Nathalie A. Smuha[*]

Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency

Abstract

In today's digital age, a large part of our lives has shifted from the physical to the virtual world. As this holds true for ordinary citizens and criminals alike, in the context of criminal investigations, many pieces of evidence nowadays concern electronic evidence (or e-evidence). Such evidence is often located on a server abroad. Bound to the principle of territoriality, Member States are, however, unable to access e-evidence located in another Member State without the latter's assistance. While a number of legal cooperation mechanisms between Member States exist on European level, the current framework is not adapted to the reality of the digital world and thus hampers swift criminal justice. Moreover, national legislation on access to e-evidence is highly fragmented, which generates legal uncertainty for the stakeholders involved. The European Commission aims to propose a new harmonizing Directive in early 2018, which will address these issues by enabling direct access to cross-border e-evidence. This paper argues that – while certainly facilitating the gathering of e-evidence in criminal investigations – the Commission's proposal inevitably creates its own challenges. Two of these shall be examined in particular. First, the adequate protection of fundamental rights will need to be ensured, which will involve a delicate balancing exercise between the rights to security and criminal justice on the one hand, and the rights to privacy and criminal defence on the other. Second, the new Directive will need to maintain consistency and coherency with already existing regulation which, in view of the latter's proliferation, will be no easy task.

I. Introduction

The digital realm has become one of the centrepieces of our lives. We all have computers, which we use not only for work, but also to store our private data, connect with people on social media, or look up information on the web. We all have smartphones

* Assistant Lecturer at the Institute for European Law, KU Leuven Faculty of Law (nathalie.smuha@kuleuven.be).

DOI: 10.5771/2193-5505-2018-1-83

with continuous access to the Internet, which we no longer use to simply text and call, but to access applications such as Whatsapp, Viber or Skype, enabling us to easily reach people worldwide. We exchanged letters for emails; photo albums for Instagram; binders for Dropbox.

In an ever more digitalizing world, it is therefore no wonder that much of the evidence in the context of criminal investigations is no longer physical and tangible, but in electronic format. Indeed, electronic evidence – also referred to as *e-evidence* – has become invaluable to enable criminal investigators to fight crime and bring the truth to light, whether it concerns small-scale fraud or large-scale terrorism.[1] Yet the prominence of this new form of evidence also creates challenges for law enforcers, as the available investigation tools and competences are not always adapted thereto. Moreover, the presence of e-evidence typically also creates cross-border scenarios,[2] which directly clash with the – still reigning – principle of territoriality.

The principle of territoriality, a corollary of state sovereignty, implies the mutual exclusiveness of states' jurisdiction when prosecuting criminal offences.[3] States are precluded from entering another's territory to conduct investigations or enforcement measures absent the other's consent.[4] And while some voices called to treat cyberspace as a '*Cyberspace Liberum*', analogous to the '*Mare Liberum*' as first conceived by Grotius,[5] these calls were convincingly rejected.[6] Consequently, states are also constrained from entering each other's virtual territory, and need to seek the other's legal assistance to obtain data stored on a server located abroad.

Needless to say, the territoriality principle is not adapted to today's digital world. Virtual borders, though existing in theory, do not form a physical obstacle and are

1 See S. Summers, C. Schwarzenegger, G. Ege and F. Young, *The Emergence of EU Criminal Law: Cybercrime and the Regulation of the Information Society*, Oxford: Portland, Oregon: Hart Publishing (2014), at p 233; M. A. Biasiotti, "A proposed electronic evidence exchange across the European Union", *Digital Evidence and Electronic Signature Law Review*, 14 (2017), at p 1.

2 Indeed, the relevant data or the service provider offering communication / data storage tools are often located abroad. See also M. Simonato, "Defence Rights and the use of Information Technology in Criminal Procedure", *Revue Internationale de Droit Pénal*, 2014/1, Vol. 85, at p 279.

3 See in this regard the S.S. Lotus case, Fr. v. Turk, 1927 P.C.I.J. (ser. A) No. 10, at 4 (Decision No. 9), 45 (Permanent Court of International Justice 1927).

4 See A. Osula, "Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data", 9 *Masaryk U. J.L. & Tech*. (2015), at p 45; I. Zerbes, "Legal Issues of Transnational Exchange of Electronic Evidence in Criminal Proceedings", *EuCLR*, Vol. 5(3), 2015, at p 306.

5 Implying that such space would be open to all nations and under no State's validly sovereignty. See for example D. R. Johnson & D. B. Post, "Law and Borders: The Rise of Law in Cyberspace", 48 *Stan L Rev* 1367, 1996.

