European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

6.2.2019

2nd WORKING DOCUMENT (B)

on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) - Scope of application and relation with other instruments

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Birgit Sippel

Co-Author: Nuno Melo

Introduction

This part of the working document will analyse possible connections of the proposed e-evidence Regulation with two already existing legal instruments regulating e-evidence, namely the Directive 2014/41/EU on the European Investigation Order in criminal matters (EIO) and the 2001 Convention on Cybercrime of the Council of Europe (CETS No.185, 'the Budapest Convention').

European Investigation Order

Directive 2014/41/EU on the European Investigation Order[1] was adopted as an overall system for mutual recognition of all investigative measures aimed at collecting evidence (except in the context of joint investigation teams).[2] All Member States, except for Ireland[3] and Denmark[4], are participating in the instrument. As an overall investigative instrument, it also covers electronic evidence. However, in terms of scope, the EIO Regulation is more narrow than the e-evidence Regulation as it does not cover third country providers nor providers in Ireland. Instead of replacing the EIO, the proposed e-evidence Regulation is intended to co-exist with the EIO.[5]

Production of e-evidence under the European Investigation Order

As regards the competent issuing authority, the EIO Directive stipulates, for all data categories, the necessity of a judicial order or a validation by a judicial authority, namely "a judge, a court, an investigating judge or a public prosecutor competent in the case concerned" (Art. 2 (c)(i) EIO), or "any other competent authority as defined by the issuing State" (Art. 2 (c)(ii) EIO) whereby, in the latter case, a validation by a judicial authority is necessary. In addition, where the investigative measure requires a court authorisation in the executing state, such order has to be sought.[6]

As regards the execution of an investigative measure, the EIO foresees different rules for

[1] It had to be transposed till 22 May 2017. All Member States affected by the EIO Directive have transposed it, although some after the foreseen deadline. It was proposed by an initiative of some Member States (Council EU, 09288/2010) but significantly transformed in the co-legislative negotiations based on strong insistence of the EP (Rapporteur for the file was Mr. Nuno Melo, EPP). The procedure took from May 2010 till April 2014 due to the complexity of legal questions raised. It was based on lengthy negotiations between Council and the EP from 2012 till 2014, whereby the internal EP position for negotiations was agreed first half of 2012 (an interesting comparison with the time-line on e-evidence as the instrument are similarly complex).

[2] Article 3 of Directive 2014/41/EIO (Scope).

[3] Protocol No. 21 to the Treaties - no Irish opt in to the EIO.

[4] Protocol No. 22 to the Treaties.

[5] See Commission document (COM(2018) 225): *"The new instrument will not replace the EIO for obtaining electronic evidence but provides an additional tool for authorities. There may be situations, for example when several investigative measures need to be carried out in the executing Member State, where the EIO may be the preferred choice for public authorities. Creating a new instrument for electronic evidence is a better alternative than amending the EIO Directive because of the specific challenges inherent in obtaining electronic evidence which do not affect the other investigative measures covered by the EIO Directive."*
Several service providers and civil society organisations, however, have already argued that, with regard to the production or preservation of e-evidence in practice, Member States will most likely opt for using the e-evidence instrument instead of the EIO.

[6] Article 2 EIO.

different types of e-evidence:

(a) Subscriber data and IP addresses (regardless of whether they are static or dynamic): Article 10(2)(e) EIO already provides that all Member States participating in the EIO, as regards their function as executing states, have to put in place investigative measures that allow for the identification of persons holding a subscription of a specified phone number or an IP address[1] Moreover, as regards these types of electronic data, the number of non-recognition grounds, as outlined in Article 11(1) of the EIO, is limited[2], which makes the refusal of a request for subscriber data and IP addresses less likely.

(b) Historical traffic data (*ex tunc*): Because of the remaining different national (constitutional) classifications of such data[3], the lack of EU harmonisation in this regard, and to respect the constitutional traditions and identities of the Member States[4], when it comes to the EIO requests for historical traffic data, the EIO Directive gave two possibilities to the Member States: In their transposition of the EIO Directive into national law, Member States could decide to consider measures on historical traffic data as coercive (invasive), or non-coercive (non-invasive) measures.

