018.

Claudia Warken

Judge at the Regional Court (Landgericht) Ulm,
Germany;
Seconded National Expert to the European
Commission (March 2016 – September 2018)

10 E.g., in May 2017, the WannaCry ransomware attack hit more than 300,000 computers across more than 150 countries within hours.

11 For more detailed information about „loss of location” and „loss of knowledge of location” see, e.g., B.-J. Koops and M. Goodwin, *Cyber-space, the Cloud, and Cross-border Criminal Investigation. The Limits and Possibilities of International Law*, 2014; A.-M. Osula, “Accessing Extraterritorially Located Data: Options for States”, in: M. N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, U. Sieber, “Straftaten und Strafverfolgung im Internet”, *Gutachten C zum 69. Deutschen Juristentag*, 2012, C 77 and C 143; C. Warken, “Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil I”, (2017) *Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt)*, 289, 295; M. Zoetekouw, “Ignorantia Terrae Non Excusat”, Discussion Paper for the Crossing Borders: Jurisdiction in Cyberspace conference – March 2016.

12 Existing general instruments are the European Investigation Order (Directive 2014/41/EU regarding the European Investigation Order in criminal matters, O.J. L 130, 1.5.2014, 1) and the European Freezing Order (Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence, O.J. L 196, 2.8.2003, 45).

13 The European Commission’s e-evidence proposal of April 2018 (“Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters”, COM(2018) 225 final – 2018/0108 (COD)) includes, e.g., “quick freeze” provisions and data disclosure obligations specifically designed for electronic data that would apply to any provider offering services in the EU, irrespective of the location of its headquarters or of the location of data storage.

14 In modern “Western” constitutions, e.g., the gender of a person, his/her religion, or his/her origin are inapplicable differentiators.

15 The term „communication data“ is not legally defined. Thus, it remains unclear what exactly is covered.

16 E.g., machine-to-machine data exchange is not always considered communication data; information about the user's bank account is only sometimes covered by subscriber data; an IP address might be subscriber data or traffic data.

17 Data protection law considers, e.g., genetic and biometric data to be equally sensitive. In criminal procedural law, however, the use of genetic data, such as information about a genetic disorder, is much more limited

than the use of biometric data, such as a fingerprint.

18 The doctoral thesis includes a table comparing different datasets and their categorizations in the traditional system (if any) with the newly proposed one; it also shows the practical and structural advantages of the new classification.

19 The doctoral thesis includes a concrete, comprehensive, and commented draft of how electronic data could be dealt with in the German Code of Criminal Procedure.

The European Commission's Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online

Dr. Gavin Robinson

In September 2018, the European Commission presented a draft Regulation on preventing the dissemination of terrorist content online. The proposal builds on EU-level initiatives to foster the voluntary cooperation of service providers in stopping the dissemination of terrorist content online, and it echoes ongoing national developments which go a step further in imposing obligations – underpinned by considerable fines – on service providers. This article describes the main features of the proposal and highlights some of the policy challenges, legal questions, and technological concerns it is likely to face on the road to adoption.

I. Introduction

At the informal European Council summit in Salzburg on 19th and 20th September 2018, the European Commission presented a draft Regulation on preventing the dissemination of terrorist content online.¹ The proposal builds upon EU-level initiatives to foster the voluntary cooperation of service providers in stopping the dissemination of terrorist content online, chiefly the cross-sectoral EU Internet Forum and the work of Europol's Internet Referral Unit (IRU). It also echoes ongoing national developments which go a step further in imposing obligations – underpinned by considerable fines – on service providers to hastily remove illegal content and prevent re-uploading, such as the German *Netzwerkdurchsetzungsgesetz* (*NetzDG*), passed in June 2017. The Regulation would apply to “hosting service providers” (HSPs), defined as “a provider of information society services consisting in the storage of information provided by and at the request of the content provider and in making the information stored available to third parties” (Art. 2(1)).² Another prerequisite is that HSPs offer

services in the Union, irrespective of their place of main establishment (Art. 1(2)).