6 See for instance M. Hildebrandt, "Extraterritorial Jurisdiction to enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace", *UTLJ* 63, 2013 and "The Virtuality of Territorial Borders", *Utrecht Law Review* Vol. 13, Issue 2, 2017; J. E. Cohen "Cyberspace as/and Space", 107 *Colum L Rev* 210, 2007; J. Spoenle, "Discussion paper: Cloud Computing and cybercrime investigations: Territoriality vs the power of disposal", *DG Human Rights and Legal Affairs*, Council of Europe, 31 August 2010.

crossed every day.[7] While criminals often leave useful evidence online and are able to move data from a server located in one country to another with the click of a mouse, police forces must stop their search at the virtual border and seek assistance from another state. If the aim is to attain swift criminal justice, this situation seems ridiculous at best, and dangerous for society at worst.

A number of mechanisms of judicial cooperation have been established in Europe to ensure the assistance of the state where the data is located, yet these are generally slow, costly and inefficient – designed for physical evidence, not digital – and hence unhelpful when it concerns e-evidence.[8] Moreover, several Member States recently introduced legislation which broadens their competences to access e-evidence, yet the laws' validity is challenged[9] and their divergence has led to a fragmented patchwork of inconsistent rules.[10]

Attentive to these difficulties, the European Commission intends to propose harmonizing legislation in the form of a directive in early 2018,[11] which will enable direct access to cross-border e-evidence.[12] While certainly addressing a number of the current issues, the proposal will at same time pose new challenges.

The aim of this paper is to clarify the problems raised by the current legislative framework and evaluate the solution proposed thereto by the Commission. To this end, Part II first provides an overview of the existing legal instruments on European and national level. In Part III, the instruments' problems are identified and the Commission's proposal aiming to address these problems is discussed. Part IV exposes the new challenges created by the Commission's proposal, focusing on two challenges in particular. First, the instrument's legitimacy will hinge upon the delicate balance between two values: the right to security and criminal justice on the one hand, and the right to privacy and a proper defence on the other.[13] Such balance is inherently difficult to achieve and, at this stage of the process, has yet to be struck. Second, the new direc-

7 See also A. Osula (fn. 4), at p 44.

8 See the Commission's Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace 15072/1/16 REV 1, Brussels, 7/12/2016 (hereafter 'Commission Non-Paper (2016)'), at p 3; P. Csonka, "The Council of Europe's Convention on Cyber-Crime and other European Initiatives", *Revue internationale de droit pénal 2006/3,* Vol. 77, at p477; J.I. James, P. Gladyshev, "A survey of mutual legal assistance involving digital evidence", *Digital Investigation* 18, 2016, at p24; M. Simonato (fn. 2), 279.

9 E.g. in Belgium, where the new law's validity is being challenged before the Constitutional Court (see also Part III).

10 Commission Non-Paper (2016), at p 4.

11 An impact assessment has already been made, see Legislative proposal on access to electronic evidence in criminal investigations, Ref. Ares(2017)3896097 – 03/08/2017 (hereafter 'The Impact Assessment').

12 See Commission Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, Brussels, 22 May 2017, 9554/17 (hereafter 'Commission Technical Document (2017)').

13 See also S. Manacorda (ed.) *Cibercriminality: finding a balance between freedom and security*, ISPAC, 2012.

tive will take its place amongst many already existing (and developing) pieces of legislation, and ensuring consistency therewith – so as to maintain a coherent regulatory framework for e-evidence as a whole – shall be no easy task.[14] Finally, Part V offers some concluding remarks.[15]

II. Access to cross-border e-evidence in criminal investigations: current framework

1. Council of Europe – Mutual Legal Assistance

When the European Union was in its infancy and EU competences in the criminal sphere still unimaginable, the first international framework for mutual legal assistance ("MLA") in criminal matters was born under the auspices of the Council of Europe. Members of the Council understood that cooperation would advance their criminal justice systems, yet – prudent to relinquish national competence in this area – preferred to use an international law tool to achieve this end.[16] Hence, in 1959, the European Convention on Mutual Assistance in Criminal Matters was established, setting up a system of state collaboration.[17] Convention signatories are committed to provide each other assistance to obtain evidence located in one country to further proceedings in another.[18]

A second and – for the purpose of this paper – more important Convention born within the Council of Europe framework concerns the Convention on Cybercrime.[19] The latter aims not only to ensure that its signatories adopt adequate criminal laws to combat cybercrime, but also that they afford one another mutual assistance in investigations or proceedings of criminal offences related to computer systems and data, and particularly in the collection of e-evidence.[20] However, as concerns the concrete mechanism of such cooperation, the Cybercrime Convention refers back to the general sys-

14 See Commission Technical Document (2017), at p 30 and following.

15 Some of the issues raised by the current framework also regard extra-EU concerns, namely cooperation with service providers located outside the EU, and the access to data located on servers outside the Union's borders. While the Commission has also put forward some measures to mitigate these concerns, this paper's focus lays on the improvement of cooperation within the EU, and shall not deal with extra-EU matters.

