As co-editor and contributor to an edited volume on the 'Cooperation of the EU and South Korea on cyber security: Towards Rules-Based Cyber-Peace' – forthcoming this year with Palgrave – internet-based problems for law enforcement and the need for judicial cooperation, within the EU and globally, got my attention.

The **Budapest Convention on Cybercrime**[1] under the auspices of the Council of Europe, is so far the only international agreement with recognised rules in the cyber area. Japan joined the Convention already in 2012.

Discussions at the level of the **United Nations** are not progressing either, as two camps oppose each other: while one group is in favour of a new treaty to regulate the internet e.g., introducing a strong state element, others fear that such a treaty could be misused and endanger the free and open internet. Striking a balance between efficiency of law enforcement, personal data protection, respect of human rights is a difficult task, whether at the European[2] or global level. Nevertheless, the problem is to stay and even getting more pronounced and acute because of technological progress, where the law is always behind.

Crime leaves **digital traces** that can serve as evidence in court proceedings. Often, such traces will be the only lead law enforcement authorities and prosecutors can collect. Therefore, effective mechanisms to obtain digital evidence are of the essence.

The **Second Additional Protocol of the Budapest Convention**[3] has been opened for signature in 2021[4]. It strives to facilitate obtaining electronic evidence stored in foreign, multiple, shifting or unknown jurisdictions. The Protocol provides tools for enhanced co-operation and disclosure of electronic evidence - such as direct cooperation with service providers and registrars, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies or joint investigations. As the Council of Europe is the watch dog over human rights (European Convention on Human Rights), all these measures are subject to control by a system of human rights and rule of law, including data protection safeguards.

The European Commission is pursuing the same goal with the EU. In 2018 the European Commission proposed the **E-Evidence legislative package**[5] to facilitate and accelerate law enforcement and judicial authorities' access to electronic evidence to better fight crime and terrorism. Law enforcement authorities need the right tools to investigate and prosecute crimes in the digital age. This also applies to rather common techniques, the use of video conferences in legal matters, whether civil or criminal.[6]

[1] https://rm.coe.int/1680081561
[2] The "e-Justice Portal", a website of the EU, provides information on the latest developments in the field, at https://e-justice.europa.eu/home?plang=en&action=home (accessed 16 March 2022)
[3] https://rm.coe.int/1680a49dab
[4] Council of Europe. Action against cybercrime, at https://www.coe.int/en/web/cybercrime/home ; see also https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention
[5] European Commission. E-evidence, at https://ec.europa.eu/home-affairs/cybercrime/e-evidence_en (accessed 17 March 2022).
[6] E-justice. Videoconferencing; at https://e-justice.europa.eu/36019/EN/videoconferencing (accessed 17 March 2022). The portal provides links to practice in Member States on taking evidence (https://e-

International cooperation is a MUST, as useful information needed for criminal investigations and prosecutions is stored in the cloud, on a server in another country and/or held by service providers that are located in other countries. Even where all other elements of a case are located in the investigating country, the location of the data or of the service provider can create a cross-border situation.

Traditional means to obtain information, the European Investigation Order or Mutual Legal Assistance agreements (MLA) were designed for traditional investigative measures, but are too slow for obtaining electronic evidence which can be transferred or deleted at the click of a mouse[7].

The Council and the European Parliament (EP) presented their **draft Regulation on European production and preservation orders for electronic evidence in criminal matters** in November 2018[8]. Ever since a fierce legal and political battle[9] is raging with civil society and interest groups[10] strongly protesting and rendering the trilogue, the procedure to find a compromise between the three EU institutions, rather difficult. 841 proposed amendments speak for themselves[11].

Fast forward: The French presidency of the Council had listed 'Evidence in criminal proceedings: European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 COD)' as a priority[12] item of the work program although acknowledging from the outset, that conclusion of this file remains uncertain. Thus, at the Justice and Home Affairs Council on 4 March 2022, ministers were informed that the creeping formal trilogue has resumed. The main point of divergence remains the question of the

justice.europa.eu/405/EN/taking_evidence_by_videoconference) as well as a Manual dealing with the technical data (https://e-justice.europa.eu/71/EN/manual).

[7] European Commission. Security union facilitating access to electronic evidence, Fact sheet; April 2018; at https://ec.europa.eu/info/sites/default/files/placeholder_2.pdf

[8] https://data.consilium.europa.eu/doc/document/ST-15020-2018-INIT/en/pdf

[9] EDRi (2018). "EU Council's general approach on "e-evidence": From bad to worse". 19 December 2018; at https://edri.org/our-work/eu-councils-general-approach-on-e-evidence-from-bad-to-worse/

[10] E-Evidence Coalition remarks on the on the Rapporteur package proposal. 2022; at https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2022/Coalition's%20remarks%20on%20EP%20package%20deal.pdf (accessed 17 March 2022).
Opinion of the European Economic and Social Committee on 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters', 2018; at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018AE2737&from=EN

[11] Theodore Christakis (2020). "E-Evidence in the EU Parliament: Basic Features of Birgit Sippel's Draft Report". European Law Blog, 21 January 2021; at https://europeanlawblog.eu/2020/01/21/e-evidence-in-the-eu-parliament-basic-features-of-birgit-sippels-draft-report/#:~:text=Despite%20difficult%20negotiations%20among%20EU%20Member%20States%2C%20the,States%2C%20including%20Germany%2C%20who%20opposed%20the%20Council%E2%80%99s%20draft.
EP (2018). An assessment of the Commission's proposals on electronic evidence. At https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf

[12] EP (2022). Priority dossiers under the French EU Council Presidency. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698865/EPRS_BRI(2022)698865_EN.pdf

procedure for the notification of the request by the requesting authority to the authority of the member state of the place of establishment of the private supplier[13].