The draft Regulation, which is strongly supported by both France and Germany, takes a four-pronged approach to terrorist content online:

- At the “light touch” end of the regulatory spectrum it seeks to establish EU-wide general duties of care on HSPs to take “appropriate, reasonable and proportionate actions [...] against the dissemination of terrorist content and to protect users from terrorist content” (Art. 3);
- It would enshrine a framework of practical arrangements for HSPs' own assessment of terrorist content once “referred” to them by national competent authorities or the relevant Union body (Europol) (Art. 5), discussed below under II.;
- It introduces removal orders, to be issued by national competent authorities, which must be complied with within one hour (Art. 4). This is the proposal's flagship measure, and is discussed below under III. In addition to the tight deadline, the removal order comes with the most bite of the measures

foreseen in the draft Regulation: whilst HSPs in breach of the quasi-totality of the obligations anchored in the draft Regulation risk incurring penalties, a “systematic failure to comply” with removal orders specifically shall be subject to financial penalties of up to 4% of the HSP’s latest yearly global turnover (Art. 18(4));

- It seeks to erect a compliance framework aiming to ensure that HSPs develop and take proactive measures, “including by using automated tools”, in order to protect their services against the dissemination of terrorist content (Art. 6). The development and use of proactive measures, discussed below under IV., are subject to rather terse obligations relating to transparency (Art. 8) and safeguards (Art. 9).

II. Referrals

The inclusion of a referral mechanism in the draft Regulation reflects increasingly intensive co-regulatory efforts undertaken by EU, national and industry actors in recent years. Most notably, 2015 saw two key developments:

- First, the European Commission launched the EU Internet Forum to bring together the internet industry and Member States, as well as Europol, the Radicalisation Awareness Network and the European Strategic Communications Network in order to tackle the spread of terrorist content online;
- Second, Europol itself established internally the so-called EU Internet Referral Unit (IRU) to actively scan the internet for terrorist content and refer it to host platforms. The Commission reports that “over 50,000 decisions for referrals across over 80 platforms in more than 10 languages have been made since 2015”, whilst five Member States have since set up their own IRUs.³

Notwithstanding this increased voluntary activity, the Commission now posits that “referrals alone will not be able to achieve the necessary impact – particularly with regards [sic] to volume and speed of response”,⁴ necessitating also the introduction of removal orders and the development of proactive measures, discussed below under III. and IV. As such, the principal attraction of formalising the referral mechanism in a Regulation is represented by the attendant fines which it would require;⁵ the firm application of as-yet-undefined penalties is envisaged specifically in relation to HSPs’ “assessment of and feedback on referrals” (Art. 18(1)(c)). Although referrals are to be assessed not against provisions in EU or national law but against service providers’ own terms and conditions (Art. 5(5)),⁶ and as a rule the idea remains that it is HSPs which shall decide whether or not to take action, the pressure which HSPs are likely to come under from competent authorities sits uneasily with the term “voluntary consideration” (Art. 5(2) and Art. 2(8)). The choice of wording is all

the more regrettable since HSPs “shall, as a matter of priority, assess the content [...]” (Art. 5(5)), meaning that HSPs’ consideration of putative referred terrorist content is actually not voluntary but mandatory, with sanctions hovering over them in case of poor performance.

In assessing referrals from national competent authorities or from Europol, HSPs will have to grapple with the Regulation’s definitions of terrorist content. According to Art. 2(5) of the draft Regulation, “terrorist content” means one or more of the following information:

- (a) inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed;
- (b) encouraging the contribution to terrorist offences;
- (c) promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 2(3) of Directive (EU) 2017/541;
- (d) instructing on methods or techniques for the purpose of committing terrorist offences.