Where Member States decide to consider the data as non-coercive according to national law,

[1] Consequently, a refusal by the executing state cannot be based on the claim that such a measure is not available under its law.

[2] See Article 11(2) EIO *("Paragraphs 1(g) and 1(h) do not apply to investigative measures referred to in Article 10(2).")*. Consequently the double criminality check is excluded for all the offences, and it applies to all offences (no limitation to catalogue offences only).

[3] See Article 10(2)(d) and Recital 30 EIO: *"Possibilities to cooperate under this Directive on the interception of telecommunications should not be limited to the content of the telecommunications, but could also cover collection of traffic and location data associated with such telecommunications, allowing competent authorities to issue an EIO for the purpose of obtaining less intrusive data on telecommunications. An EIO issued to obtain historical traffic and location data related to telecommunications should be dealt with under the general regime related to the execution of the EIO and may be considered, depending on the national law of the executing State, as a coercive investigative measure."* Further, Recital 16 provides guidelines on the term "non-coercive" ("*Non-coercive measures could be, for example, such measures that do not infringe the right to privacy or the right to property, depending on national law."*). Thus, coercive (invasive) measures could be, for example, the ones infringing the right to privacy or property.

[4] Respect for national constitutional traditions and identities is specifically mentioned in Article 4(2) TEU and Article 67(1) TFEU. However, it seems that there is a trend that traffic data is considered as a sensitive category (similar to content data) and therefore additional safeguards are necessary. See, for example the EU Court of Justice, joint cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others - *"Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them"*. (para. 27)
See also Court of Justice, Joined Cases C-203/15 and C-698/15, Tele2 and Secretary of State for the Home Department - *"119. ...the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime... 120. In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime..."* The understanding of gathering traffic data as (non)coercive measures has to be seen in light of this recent legal developments.

the same ("lighter") approach as for subscriber data (see above) can be applied. However, where Member States decide, due to their national (constitutional) law, to consider measures for gathering of historical traffic data to be coercive (invasive), similar to content data, the general EIO regime applies. Thus, the full general catalogue of non-recognition grounds applies (including, outside the catalogue of 32 offences, a double criminality check and the limitation of any requested measures to certain serious offences only).

(c) Data gathered in real time, continuously and over a certain period of time (non-historical traffic data, *ex nunc*)[1]: The conditions for an investigative measure relating to data gathered in real time, continuously and over a certain period of time are outlined in Article 28 EIO, which defines an additional non-recognition ground for this type of data besides the general non-recognition grounds, namely "if the execution of the investigative measure concerned would not be authorised in a similar domestic case".

(d) Content data for interception of telecommunications: As regards the content data for interception of telecommunications, Articles 30 and 31 EIO apply. As for point (c), the EIO stipulates that for this type of data, not only the general non-recognition grounds apply, but an additional non-recognition ground of "if the execution of the investigative measure concerned would not be authorised in a similar domestic case" applies.

The e-evidence proposal does not cover the real-time gathering of data but is limited to stored data only.

The EIO Directive introduces strict obligations on Member States. With regard to the time limits for e-evidence measures under the EIO Directive, the general EIO time limits apply. This means that any investigative measure shall be carried out with the same celerity and priority as for a similar domestic case, and within a maximum of 30 days for recognition, and maximum of 90 days for execution.[2] However, the issuing Member State can insist that the measure is urgent and that a shorter timeframe is necessary. The EIO requires the executing authority to take this indication into account as much as possible when complying with the measure.[3]

Preservation of e-evidence under the European Investigation Order

In Article 32 of the EIO, provisional measures are foreseen, which means that "the issuing authority may issue an EIO in order to take any measure with a view to provisionally preventing the destruction, transformation, removal, transfer or disposal of an item that may be used as evidence". For this type of provisional measure, the EIO Directive already applies stricter deadlines to take the decision and communicate it to the issuing authority than for other e-evidence measures under the EIO, namely "as soon as possible and, wherever practicable, within 24 hours of receipt" (see Art. 32(2)). With Article 32, the EIO Directive has thus put in place a regime which has basically the same purpose as the proposed preservation orders in the proposed e-evidence Regulation.