16 S. Summers et al (fn. 1), at p 237.

17 European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 20 April 1959, ETS – No. 30.

18 See also the Explanatory Report to the Convention, Strasbourg, 20 April 1959, ETS – No. 30. The Convention inter alia sets out rules to enforce letters rogatory aimed to procure evidence (audition of witnesses, experts and prosecuted persons, service of writs and records of judicial verdicts) or to communicate evidence (records or documents) in criminal proceedings undertaken by the judicial authority of a convention party.

19 Also referred to as the Budapest Convention after its birthplace. See Convention on Cybercrime, ETS No.185, Budapest, entry into force: 01/07/2004 (hereafter the "Cybercrime Convention").

20 See also P. De Hert et al, "Fighting cybercrime in the two Europes. The added value of the EU framework decision and the council of Europe Convention", *Revue internationale de droit pénal* 2006/3, Vol. 77, at p 504.

tem, stating that mutual assistance shall be subject to the conditions provided for "*by the law of the requested Party or by applicable mutual assistance treaties*".[21]

When computer data relevant to a criminal offence is located abroad, a Convention party may request another party for assistance with investigative competences, such as the search, access, seizure, preservation and/or disclosure of data located within the other party's territory.[22] Furthermore, if there are grounds to believe that the relevant data are particularly vulnerable to loss or modification, or if international legal instruments provide for expedited co-operation, a MLA request must be responded to on an expedited basis. The Convention's text, however, leaves open the precise 'expeditiousness' of such expedited basis.[23]

Crucially, the envisaged system of cooperation does not foresee a free pass for a State to bypass the MLA mechanism and directly access e-evidence located in another State without the latter's consent.[24] Pursuant to Article 32 of the Cybercrime Convention, this is only different when (a) the evidence concerns publicly accessible data (i.e. open source), or when (b) the person with the authority to disclose the data voluntarily provides the requesting state with access thereto through a computer system located in that state's territory.[25] Accordingly, unless the data are publicly available or the data holder voluntarily hands them over, states are not allowed – without prior approval or assistance – to access e-evidence located outside their territory.[26]

Since the adoption of these Conventions, the European Union has slowly but surely acquired competences in the area of police and judicial cooperation in criminal matters. Consequently, and as shall be addressed below, within the EU other legal instruments have become increasingly important. Nevertheless, for all matters where the Union has not yet exerted its competence, Member States still operate under the Council of Europe's conventions.

21 See Article 25 of the Cybercrime Convention.

22 See Article 31. This also includes data which was already provisionally preserved pursuant to Article 29.

23 See Article 31 (2) of the Cybercrime Convention.

24 Note however that the Council of Europe is currently undertaking a review of the Cybercrime Convention, planning a revisit in 2019. See the Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, approved by the 17th Plenary of the T-CY on 8 June 2017. In particular, the revision aims to provide more effective mutual assistance, and shall likely contain provisions allowing for direct cooperation with service providers abroad with regard to requests for subscriber information, preservation requests, and emergency requests. This would bring the Convention closer to the Commission's new proposal.

25 See Article 32 of the Cybercrime Convention. See also J. Spoenle (fn. 6), at p 7; S. Mason, E. George, "Digital evidence and 'cloud' computing", *Computer law & Security review* 27, 2011, at p 528; I. Zerbes (fn. 4), at p 307.

26 At the time the Convention was negotiated, while recognizing Article 32's limitations and the need for a solution, the negotiating states were unable to reach an agreement on cross-border access. See M. Simonato (fn. 2), at p 284.

2. European Union – Mutual recognition

a) Constitutional Framework

Cooperation in criminal matters only developed into a true EU competence over the last years.[27] Under the Maastricht Treaty[28], issues dealing with *Justice and Home Affairs* were confined to the so-called third pillar, where decision-making was primarily intergovernmental.[29] Member States were not only reluctant to surrender criminal competences to a supranational level, but the differences in their political approaches thereto – touching upon highly sensitive fundamental rights issues – made supranational control undesired.[30] At the same time, it was acknowledged that cooperation in criminal matters, especially in view of their increasing cross-border nature, was indispensable and that mere international tools didn't do.[31] The *communitarisation*[32] of the competence for *Justice and Home Affairs* was initiated by the Amsterdam Treaty[33] and finalised under the Lisbon Treaty[34], which renamed it the *Area of Freedom, Security and Justice*.[35]

Initially, the Member States decided to build further on the MLA mechanism of the Council of Europe and signed their own EU Convention on Mutual Assistance in Criminal Matters"[36] aiming to supplement the former. In a next step, MLA mechan-

27 See V. Mitsilegas, *EU Criminal Law after Lisbon: Rights, Trust and the Transformation of Justice in Europe*, Oxford: Hart Publishing, 2016, at p 4. Note that competence on the Area of Freedom, Security and Justice is shared between the Union and Member States (see also Article 76 TFEU).