The Commission presents the inclusion of the last three categories, which are broader than the corresponding provisions in the 2017 Directive on combating terrorism,⁷ as a step to provide clarity to HSPs and competent authorities and as a basis for more effective preventative action,⁸ given the variable nature of content used for radicalisation purposes. In this context, the Commission refers to real-life cases:⁹ (1) a Danish schoolgirl found guilty in 2017 of attempted terrorism having tried to make bombs to be used in attacks against her former school (radicalised via internet and chat contacts within a few months); (2) *Daesh*’s tactics to “groom” young children (using cartoons); and (3) the attack on the Thalys train in 2015 that was provoked in the preceding moments by a “call to arms” on a YouTube audio file. Yet the examples of terrorist content cited all ostensibly feature an element that was not taken up by the definition in the draft Regulation: intent. This has raised concerns that any communication of terrorist-related content will be automatically deleted, irrespective of the context of its use (i.e. for confrontation, reporting, research or historical purposes).¹⁰ Without offering an explicit justification, the draft not only “draws on” (cf. recital 9), but also goes beyond the wording of the takedown obligation in the Directive on combating terrorism.¹¹

With that said, the converse would have seen HSPs tasked with assessing the intentions of content providers, thereby adding a further level of complexity to their task of identifying the content *per se* as terrorist, meaning *inter alia* “the nature and wording of the statements, the context in which the statements were made and their potential to lead to harmful consequences, thereby affecting the security and safety of persons”.¹² Faced with this heavy responsibility, HSPs as well as competent authorities are suitably reminded of the importance

of freedom of expression and information, “one of the values on which the Union is founded”.¹³ Digital rights campaigners, however, are unlikely to be reassured by much of the supporting argumentation put forward by the Commission.

In explaining its decision to broaden the definition of terrorist content to include recruitment and training for terrorism, the Commission draws attention to safeguards including (domestic) “judicial reviews of removal orders and the possibility to issue a counter-notice, as well as measures taken to mitigate the possibility of erroneous removals when deploying proactive measures”.¹⁴ Yet as regards referrals, which are non-binding, available redress is in fact limited to (private) complaint mechanisms (Art. 10). Moreover, the fact that HSPs’ assessments are to be facilitated by the prior appraisal of Europol and national authorities (which may be of a judicial, administrative, or most pertinently law enforcement nature) “with particular expertise to identify whether or not the content could potentially constitute terrorist content as defined by law” is proffered as a “safeguard” against erroneous removals.¹⁵ This reasoning seems to presuppose – and depend on – high levels of trust in the competent authorities.

III. Removal Orders

Under the proposal, national competent authorities may also issue removal orders to HSPs. Member States are free to assign this task to either administrative, law enforcement or judicial authorities.¹⁶ In contrast to referrals (see II.), HSPs must comply with removal orders within one hour of reception (Art. 4(2)). Thus, the provider can only decide whether to remove the relevant content or to block access thereto.¹⁷ Removal orders sent to HSPs shall contain, *inter alia*, a statement of reasons explaining why the content is considered terrorist content by reference to the definitions used in the draft Regulation, information enabling the identification of the content referred (typically a URL), and information about redress available to both the HSP and to the content provider.

From the content providers’ perspective, the draft Regulation provides that HSPs are in turn to supply them with “information” regarding the removal or blocking of content (Art. 11(1)) and (upon request of the content provider) reasons for such action (Art. 11(2)). However, these obligations may be suspended for up to four weeks where the competent authority decides for reasons of public security, such as the prevention, investigation, detection and prosecution of terrorist offences, that no information on removal or blocking should be disclosed. Although the instrument would require HSPs to establish (private) mechanisms allowing content providers to complain and request the reinstatement of content removed

or blocked pursuant to a referral or via proactive measures (Art. 10), this – understandably – does not apply to content removed or blocked by HSPs pursuant to a non-negotiable one-hour removal order.

Rapidity is the order of the day not only as regards HSPs’ responses to removal orders; it also characterises the recent policy-making flurry at EU level. The proposal for a Regulation comes hot on the heels of the Commission’s March 2018 Recommendation on measures to effectively tackle illegal content online. It encouraged Member States to develop their response to all types of illegal content, *inter alia*, through systems of notices to HSPs, informing content providers and counter-notices, transparency and safeguards, and the cooperation of HSPs with national competent authorities, with “trusted flaggers”, and amongst themselves.¹⁸ Indeed, most of the core provisions of the draft Regulation have been fleshed out from the Commission’s earlier specific recommendations relating to terrorist content, which featured *inter alia* a ban on terrorist content in HSPs’ terms of service, referrals, proactive measures, cooperation and the one-hour rule.¹⁹

Hosting service providers should assess and, where appropriate, remove or disable access to content identified in referrals, as a general rule, within one hour from the moment at which they received the referral.