[1] In comparison with point (b) this traffic (meta) data does not exist yet (it is not historical).
[2] Article 12 EIO.
[3] Article 12(2) EIO - "Where the issuing authority has indicated in the EIO that, due to procedural deadlines, the seriousness of the offence or other particularly urgent circumstances, a shorter deadline than those provided in this Article is necessary, or if the issuing authority has indicated in the EIO that the investigative measure must be carried out on a specific date, the executing authority shall take as full account as possible of this requirement."

The Budapest Convention

The Council of Europe Convention on Cybercrime (the Budapest Convention)[1], signed in 2001, is considered the first international treaty seeking to address crime committed via the Internet and other computer networks, by pursuing common criminal policy. It has been signed by all EU Member States but has not yet been ratified by Ireland and Sweden.

The Convention introduced provisions on cross-border cooperation and certain investigative techniques concerning e-evidence. The Convention as such introduces:

- (i) certain definitions relevant to the e-evidence debate,
- (ii) measures that shall be enacted at national level as regards substantive (material) criminal law, criminal procedural law and jurisdiction,
- (iii) international cooperation provisions, and
- (iv) final provisions.

As regards the e-evidence debate, the following provisions are of specific importance:

- Article 18 on production orders (especially Article 18(1)(b));
- mutual assistance as regards provisional measures (Articles 29-30);
- and mutual assistance regarding the investigative powers (Articles 31-34), especially Article 32 –"Trans-border access to stored computer data with consent or where publicly available".

Article 18(1)(b) - Production orders for subscriber data from providers operating on the territory

According to Article 18(1)(b) of the Budapest Convention, each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

This logic seems very similar to one element of the e-evidence proposal of the Commission. Yet, it should be acknowledged that the scope of Article 18(1)(b) has been subject to much debate amongst the Parties to the Convention. The domestic nature of the provision[2] has raised particular questions on the interpretation of what constitutes 'offering in the territory', especially in view of the increased use of cloud computing services where the actual location of infrastructure or data is of less relevance. This is particularly problematic since under the Budapest Convention, the authority issuing the production order must have jurisdiction over the offence

[1] Convention on Cybercrime, 2001, ETS 185. It was ratified by a big majority of Council of Europe Parties (43) and 19 non-Parties - together 62 states. Consequently, Ireland is the only EU Member State that did neither ratify the Convention nor opt-in into the EIO system. However, Ireland opted-in into the e-evidence proposal (see letter of 17 July 2018; Council doc. 11375/18). See also the 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).

[2] Article 18 falls within Section 2 of the Convention which deals with national procedural law.

The important elements that have to be clarified according to the wording of Article 18(1)(b) are:

- what is considered as subscriber data;

- when to consider that a provider offers services in the territory; and

- when the data is in "that service provider's possession or control".

The Convention defines "subscriber information" as any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic[1] or content data, and by which the following can be established:

a) the type of communication service used, the technical provisions taken thereto and the period of service;
b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

The mentioned definition of subscriber information and its explanation is not fully clear as, on one hand, it explicitly excludes "other than traffic data or content data"[2], but, on the other hand, there is no agreement among Parties to the Convention on the demarcation between subscriber information and traffic data. This blurring of lines between subscriber data and traffic data has been pointed out by the Cyber Crime Committee on the issue of dynamic v. static IP addresses, especially as regards the issue of which authority can order such measures.[3] In some Member States, subscriber data can be gathered by police or prosecutors, whilst in others, the data gathering has to be based on a court order (where there is the need to use traffic data to get subscriber data - dynamic IP addresses).[4] Moreover, some Member States treat IP addresses as