28 Signed on 7/02/1992 as Treaty on European Union (TEU) (OJ C 191, 29.7.1992), entered into force on 1/11/1993.

29 Legislative competence over criminal matters – to the extent not contested – was subject to Council unanimity.

30 Jurisdiction of the Union Courts over matters belonging to the third pillar was limited; for instance, preliminary rulings could only be granted to Member States that made a declaration accepting such jurisdiction, and the Commission had no competence to bring an enforcement action before the Courts if a Member State breached EU law in this field.

31 In particular, the increasing emergence of terrorist attacks on European territory emphasised the need for a more coordinated approach in criminal matters. See also J. S. Hodgson, "Safeguarding Suspects' Rights in Europe: A Comparative Perspective", 14 *New Crim. L. Rev*., 2011, at p 615.

32 I.e., the process of bringing this competence under the community pillar.

33 Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, OJ C 340, 10.11.1997, at p 115..

34 And only after a transitional period of 5 years after its entry into force, see Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, 17.12.2007, p. 1–271. See in particular Title VII, Article 10.

35 See Title V of the TFEU. See also S. Summers et al (fn. 1), at p 5; J. Öberg, "Subsidiarity and EU Procedural Criminal Law", *EuCLR* Vol. 5, 1/2015, at p 21; V. Mitsilegas (fn. 27), at p 7.

36 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000. As shall be explained below, this Convention is now largely replaced by Directive 2014/41/EU.

isms in the EU progressively made room for mutual recognition instruments.[37] The difference between the two methods of cooperation seems subtle, but the consequences are rather significant. While the system of mutual legal assistance is relatively flexible and provides the state receiving a request for assistance with a broad discretion as to whether or not the request is dealt with, the system of mutual recognition aims to obliterate such discretion. [38] Based on the principle of mutual trust, the mutual recognition system allows Member States' criminal laws to diverge, but they must trust in the validity of each other's procedures. Member States are hence expected to duly recognise decisions taken by another State's authority and enable the swift execution thereof.[39]

Article 82 of the Treaty of the Functioning of the European Union (TFEU) now states that judicial cooperation in criminal matters "*shall be based on the principle of mutual recognition of judgments and judicial decisions*", indicating that the era of cooperation based on mutual legal assistance in the Union is coming to an end. Moreover, judicial cooperation shall also "*include the approximation of the laws and regulations of the Member States in the areas referred to in Article 82(2)*".[40] While the Union's toolbox thus consists first and foremost of the principle of mutual recognition[41] – with analogy to the principle's use in the context of the internal market[42] – it also, and only for those elements specifically delineated, entails the possibility to harmonise Member State legislation.[43]Article 82(2) provides that such harmonization, through the establishment of minimum rules, can occur for the purpose of facilitating (a) mutual recognition of judgments and judicial decisions and (b) police and judicial cooperation in criminal matters having a cross-border dimension. These minimum rules can concern the mutual admissibility of evidence between Member States; the rights of individuals in criminal procedure; the rights of victims of crime; and – a bit of

37 A well-known illustration of the mutual recognition mechanism at work is the European Arrest Warrant (Council Framework Decision of 13 June 2002, OJ L 190, 18.7.2002).

38 See S. Lavenex, "Mutual recognition and the monopoly of force: limits of the single market analogy", *Journal of European Public Policy*, 14:5, 2007, 762-779; C. Heard, D. Mansell, "The European Investigation Order: Changing the Face of Evidence-Gathering in EU Cross-Border Cases", 2 *New J. Eur. Crim.* L. 4, 2011, 353-367; O. Löfgren, "A Manifesto for European Criminal Procedure Law – A Prosecutorial Perspective", *EuCLR*, Vol.5 (1), 2015, 54-59.

39 In order to ensure the process' efficacy, grounds for refusal (and hence discretion) are severally limited and time limits to respond to and execute the requests have been implemented.

40 This article also refers to Article 83 TFEU, less of relevance for this paper; it focuses on substantive law and allows the establishment of minimum rules concerning the definition of criminal offences and sanctions for particularly serious crimes with cross-border dimensions (e.g. terrorism or human trafficking).

41 See S. Summers et al (fn. 1), at p 79; W. Van Ballegooij and P. Bárd, "Subsidiarity and EU Procedural Criminal Law", *EuCLR* Vol. 5, 1/2015, at p 440.

42 In this respect, see S. Lavenex (fn. 38); A. Sulima, "The Normativity of the Principle of Mutual Trust between EU Member States within the emerging European Criminal Area", *Wroclaw Review of Law, Administration & Economics*, Vol 3:1, 2013, at p 74.