Should the draft Regulation enshrine the one-hour rule in EU law, this will represent a real change of gear compared to the existing general, open-ended obligation on Member States to “take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence” (Art. 21 of Directive (EU) 2017/541 on combating terrorism). The deadline for implementation of the Directive passed on 8 September 2018 – less than a fortnight before the draft terrorist content Regulation was unveiled – with the Commission stating that 15 Member States had notified it of measures giving effect to their Art. 21 obligation in their domestic systems.²⁰ Arguably, an evaluation of national measures taken pursuant to Art. 21 would be essential to gauging the added value of the Directive, as well as “its impact on fundamental rights and freedoms, including on non-discrimination” (Article 29, Directive on combating terrorism). The distant deadline for the Commission’s added value report, however, is 8 September 2021.

In opting to respond to Member State pressure with a proposal for a Regulation²¹ before any such evaluation of the Terrorism Directive has occurred, the Commission may also have been swayed by its experience of chasing up the slow and patchy implementation of Art. 25 of Directive 2011/92/EU. This provision stipulates that Member States *shall* on the one hand take the necessary measures to ensure the prompt removal of, and *may* on the other hand take measures to

block access to, web pages containing or disseminating child pornography.²²

The draft Regulation covers the main practical matters on the procedure for removal/blocking orders, e.g. nomination of HSP points of contact or legal representatives, framework for interaction between HSPs and competent authorities, provisions on language etc., but, as noted above, controversially²³ leaves open a key aspect to the Member States: the choice of competent authority. The Commission itself notes that in the majority of national systems a takedown order may come only from a judicial body within criminal proceedings. Some Member States, however, provide for administrative orders – subject to appeal before a court – and in a few Member States even law enforcement authorities can issue removal orders and refer content to service providers.²⁴

This flexibility stands in contrast to the one-hour rule, which applies only to removal orders, is far tighter than existing provisions in national law mandating, for instance, removal within 24 or 48 hours,²⁵ and is justified by the Commission by reference to the speed at which terrorist content is claimed to spread across online services.²⁶ The preference for such a short window for removal or blocking goes hand-in-hand with the Commission's choice to eschew an "all illegal content" approach – deemed "unnecessary and disproportionate"²⁷ – and focus instead on terrorist content as a priority, at least for now.

The immediate imperative to act at national level is of course constituted by the increasing use of HSPs to disseminate terrorist content. The main driver for EU action on an Art. 114 TFEU legal basis, meanwhile, is the hindrance to the effective exercise of freedom of establishment and freedom to provide services across the Union which may result from the legal uncertainty caused by a deepening "fragmentation" of national responses to the removal or disabling of access to illegal content in general (as already envisaged in the e-commerce Directive)²⁸ and terrorist content in particular (as recently mandated by the Terrorism Directive). Here too, there is fertile ground for debate over the coming months as to the true necessity of EU action – and not only from a freedom of expression perspective. Notably, whereas one might expect the anchoring of such a forceful rule as the one-hour window in a Regulation to receive solid backing from law enforcement circles, national law enforcement authorities are in fact cited by the Commission as favouring the continuation of self-regulatory initiatives, "allowing industry to take the lead ... whilst working closely with them".²⁹

On the HSP side, the Commission also cites input from "companies" to the effect that diverging legislation is a serious concern and smaller companies are likely to suffer the most from

28 different sets of rules.³⁰ This position calls for two remarks. First, although it seems undeniable that the functioning of the "country of origin" principle would likely be undermined by the continued proliferation of national removal order systems with differing assessments of terrorist content (e.g. compliance with regulatory requirements in one Member State ensuring access to all others, only for one or several of those other Member States to remove or block access to content), the added value of the draft Regulation in this specific respect would seem to depend on levels of cohesiveness between competent authorities which are high enough to produce similarity between the decisions they take.³¹ This may raise workability concerns, particularly given the likely varying nature of competent authorities and the open-ended definition of terrorist content they are to be mandated to apply. Second, with regard to impact on smaller HSPs, achieving readiness to respond to one-hour takedown orders could indeed affect small companies even more compared to the status quo – although this is, in principle, to be factored into sanctioning decisions.³² In these respects, we can expect industry to call for further clarification and substantiation in the near future.