[1] See Article 1(d) of the Convention - *"'Traffic data' means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."*
[2] See also the Explanatory note to the Convention.
[3] Cybercrime Convention Committee, Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments, T-CY (2018)26, 25 October 2018: *"...a service provider may assign an IP address to multiple users in a dynamic manner, and a time stamp is needed to determine the subscriber... For this, the service provider may need to look up or analyse data of multiple users. According to the jurisprudence of some courts, this fact looking up traffic data as such may be considered an interference with the right to private life and specifically the right to secrecy of communications and not only an interference with data protection rules"* (p. 4). See also See Cybercrime Convention Committee, Rules on obtaining subscriber information, T-CY(2014)17 showing very different (constitutional) sensitivity between the States on the issue. It stated *"The question remain whether domestic regulations clearly distinguish subscriber information from traffic data, and under what circumstances."* (p. 16) See also on the different authorities to be able to request IP addresses - in some States only courts in some the police or prosecutor alone and in some States differentiation between static v. dynamic IP address (for dynamic a court order is necessary), p. 17-20.
[4] See, Cyber Crime Committee, T-CY (2018)26, Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments, p. 5-6. A majority of States that replied to the questionnaire (28 replied) need, it seems, a court order. The report states: "In 13 Parties,

subscriber data. However, some national constitutional courts and the ECtHR have stated that additional safeguards are necessary when it comes to analysing or storing traffic data in quantities that allow for profiling of individuals - which is not covered by the definition of subscriber data since this affects additional fundamental rights.[1]

In the proposed e-evidence Regulation, access data, i.e, individual IP addresses or other identifiers, is treated similarly to subscriber data, namely without a higher level of safeguards such as the requirement of a court order. Yet, if larger quantities of such identifiers might allow for profiling and are thus more sensitive in nature, they will be subject to the same safeguards as content data. According to the Commission, this approach would be in line with recent Court of Justice jurisprudence.[2]

As far as the interpretation of the notion of 'offering services in the territory' is concerned, discussions amongst Parties to the Convention resulted in a Guidance Note on the interpretation of Article 18(1)(b).[3] In the Guidance Note, Parties to the Convention agreed to a common interpretation of the notion of 'offering services in the territory' to address challenges raised by the growth of cloud computing. This interpretation is similar to the definition provided in the Commission's e-evidence proposals. However, Parties to the Convention explicitly stated that the guidance note is not binding and also acknowledged the limitations of Article 18(1)(b) to address the challenges presented by the growth of cloud computing, as they noted that '[t]he service and enforceability of domestic production orders against providers established outside the territory of a Party raises further issues which cannot be fully addressed in a Guidance Note'.

Under the Convention, Article 18 is applied under the procedures and safeguards enlisted in Articles 14 and 15.[4] Article 14 refers mostly to the possible reservations as regards the real-time collection of evidence. Article 15 requires the introduction of "conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 ECHR, the 1966 UN International Covenant on Civil and Political Rights, and other

---

an order by a judge was required either always or – in some Parties – in some cases (e.g. dynamic IP addresses, information beyond basic subscriber information, information related to a specific communication and thus representing data falling under data retention rules)." In addition, also Slovenia and Denmark have to be counted into this category ("However, in three of these (Austria, Denmark and Slovenia) this applied only to static IP addresses, and an order of a prosecutor (Austria) or judge (Denmark, Slovenia) was required for dynamic IP addresses.").

[1] See, for example, *Bundesverfassungsgericht*, 1 BVR 1299/05, whereby also the right to secrecy of communications is at stake; Canada Supreme Court - R. Spencer (2014 SCC 43); etc. See also ECtHR, *Benedik v. Slovenia - »in order to identify a subscriber to whom a particular dynamic IP address has been assigned at a particular time, the ISP must access stored data concerning particular telecommunication events«* (para. 108).

[2] The proposed Regulation introduces four categories (Article 2): (a) subscriber information and (b) access data requiring only a prosecutorial decision/validation for all offences, and (c) transactional (traffic) data and (d) content data requiring a judicial limitation and limited to certain offences.[2] Basically, subscriber data has been delimited into two categories, namely subscriber information and access data. For those two categories court authorisation is not obligatory. The category of "access data" raises some issues as stated by the Cybercrime Convention Committee. See Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments, T-CY (2018)26, 25 October 2018. It stated that. *"Introducing new categories of data, such as 'access data', may lead to further misunderstanding regarding applicable rules... of access to such data and may be difficult to apply by practitioners"*. (p. 23).

[3] See T-CY Guidance Note #10 on Production orders for subscriber information (T-CY(2015)16).