43 See also S. Summers et al (fn. 1), at p 259.

a catch-all – any other specific aspects of criminal procedure which the Council has identified in advance by a decision.[44]

The most relevant EU judicial cooperation mechanism spirited by the principle of mutual recognition for the purpose of this paper is the European Investigation Order ("EIO")[45]. Having largely replaced the EU Convention on Mutual Assistance – at least as concerns the Member States participating thereto – the EIO today sets the tone for the access to and exchange of cross-border e-evidence in criminal investigations, and thus merits a more detailed examination.

b) The European Investigation Order

The European Investigation Order was introduced by Directive 2014/41/EU ("the EIO Directive") and implemented into national legislation in May 2017.[46] Based on the principle of mutual recognition, it establishes a comprehensive mechanism to obtain cross-border evidence.[47] Pursuant to paragraph 35 of the EIO Directive, which refers to the existing MLA regime, between Member States bound by the Directive the latter takes precedence.

44 See Article 82(2) TFEU. Importantly, such minimum rules are adopted by the ordinary legislative procedure, yet considering the sensitiveness of this area, the Treaty foresees a number of additional protection mechanisms for Member States. First, it is clarified that minimum rules shall take into account "*the differences between the legal traditions and systems of the Member States*". Second, the adoption of minimum rules shall not prevent Member States from maintaining or introducing a higher level of protection should they wish to do so. Third, if a member of the Council considers that a draft directive proposed under Article 82(2) affects fundamental aspects of its criminal justice system, it may request referral of the draft to the European Council, and hence generate a suspension of the legislative procedure until a consensus is reached. Furthermore, three Member States have chosen for an opt-out from all legislation adopted in the Area of Freedom, Security and Justice. While Ireland and the UK have opted for a flexible opt-out, allowing them to opt-in or out of such legislation on a case-by-case basis, Denmark has opted for a rigid opt-out, whereby participation in these policies standardly occurs on a more intergovernmental basis. See Protocols 21 and 22 to the TFEU. See also S. Summers et al (fn. 1), at p 52; V. Mitsilegas (fn. 27), at pp 15 & 44.

45 Introduced by Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014 (hereafter 'the EIO Directive').

46 The EIO Directive harmonises and replaces the previous frameworks of the European Evidence Warrant and the European Freezing Order, both of which existed in parallel with the traditional cooperation instrument of MLA and which – unaided by their inefficient procedures – were barely used. Note that in February 2018, i.e. almost a year past the deadline, a number of Member States are still in the process of implementing the new Directive.

47 See C. Heard, D. Mansell (fn. 38); R. Belfiore, "The European Investigation Order in Criminal Matters: Developments in Evidence-gathering across the EU", *EuCLR* Vol.5(3), 2015, 312-324; R. Jurka, "Movement of evidence in the European Union: Challenges for the European Investigation Order", *Baltic Journal of Law & Politics* 9:2, 2016, 56–84.

The EIO ensures a great deal of things. It creates a single instrument with a large scope, covering the entire process of evidence collection, freezing and transfer[48]; it sets strict deadlines for the gathering of requested evidence[49]; it limits the reasons which Member States can invoke to refuse a request[50]; it introduces a standard form to request assistance, hence reducing paperwork[51]; it ensures that any EIO must be validated by a judicial authority[52] and it imposes the adoption of legal remedies to ensure a right to legal recourse.[53] What it, however, does not ensure is a framework to deal with the specificities of electronic evidence. This is to be regretted.

The question of how to handle e-evidence – increasingly raising important issues – would have been ideally addressed in this new instrument. Additional rules were, for instance, also foreseen for specific types of investigative measures, such as the interception of telecommunications or the access to information related to bank accounts or banking transactions.[54] Yet the EIO Directive contains no guidance for the difficulties evoked by e-evidence, despite the pre-eminently cross-border character thereof.

Most akin to accessing e-evidence is the measure governing the interception of telecommunications, dealt with under Article 30 of the EIO Directive. This provision covers the interception of both the content of communications and the related metadata. However, this Article operates under the assumption that assistance of another State – namely the State in which the investigated subject finds itself – is still required to execute the measure. The generally applicable lengthy timeframe of 30 days for the State receiving the EIO to decide on its execution, and the timeframe of 90 days for this State to execute the EIO, remains in place.[55] Moreover, given the invasiveness of the measure, an additional ground for non-execution is foreseen. Article 30(5) provides that, besides the refusal grounds listed in Article 11, execution of a EIO requesting the interception of telecommunications can also be refused where the measure would not have been authorised in a similar domestic case.

The scenario under which the assistance of another State is technically not necessary to execute the measure is dealt with under Article 31. When a Member State authorises the interception of telecommunications, and the communication address of the subject

48 See also L. Bachmaier Winter, "Cross-border Investigation of Tax Offences in the EU: Scope of Application and Grounds for Refusal of the European Investigation Order", *EuCLR* Vol. 7, 1/2017, at p 50.