IV. Proactive Measures

Perhaps the most novel section of the draft Regulation entails a duty on HSPs to take proactive measures to protect their services against the dissemination of terrorist content (Art. 6). HSPs are to report to the competent authority³³ on "the specific proactive measures [...] taken, including by using automated tools, with a view to:

- preventing the re-upload of content which has previously been removed or to which access has been disabled because it is considered to be terrorist content;
- detecting, identifying and expeditiously removing or disabling access to terrorist content".³⁴

Should the competent authority deem such measures to be insufficient, the HSP is bound to cooperate with it in order to establish "key objectives and benchmarks as well as timelines for their implementation" (Art. 6(3)). Where no agreement can be reached, the taking of specific proactive measures can be imposed on HSPs by the competent authority (Art. 6(4)). Penalties for HSPs which fail to report on proactive measures, or to adopt such measures following a decision imposing them, are to be set out at national level (Art. 18(1)(d)).

This mini-compliance framework for the automated detection and removal of terrorist content channels a fairly recent but major growth in political pressure³⁵ as well as industry activity, chiefly in the form of a pooled "hash database".³⁶ The extent to which such initiatives and the technologies they employ are truly effective at accurately identifying terrorist content (as

distinct from removing vast swathes of content)³⁷ raises a set of thorny issues which are likely to play out in the months to come, particularly given the European Parliament's position on the importance of transparency in the use of algorithms. In this context, the EP recently called on the Commission and the Member States to "examine the potential for error and bias in the use of algorithms in order to prevent any kind of discrimination, unfair practice or breach of privacy".³⁸

Counterbalancing its provisions designed to foster the uptake of proactive measures, the draft Regulation stipulates standard GDPR-era obligations on HSPs. These include the provision of a meaningful explanation of such tools in their terms and conditions, the publication of transparency reports (including "information" and absolute figures on action taken and complaint procedures) and the provision of safeguards to ensure that decisions taken concerning stored content are "accurate and well-founded". Safeguards shall consist, in particular, of "human oversight and verifications where appropriate and, in any event, where a detailed assessment of the relevant context is required in order to determine whether or not the content is to be considered terrorist content" (Art. 9). Beyond the European Parliament's calls for caution, it is worth noting the concerns voiced by *David Kaye*, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, a few weeks before publication of the draft Regulation. In his report, *Kaye* makes specific reference to the application of artificial intelligence (AI) tools to online content and states:³⁹

Even when algorithmic content moderation is complemented by human review – an arrangement that large social media platforms argue is increasingly infeasible on the scale at which they operate – a tendency to defer to machine-made decisions (...) impedes interrogation of content moderation outcomes, especially when the system's technical design occludes that kind of transparency.

The Commission considered several options with regard to the use of automated tools: deferring to companies' own risk assessment; mandatory uptake of measures limited to the prevention of re-uploading of known terrorist content; and mandatory uptake of "appropriate proactive measures, including by using automated detection tools".⁴⁰ Despite the above-mentioned misgivings, which can also be found amongst EU Member State governments,⁴¹ the Commission has chosen the most far-reaching option. It does so whilst acknowledging⁴² that should proactive measures inadequately distinguish between unlawful and lawful conduct, this may risk undermining, *inter alia*, freedom of information in contravention of settled EU law.⁴³ This tense relationship with standing CJEU case law barring the imposition of systematic ISP (internet service provider) filtering for copyright breaches is also reflected in the wording of recital 16 to the draft Regulation. That recital states that whilst on the one hand it is up to HSPs to determine what proactive measure should be put in place, on the other hand "(t)his re-

quirement should not imply a general monitoring obligation". Should the co-legislators concur with those judges who have remarked that the use of automated processes is "pushing in the direction" of a general monitoring obligation,⁴⁴ we may yet see a return in the final text to one of the more limited policy options evoked in the Commission's Impact Assessment.