[4] Article 18(2) of the Convention.

applicable international human rights instruments, and which shall incorporate the principle of proportionality".[1] In that regard, the explanatory report clarifies that *"these domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise. The modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties."*[2] In addition to these domestic national standards (that might be also higher), certain common minimum standards have to be respected, which are also outlined in the explanatory statement.[3] It specifically highlights the importance of judicial supervision, while Article 15 underlines the need for adequate grounds for justification and limitation of the scope and duration[4], as well as consideration of the sound administration of justice as well as rights and legitimate interests of third parties.[5]

Mutual assistance regarding provisional measures (Articles 29-30)

Apart from the modalities applied for production orders on subscriber data, as outlined above, the Convention establishes preservation orders at national level (Article 17) as well as a mutual legal assistance (MLA) regime for the provisional measures (Articles 29 and 30) based on a justified request from an authority in one Party to an authority in another Party[6]. Article 29 outlines the modalities for "expeditious preservation of data stored by means of a computer system, located within the territory of another Party and in respect of which the requesting Party intends to submit a request for mutual assistance, for the search or similar access, seizure or similar securing, or disclosure of the data". Even though no specific timeframe is indicated for executing the measure, the Convention obliges the receiving Party to "take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. Although dual criminality is in principle abolished, a Party that requires dual criminality in relation to other offences than those listed in Articles 2-11 of the Convention may reserve the right to refuse the request for preservation for this type of data, if the condition of dual criminality cannot be fulfilled.[7] In addition, some specified non-recognition grounds exist, namely: (a) where the request concerns an offence, which the requested Party considers a political offence or an offence connected with a political offence, or (b) where the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.[8]

The required preservation period is at least 60 days (with the intention that an MLA request follows). Once the MLA request has been received, the data shall continue to be preserved

[1] Article 15(1) of the Convention. Proportionality is further elaborated in the Explanatory report stating that *"proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law"*, taking into account the minimum of certain common standards. And further that "the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle". Explanatory report to the Convention, Point 146.
[2] Explanatory report to the Convention, Point 145.
[3] Explanatory report to the Convention, Point 145.
[4] Article 15(2) of the Convention.
[5] Article 15(3) of the Convention.
[6] See Article 29(2) of the Convention.
[7] Article 29(3) and (4). In that regard several Parties made such a reservation (it seems 16/62), including some EU Member States.
[8] Article 29(5).

pending a decision on that request.[1] However, Article 30 foresees an expedited disclosure of preserved traffic data where, in the course of the execution of a request made pursuant to Article 29, the requested Party discovers that a service provider in another State was involved in the transmission of the communication. In that case, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. Notwithstanding this, the same two non-recognition grounds apply as mentioned above.[2] For facilitating preservation requests, Parties to the Convention have to establish 24/7 contact points.[3]

Article 32 on limited trans-border access[4]

Regarding a very limited number of cases, Article 32 of the Budapest Convention introduces the possibility of trans-border access, without the authorisation of another Party. In that case a Party may (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or (b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Point (a) covers situations such as taking data from a public website. Point (b) is more complex as the Convention does not provide clear answers regarding location (and what happens if the location cannot be clarified), when it comes to the issue of consent and who can provide it, etc.[5] The Convention only settled the commonly acceptable minimum at the time of drafting.[6] As a consequence, debates regarding trans-border access and jurisdiction have been going on for several years in the framework of the specialised subgroup of the Cybercrime Convention Committee, which has highlighted the extreme complexity of the issue[7]. In view of the

[1] Article 29(7).

[2] Article 30. See also the Explanatory Report stating: *"290. ...the requested Party may discover that the traffic data found in its territory reveals that the transmission had been routed from a service provider in a third State, or from a provider in the requesting State itself. In such cases, the requested Party must expeditiously provide to the requesting Party a sufficient amount of the traffic data to enable identification of the service provider in, and path of the communication from, the other State. If the transmission came from a third State, this information will enable the requesting Party to make a request for preservation and expedited mutual assistance to that other State in order to trace the transmission to its ultimate source"*.

[3] Article 35 of the Convention. It seems all Parties have now such points. See Cybercrime Convention Committee, Assessment report on the Implementation of the preservation provisions, T-CY(2012)10.

[4] However, also Article 26 of the Cybercrime Convention provides for the possibility of spontaneous information exchange. However, according to TC-Y reports no systematic statistical data exists in the Parties on the issue, although some indicated that it is used very often.