49 See also § 21 of the Directive's Preamble.

50 The grounds for refusal to execute or recognise a EIO are listed in Article 11 of the Directive.

51 Annex A of the Directive contains a standard form for Member States to use when issuing an EIO.

52 See also Article 1(1) of the Directive, defining the EIO as "*a judicial decision which has been issued or validated by a judicial authority of a Member State ('the issuing State') to have one or several specific investigative measure(s) carried out in another Member State ('the executing State') to obtain evidence in accordance with this Directive*.".

53 See Article 14 of the Directive.

54 See Chapter IV of the Directive setting out these rules, as well as § 24 of the Preamble explaining their rationale.

55 See Article 12 of the EIO Directive.

is used on another Member State's territory, the latter – from which no assistance is needed to carry out the interception – must first be notified. Notification must occur prior to the interception when the competent authority knows, at the time of ordering the interception, that the subject is or will be on another's territory. It can only occur during or immediately after the interception if the authority becomes aware at a later stage that the subject is or was on the other's territory.[56]

Notification is crucial, as this enables the other Member State to conduct a (marginal) check on the measure's validity and to take action if the interception would not have been authorised in a similar domestic case. Within 96 hours after the notification's receipt, the notified Member State can claim that (i) the interception may not be carried out or shall be terminated and (ii) that any material already intercepted while the investigated subject was on its territory may not be used, or may only be used under specified conditions.[57] Whether and when the subject of the interception is notified – in turn crucial for the latter to exercise its procedural rights – is not governed by the EIO Directive but remains a matter of national law.[58] Note that the above mechanism – which in theory allows for cross-border access to data by mere notification – only applies to the interception of telecommunications (in principle also including data communicated through online services like Skype or Whatsapp[59]), and excludes access to stored evidence (such as data saved through services like Dropbox).[60] For the latter type of data, States must issue a prior EIO, to which the abovementioned time limits apply.[61]

Accordingly, though the EIO procedure certainly has merit in facilitating the exchange of evidence and the carrying out of investigative measures in cross-border situations, it does not provide a comprehensive framework for the collection of e-evidence, and – as shall be discussed further below – is far from adapted to the fast pace of the digital world.

56 See Article 31(1)(b) of the EIO Directive.
57 See Article 31(3) of the EIO Directive.
58 See I. Zerbes (fn. 4), at p 306. Note that, pursuant to Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities in criminal matters (to be implemented in Member State legislation by May 2018), individuals whose data are being processed by such authorities (referred to as data subjects) have the right (subject to certain exceptions) to be informed thereof. See also further under Part IV.
59 The fact that the term "communications" also encompasses online channels of communications is also apparent from the Explanatory Report on the EU MLA Convention under Art. 18.
60 Pursuant to § 30 of the Directive's preamble, 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.
61 An expedited procedure is foreseen in Article 32, applying only to the provisional prevention of destruction, transformation, removal, transfer or disposal of an item that may be used as evidence. The executing authority must decide on such measure as soon as possible and – "wherever practicable" – within 24 hours of the EIO's receipt.

3. National level – a fragmented patch-work of regulation

While EU Member States which are signatories to the Council of Europe conventions are bound thereto, and while they were obliged to implement the EIO Directive into national law by 22 May 2017, the role of domestic legislation is far from over. A large number of criminal procedural matters are not yet dealt with by international and supranational instruments, leaving ample scope for (divergent) national approaches.[62] Indeed, while some Member States introduced new legislation specifically addressing the handling of e-evidence by their authorities, others (not always without a struggle) continue to apply their traditional frameworks, reinterpreting provisions where necessary rather than amending them.[63]

Moreover, amongst those Member States who adopted new rules for e-searches and e-evidence, the manner in which the pertinent issues are dealt with greatly differs. This is evident when examining the variety of definitions of 'electronic data' provided in the various national laws, to the extent provisions dealing therewith are foreseen.[64] Member States also employ different connecting factors for the exercise of investigatory measures allowing access to e-evidence, in particular to establish whether a service provider is foreign or domestic (and hence whether jurisdiction can be exercised thereon).[65] Based on the Commission's findings[66], 16 Member States utilise the concept of the 'main seat of the service provider', 6 Member States use 'the place where services are offered', and 6 use 'the place where data is stored'.[67]

Additionally, the scope of competences attributed to the Member States' authorities significantly differs.[68] For example, following the principle of territoriality, the German code of criminal procedure (in principle)[69] only allows the authority to expand a

62 See also S. Summers et al (fn. 1), at p 82; V. Mitsilegas (fn. 27), at p 14.

63 G. Di Paolo, "Judicial Investigations and Gathering of Evidence in a Digital Online Context", *International Review of Penal Law*, 2009, vol. 80, at p 202. See also M. Simonato (fn. 2), at p 268.

64 See Deliverable "*D3.1 Overview of existing legal framework in the EU Member States*", in the context of the EVIDENCE Project (European Informatics Data Exchange Framework for Courts and Evidence), Ref nr FP7- SEC-2013.1.4-2, 30 October 2015, at p 64. See also Commission Technical Document (2017), at pp 6 and 18.