Lastly, a less immediately obvious legal tangle may await the proposal in general, and its drive toward proactive measures in particular. Art. 7 of the draft Regulation obliges HSPs to preserve terrorist content which has been removed or disabled as a result of a removal order, a referral or proactive measures. With a preservation period set at six months (extendable), the potential ramifications of this framework are bound to attract comparisons to the (annulled) Data Retention Directive – especially insofar as the obligation not only covers the targeted terrorist content per se but also extends to "related data removed as a consequence of the removal of the terrorist content" (Art. 7(2)).

The term "related data" is not defined in the main text of the draft Regulation, but subscriber data and access data are given as examples in recital 20. This is unlikely to quell fears of over-preservation by HSPs and will likely fuel calls for a more precise wording. Moreover, whatever data is preserved by HSPs as being in their estimation "likely to have a link with terrorist offences" (recital 21) may be used for the prevention, detection, investigation and prosecution of terrorist offences (Art. 7(1)(b)). Depending on definitions in place in national systems, these purposes may open broad channels of access to large amounts of data generated by the customers of HSPs. In turn, this approach triggers concerns regarding profiling, particularly in light of the CJEU's language on the use of non-content data to draw "very precise conclusions concerning the private lives of the persons whose data has been retained"⁴⁵ and lead to "the feeling that (users') private lives are the subject of constant surveillance".⁴⁶

V. Outlook

For the reasons evoked in this overview, the strong political support for swift regulatory action on terrorist content online, which is reflected in the Commission's draft Regulation, is sure to be tested as the proposal progresses through the EU's legislative procedure – in particular by pressure from the Internet industry and digital rights groups.

Taken as a whole, the proposal envisages the transformation of extant co-regulation and voluntary self-policing by hosting service providers (HSPs) into a framework of obligations (to respond to referrals; to comply with removal orders; to imple-

ment proactive measures) bolstered by sit-up-and-take-notice sanctions. To deliver on this vision, the dossier will have to navigate doubts as to the necessity of taking such action at EU level. This may be accompanied by principled objections on grounds of freedom of expression. The initiative will also encounter narrower concerns over its potential impact on smaller HSPs and over key matters of scope and legal certainty – right down to the broadly termed definition of “terrorist content” provided therein.

With the EU Council having agreed its negotiating position on the proposal in early December 2018,⁴⁷ the ball is now squarely in the European Parliament’s court. Given that the next elections to the Parliament are scheduled for late May 2019, we can expect the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) to finalise its report on the proposal before then. We may have to wait until the fourth quarter of 2019, however, to see interinstitutional talks begin.

1 COM(2018) 640 final.

2 Recital 10 of the draft gives as examples: “social media platforms, video streaming services, video, image and audio sharing services, file sharing and other cloud services to the extent that they make the information available to third parties and websites where users can make comments or post reviews”.

3 SWD(2018) 408 final, “Impact Assessment”, 140.

4 Impact Assessment, *ibid.*

5 The draft Regulation also advises that receiving a high number of referrals – or removal orders – indicates a high level of exposure to terrorist content, meaning proactive measures are more likely to be necessary (see e.g. recital 16).

6 By virtue of the aforementioned duties of care (and in a rather circular dynamic) such terms and conditions must include provisions to prevent the dissemination of terrorist content (Art. 3(2)).

7 “Member States shall take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence”; Art. 21 of Directive (EU) 2017/541 of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, *O.J. L* 88, 31.3.2017, p. 6.

8 See recital 9 of the draft Regulation.

9 Cf. Impact Assessment, *op. cit.* (n. 3), 17.

10 *EDRi*, “EU’s flawed arguments on terrorist content give big tech more power”, 24 October 2018, <<https://edri.org/eus-flawed-arguments-on-terrorist-content-give-big-tech-more-power/>> accessed 3 January 2019.

11 Public provocation to commit a terrorist offence is defined non-exhaustively in the Directive on combating terrorism (*op. cit.* n. 7) as “the distribution, or otherwise making available by any means, whether online or offline, of a message to the public, with the intent to incite the commission of one of the offences listed in points (a) to (i) of Art. 3(1), where such conduct, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed, is punishable as a criminal offence *when committed intentionally*” (Art. 5; emphasis added).