In addition, the **Covid-19 pandemic**[14] has given a boost to **e-justice** e.g., the overall technical framework of exercising justice and guaranteeing fundamental rights and the rule of law. The 'old courtrooms' have to open to new technologies; the working methods are undergoing fundamental changes.

More specifically, the experience of the discussion of the **rule of law** in some member states and the temporary introduction of emergency measures because of COVID-19 limiting fundamental freedoms, have created a heightened concern that legislation in such a sensitive area has to life up to high judicial standards.

Therefore, the EP suggests, that orders originating with a member state under observation according to Article 7 of the EU Treaty ("a clear risk of a serious breach by a Member State of the values referred to in Article 2") [15], the executing state has to confirm the release of any data. This procedure includes additional safeguards compared to the normal procedure where the EP suggests "a notification procedure by the executing state for all production and preservation orders, in some cases with suspensive effect. The issuing or validation of an order for the production of traffic or content data must be carried out by a judge."[16]

Thus, this remains work in progress!

For discussion:

1. ***How to solve the dilemma of the speed of the internet in criminal matters (a mouse click) vs. procedural safeguards in legal proceedings as well as international cooperation, which has become essential in cyber issues.***
2. ***Cyber platforms, connections are primarily owned and managed by private service providers and their cooperation is required (pursuing electronic traces, taking down hate speech, child pornography…) – to which extend can they be entrusted with law enforcement.***
3. ***How to safeguard the fundamental rights of persons against attempts by states to infringe rights in breach of rule of law, either in form of "fishing expeditions" or to obtain data for political purposes.***

[13] Council of the European Union (2022) https://www.consilium.europa.eu/en/meetings/jha/2022/03/03-04/
[14] E-justice. "Impact of COVID-19 on the justice field", offering a comprehensive overview; at https://e-justice.europa.eu/37147/EN/impact_of_covid19_on_the_justice_field?clang=en; see also Council of Europe. "Management of the judiciary - compilation of comments and comments by country", with an interactive map; at https://www.coe.int/en/web/cepej/compilation-comments
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016M007
[16] Thomas Wahl (2021). "E-Evidence Package: EP Paves Way for Trilogue Negotiations". eucrim 19 January 2021; at https://eucrim.eu/news/e-evidence-package-ep-paves-way-trilogue-negotiations/

These concerns can also be found in the questions raised in relation to the e-evidence package, as formulated by EDRi[17], the biggest European network defending rights and freedoms online, which comprises 45 non-governmental organisations:

- *Missing involvement of the "affected State"*

Under the Committee Report[18], the judicial authorities of the affected person's country of residence are no longer consulted nor required to validate any e-evidence orders as originally suggested in the Rapporteur's draft report. The so-called "affected State" would therefore be unable to block illegal foreign data requests. This is particularly unfortunate as the affected person's Member State of residence is usually best placed to protect their fundamental and procedural rights and to know about potential special protections of journalists, doctors, lawyers, etc. This also creates barriers for the affected person's right of access to justice.

- *Insufficient involvement of the executing State*

The service provider is requested to hand over subscriber data and IP addresses as soon as possible and within set short deadlines without being allowed to await a validation of the judicial authorities of its Member State of establishment. Extending an EU member state's law enforcement powers beyond its own national borders is a fairly novel and highly risky approach. What is more, some of the safeguards approved by the Committee will have little to no effect in practice, such as the erasure obligation in case the executing State objects to an order after the data has been transferred.

- *Lack of safeguards against fishing expeditions*

The report fails to adequately protect against fishing expeditions, whereby law enforcement authorities request untargeted, massive amounts of data without justification in order to uncover incriminating evidence that was not previously suspected to exist. The Committee Report should have clarified a service provider's right to refuse an order in case it is "manifestly abusive" because it is not targeted at a specific person or a limited group of persons.

- *Lack of safeguards against deficiencies in mutual trust and EU judicial cooperation*

The Committee report introduces stronger safeguards for data requests coming from Member States that are currently under Article 7 investigations for systematically breaching the rule of law. Those stronger safeguards should have been the norm for all EU Member States and be extended to e-evidence orders for subscriber information and IP addresses as well.

[17] EDRi, "E-evidence": Mixed results in the European Parliament; at https://edri.org/our-work/ e-evidence-mixed-results/

[18] European Parliament (2020). "Report on the 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)0225 – C8-0155/2018 – 2018/0108(COD)"; at https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html