65 At times, the connecting factor may even depend on the type of data concerned. See Commission Technical Document (2017) at p 5.

66 See the Commission's Non-paper (2016).

67 Some domestic laws provide a combination of connecting factors. Other factors could also be considered, such as the nationality of the suspect or of the victim to which the e-evidence pertains.

68 See also V. Mitsilegas (fn. 27), at p 99.

69 See Article 110(3) of the German Code of Criminal Procedure (StPO). Admittedly, since this provision does not explicitly limit the authority's competence to search data to Germany alone, a debate is still ongoing amongst German scholars and practitioners on the extent to which the authority could potentially also access data stored on a server abroad. However, the fact that the provision applies only to data stored domestically, and that any virtual cross-border access would thus infringe not only the German Code but also the Cybercrime Convention to which German is a party, was recently confirmed in a judgment of the Mu-

search from data stored on a computer to data accessible through that computer if such data is located in Germany. In contrast, Belgium's code of criminal procedure allows the authority to access and copy e-evidence even when located abroad, though foreseeing the requirement of notification.[70] Moreover, while in some states law enforcers are competent to use investigative techniques to access e-evidence also when the location is unclear or impossible to establish, other states' laws either do not foresee such possibility or specifically preclude it.[71]

More importantly, the level of protection afforded in terms of due process and rights of defence are not always the same.[72] In particular, the question of whether in each instance a judicial decision is necessary to access e-evidence – hence ensuring review by an impartial authority before the invasive measure occurs – or whether the public prosecutor (or even police force) can decide on such access by itself, is dealt with differently.[73] As this issue touches the core of fundamental rights, many of the newly-introduced laws dealing with access to e-evidence have been heavily criticised in view of their (at times poor) level of procedural protection.[74] Indeed, while on the one hand expanding prosecutors' toolboxes to investigate crimes by facilitating access to e-evidence, the complementary expansion of procedural guarantees on the other hand – which may arguably be even more at stake when searching a person's computer than a person's house – is not always ensured.

In light of the above, it can be concluded that the framework to access cross-border e-evidence on Member State level consists of a fragmented patchwork of rules. While the principle of mutual recognition ensures that divergent national approaches can co-

nich Court (see judgment of 13 June 2017, case number 6 Qs *9/17 – 6 Qs 14/17,* First Munich Regional Court, Criminal Division). See also further under Part III.1.a of this paper.

70 See Article 39bis(3) of the Belgian Code of Criminal Procedure (Sv).

71 See Commission Non-Paper (2016), at p 6.

72 See also J. S. Hodgson (fn. 31), at p 618.

73 See Commission Non-Paper (2016), at p 6; M. Simonato (fn. 2), at p 282; M. T. Schunke, "The Manifesto on European Criminal Procedure Law; a commentary on the perspective of mutual recognition and violations of defence rights", 5 *EuCLR*, 2015, at p 51.

74 In this regard, the new provisions of the Belgian code of criminal procedure which entered into force in January 2017 can offer an example. While previously, invasive investigation measures such as the search of an IT system required intervention by an independent judge (*juge d'instruction*), today in a number of scenarios authorization from the public prosecutor – and at times even a decision from the police forces – suffices. See e.g. Article 2 § 3 of the new law of 25 December 2016 amending the Belgian Criminal Procedure Code. Hence, what was announced as a procedural milestone in the fight against crime in the digital age, is deemed by many to be a blatant infringement of due process. The Belgian Human Rights League decided to challenge the law's legality before the Constitutional Court, and the case is currently pending (roll number 6711). Criticism on new legislation dealing with e-evidence is not confined to Belgium; in the Netherlands, the adoption of new provisions governing the collection of e-evidence in July 2017, potentially granting even more far-reaching competences to the authority than the Belgian law, has likewise been the object of heavy protests. Similarly, the French Intelligence Act of 24 July 2015 has been challenged before the French courts in view of its strong impact on the fundamental right to privacy. In contrast, a number of Member States still did not adopt any specific laws dealing with the gathering of e-evidence.

exist, this does not facilitate interaction between the different stakeholders and in fact creates difficulties in cross-border cooperation. Those difficulties are addressed more in details in the following Part.