12 Recital 9 taking up relevant ECtHR case law. Moreover, recital 9 mentions that “(t)he fact that material was produced by, is attributed to or disseminated on behalf of an EU-listed terrorist organisation or person constitutes an important factor in this assessment”.

13 Recital 7.

14 Impact Assessment, *op. cit.* (n. 3), 103.

15 Impact Assessment, *op. cit.* (n. 3), 42. See also Annex 5, Impact on Fundamental Rights: “(W)hen referrals are issued by Europol, the fact that Europol is bound to act only within its mandate (...) makes it unlikely that any removal decision based on referrals would concern protected speech. The obligation on HSPs to assess the content flagged through referrals could have a significant impact on the freedom to conduct a business (...). The burden is alleviated by the high quality of the Europol and Member States (sic) referrals” (Impact Assessment, p. 104).

16 Cf. recital 13.

17 Cf. recital 13.

18 Recommendation (EU) 2018/334, *O.J. L* 63, 6.3.2018, 50. See also the subsequent European Council conclusions of 28 June 2018, at para. 13: “... welcomes the intention of the Commission to present a legislative proposal to improve the detection and removal of content that incites hatred and to commit terrorist acts”.

19 Recommendation (EU) 2018/334, *ibid.*, para. 35.

20 Impact Assessment, *op. cit.* (n. 3), 9 and 116.

21 An amendment of the Terrorism Directive, for instance to broaden the activities/material covered therein from incitement to terrorism only to other offences (as proposed in the draft Regulation), was discarded by the Commission. It argued that “the focus on criminalisation of terrorist offences as opposed to purely preventative measures, the geographical limitations and limitations in terms of safeguards and other flanking measures (which would not have been possible under this legal basis) (...) would have had limited impact on the objective of preventing the dissemination of terrorist content” (Impact Assessment, *op. cit.* (n. 3), 25).

22 See COM(2016) 872 final, where the Commission (at 12) stated that continued work was still required to ensure the “complete and correct implementation” of Art. 25 across the Member States – a full three years after the deadline of 18 December 2013, with the Commission having opened infringement proceedings against a total of 15 Member States.

23 In this regard, see the concerns raised by a coalition of 31 civil society organisations in a letter sent to EU Member States’ Home Affairs Ministers on 4 December 2018, available at <https://edri.org/files/counterterrorism/20181204-CivilSociety_letter_TERREG.pdf> accessed 3 January 2019.

24 Impact Assessment, *op. cit.* (n. 3), 9-10.

25 Impact Assessment, *op. cit.* (n. 3), 116.

26 See also the “evidence summary” on terrorist content online (Annex 9, Impact Assessment, *op. cit.* (n. 3), 138), referring to one example of UK Home Office analysis showing that a third of Daesh links are disseminated within the first hour.

27 Impact Assessment, *op. cit.* (n. 3), 23.

28 Art. 14(3) of Directive 2000/31/EC: “This article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States

Dr. Gavin Robinson

Postdoctoral Researcher: Criminal law & IT law,
University of Luxembourg



of establishing procedures governing the removal or disabling of access to information”.

29 Impact Assessment, *op. cit.* (n. 3), 116.

30 Impact Assessment, *op. cit.* (n. 3), 10.

31 See e.g. Art. 13(1) of the draft Regulation: “Competent authorities in Member States shall inform, coordinate and cooperate with each other and, where appropriate, with relevant Union bodies such as Europol with regard to removal orders and referrals to avoid duplication, enhance co-ordination and avoid interference with investigations in different Member States”.

32 Member States shall take into account *inter alia* “the financial strength of the legal person liable” in applying sanctions (Art. 18(3)(d)).