[5] See Cyber Crime Convention Committee, Transborder access and jurisdiction: What are the option?, T-CY(2012)3, pp. 21-23.

[6] See Explanatory Report, para. 293.

[7] See, for example Cyber Crime Convention Committee, Transborder access and jurisdiction: What are the option?, T-CY(2012)3 indicating, inter alia, the legal complexity of the issue *("The question of unilateral transborder access by law enforcement authorities of one territory to data stored on computer systems in a foreign territory without the need for mutual legal assistance is a very complex one as it touches upon agreed principles of international law (in particular the territoriality principle and thus the question of national sovereignity) and procedural law safeguards protecting the rights of the individual"*, p. 6). And further *"Transborder access could also raise legal and policy issues when a law enforcement entity gathers evidence in a manner that is unlawful in the State where the data is located... Further, extending transborder search may lend itself to misuse by States that are less committed to following the rule of law. For example, transborder access might be used in the guise of*

complexity of the matter, the Convention Committee (T-CY) also adopted a Guidance Note, which clarifies a number of issues in relation to the scope of the measure.[1] As regards the situations covered by Article 32, the Guidance Note clarifies that Article 39(3) of the Convention provides that other situations are neither authorised, nor precluded.[2] The additional protocol to the Convention which is currently underway could bring more clarity in this regard.[3]

Conclusions

- The aim of this document was to present the existing minimum of the current level of cooperation as foreseen by the EIO and the CoE Cybercrime Convention, especially as regards subscriber data, current level of trans-border possibilities (Article 18 and 32 of the Cybercrime Convention adequately applied) and existing mechanisms for preservation under the Budapest Convention and under the EIO.

- Regarding subscriber data, the data category required the most in trans-border cases, and needing swift action in order to start a criminal investigation and identify a suspect or link a suspect with a certain communication, [4] both, the EIO and the Cybercrime Convention already allow a more forthcoming framework. With subscriber data being considered the category with the lowest intrusion into fundamental rights, the EIO removes some non-recognition grounds for requests for this type of data (for example, no dual criminality and applicability to all offences). Furthermore, requests for such data have to be always possible under the system of the other Member state. The same applies to the Cybercrime Convention, whereby subscriber data can also be requested from a provider operating on its territory (but not necessarily stored there). However, due to the fact that not all Member States are part of these two instruments, that some service providers are not covered and that the deadlines might be quite long with regard to the volatile nature of e-evidence, both the EIO and the Budapest Convention also have some limitations.

- However, under the existing frameworks for cross-border cooperation, the notion of subscriber data or subscriber information has to be clear, especially as regards the subscriber data gathered by use of certain traffic data, for which some Member States will require a court authorisation while others allow police/prosecutorial to request such data.

---

legitimate law enforcement activity as a means to improperly investigate political dissidents and chill legitimate political activity" (p. 13)

[1] T-CY Guidance Note #3 on Transborder access to data (Article 32), (T-CY(2013)7 E)

[2] T-CY Guidance Note # 3, p. 22.

[3] See T-CY(2017)3, Terms of reference for the preparation of a draft 2nd additional protocol, namely a simplified regime for MLA requests for subscriber info, international production orders, direct cooperation between judicial authorities in MLA requests, joint investigation teams, requests in English, audio/video hearings, emergency MLA procedures.

[4] See Cybercrime Convention Committee, Rules on obtaining subscriber information, T-CY(2014)17, 3 December 2017 stating "*Obtaining information from Internet Service Providers to identify a user (subscriber) of a specific Internet protocol (IP) address at a specific time or, vice versa, to identify the IP addresses used by a known person is crucial for criminal investigations and proceedings related to cybercrime and electronic evidence. Subscriber information is also the most often sought data in the context of international cooperation."* (p. 4). See also a country overview in T-CY(2013)17, The mutual assistance provisions of the Budapest Convention, pp. 11-18.

- The proposed Regulation, however, introduces four categories of data in Article 2, whereby subscriber data would be split into two categories, namely “subscriber data” and “access data”, with the later only requiring a prosecutorial decision/validation, i.e. a prior court authorisation would not be obligatory.