33 The “competent authority” may be different to that in charge of referrals and removal orders, see Art. 17.

34 Cf. Art. 6(2) of the Commission’s proposal COM(2018) 640.

35 See the European Council conclusions on security and defence of 22 June 2017, point 2: “Building on the work of the EU Internet Forum, the European Council expects industry to establish an Industry Forum and to develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts. This should be complemented by the relevant legislative measures at EU level, if necessary”. See also, subsequently to the Commission’s proposal for a Regulation, European Parliament, Report on findings and recommendations of the Special Committee on Terrorism (2018/2044(INI)), 21 November 2018, 47: “underlines the need to achieve automatic detection and systematic, fast, permanent and full removal of terrorist content online on the basis of clear legal provisions including safeguards, and human review; [...] welcomes the Commission’ legislative proposal [...]; calls on the co-legislators to urgently work on the proposal [...]”.

36 Under the aegis of the Global Internet Forum to Counter Terrorism, founded in June 2017 by the Big Four of Facebook, Microsoft, Twitter and YouTube. See <<https://gifct.org/about/>> accessed 3 January 2019.

37 Cf. the comment of D. Keller, “Inception Impact Assessment: Measures to Further Improve the Effectiveness of the Fight Against Illegal Content Online”, 29 March 2018, available at SSRN: <<http://dx.doi.org/10.2139/ssrn.3262950>>,

accessed 3 January 2019: “Technical filters cannot assess context or tell whether potentially terrorist content is actually illegal. No existing machine – be it a simple filter or the most advanced artificial intelligence – can review new material, or look at old material in a new context, and say with certainty whether it violates the law”.

38 European Parliament, Report on online platforms and the digital single market (2016/2276(INI)), 31.5.2017, at 17 (Legal Affairs Committee) and 12 (full report).

39 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 29 August 2018, A/73/348, para. 15.

40 Impact Assessment, *op. cit.* (n. 3), 105.

41 Cf. Impact Assessment, *op. cit.* (n. 3), 120: “Regarding filtering, the (Dutch) government has indicated that this does not work adequately, since in case of terrorism unlawful content is not as evident as compared to e.g. child pornography, resulting in a disproportionate interference with the right to freedom of speech”.

42 Impact Assessment, *op. cit.* (n. 3), 105.

43 CJEU, 24 November 2011, Case C-70/10, *Scarlet Extended SA v SABAM*, paras 50 *et seq.*

44 Impact Assessment, *op. cit.* (n. 3), 76.

45 CJEU, 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger*, para 27.

46 *Digital Rights Ireland*, *ibid*, para 37 and CJEU, 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB and Secretary of State for Home Department v Tom Watson and Others*, para 100. Cf. CJEU, 2 October 2018, Case C-207/16, *Ministerio Fiscal*, wherein a targeted request for access to data concerning a stolen mobile telephone was deemed to “not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned” (para 60).

47 Press release, “Terrorist content online: Council adopts negotiating position on new rules to prevent dissemination,” 6 December 2018, <<https://www.consilium.europa.eu/en/press/press-releases/2018/12/06/terrorist-content-online-council-adopts-negotiating-position-on-new-rules-to-prevent-dissemination/>>, accessed 3 January 2019.

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



MAX-PLANCK-GESellschaft

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



© Max Planck Institute for Foreign and International Criminal Law 2019. All rights reserved: no part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical photocopying, recording, or otherwise without the prior written permission of the publishers.

The views expressed in the material contained in eucrim are not necessarily those of the editors, the editorial board, the publisher, the Commission or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the Commission are not responsible for any use that may be made of the information contained therein.

Editor in Chief: Prof. Dr. Dr. h.c. mult. Ulrich Sieber
Managing Editor: Thomas Wahl, Max Planck Institute for Foreign and International Criminal Law, Freiburg
Editors: Dr. András Csúri, Utrecht University; Cornelia Riehle, ERA, Trier
Editorial Board: Peter Csonka, Head of Unit, DG Justice and Consumers, European Commission Belgium; Francesco De Angelis, Directeur Général Honoraire, Commission Européenne Belgique; Prof. Dr. Katalin Ligeti, Université du Luxembourg; Lorenzo Salazar, Ministero della Giustizia, Italia; Prof. Rosaria Sicurella, Università degli Studi di Catania, Italia
Language Consultant: Indira Tie, Certified Translator, Max Planck Institute for Foreign and International Criminal Law, Freiburg
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