III. Problems with the current framework & the Commission's proposal

1. The current framework – inadequate, inefficient and cultivating legal uncertainty

In Part II above, the legal procedures available to Member States to access cross-border e-evidence have been discussed. A brief re-visitation of those procedures allows to identify a number of problems with the current framework, which necessarily have to be dealt with if the aim is to improve criminal justice. These problems can be narrowed down to two main critiques: (a) the available legal tools to access cross-border e-evidence are inefficient and inadequate for the digital age and (b) the fragmentation of Member State legislation generates inconsistency and hampers legal certainty. Both issues shall be examined below.

a) The legal framework to access cross-border e-evidence is inadequate & inefficient

As was already hinted at above, the procedures currently in place to access cross-border e-evidence are inadequate for the reality of the digital age.[75] Whether it concerns the issuing of a European Investigation Order or the more traditional Mutual Legal Assistance request, these mechanisms are too slow and cumbersome to deal with evidence that can be moved or erased with the click of a mouse. Much has been written on the inadequacy of MLA in the context of e-evidence.[76] While less has been written on the inadequacy of the brand new EIO, its provisions do not offer much more comfort for authorities aiming to gain rapid access to cross-border data.[77]
This was recently illustrated in a German case which concerned a criminal investigation against a car manufacturer.[78] In the context of the investigation, the German authority obtained a warrant to conduct an unannounced search with a third party, namely the car manufacturer's law firm, hoping to find evidence to build its case.

75 See also J. Spoenle (fn. 6), at p 12.
76 See for example P. Csonka (fn. 8); C. Leacock, "Search and Seizure of Digital Evidence in Criminal Proceedings", *Digital Evidence and Electronic Signature Law Review*, Vol 5, 2008; S. Mason & E. George (fn. 25); M. Simonato (fn. 2); J.I. James, P. Gladyshev (fn. 8); M. A. Biasiotti, (fn. 1).
77 See in this regard also the Commission Non Paper (2016), at p 12: "*Although the use of the EIO will considerably improve the formal cooperation between the relevant authorities of Member States for obtaining cross-border access to electronic evidence, it has not been developed specifically with the objective to improve cross- border access to electronic evidence. Compared to direct cooperation with service providers, requests on the basis of mutual recognition are expected to be slower, more cumbersome and resource-intensive.*".
78 See Ruling by the 6th Criminal Chamber of the 1st Munich Regional Court on June 7, 2017, 6 Qs *9/17 – 6 Qs 14/17.*

Leaving aside whether the search was legal and whether legal privilege was respected, the case exemplifies the problems with the current framework; while the law firm's office was in Munich, its server – and thus its data – was in Brussels. The German authority was, however, perfectly able to access the data from the computer in Munich. It hence decided to copy the data – for which it first briefly accessed the Belgian server – notwithstanding the heavy protests from the law firm.

Neither a EIO nor a request for MLA had been issued to Belgium prior to the search. In fact, it is not clear whether the authority was aware of the server's location beforehand. Nevertheless, by accessing from Germany data on the Belgian server, the German authority illegally exerted its enforcement jurisdiction outside its territory. This was confirmed by the Munich Court where an appeal was filed against the search. Referring to the Cybercrime Convention, the Judge found that absent the data's public availability or the subject's consent, and absent a request for Belgium's assistance, the authority had breached the law.[79]

This case did not concern the search of a criminal suspect, nor did it contain any particular urgency (in fact, the legality of the search is seriously questioned[80]). However, placing oneself in a different scenario – whereby the data to be searched may contain crucial information to halt a possibly imminent terrorist attack – instantly points to the situation's absurdity. Under the current regulatory framework, the authority is required to go through a lengthy procedure to obtain a result which it could instead achieve instantly, and this solely because the server – and not the subject of the search, nor the object of the crime – is located abroad. Moreover, the fact that such State may have no connection whatsoever with the case other than the server's location (as was the case for Belgium in the car manufacturer case), does not alter this murky situation.[81]

Evidently, such course of business is certainly not conducive to the swift attainment of criminal justice. Furthermore, especially in the digital context, the existing procedures are time-consuming, complex (despite the simplification brought by the EIO), resource-intensive and little transparent. In sum, the tools available to Member States are not adapted to reality, despite the fact that e-evidence is becoming the most important type of evidence in criminal matters.[82]

79 *Ibid*.

80 The car manufacturer and the law firm in question appealed against the German authority's seizure and submitted a constitutional complaint with the German Constitutional Court, including a request for interim measures barring the authority from using the seized data. The latter ruled on 25 July 2017 that the interim measure should be granted (see http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2017/bvg17-062.html, 2 BvR 1287/17, 2 BvR 1583/17, 2 BvR 1405/17, 2 BvR 1562/17).

81 See C. Conings, "De lokalisatie van opsporing in een virtuele omgeving – wie zoekt waar in cyberspace?", 9 *Nullum crimen* 1, 2014, at p 15.

82 See also C. Leacock (fn. 76), at p 221.

b) The fragmentation of national laws cultivates legal uncertainty & forum shopping

The abovementioned fragmentation of Member State laws regulating access to cross-border e-evidence is causing particular difficulties and uncertainty amongst electronic service providers. These often offer their services in multiple EU Member States and thus need to comply with various – and at times conflicting – national obligations. While a number of laws ensure that such service providers cannot share private user information with third parties[83], including with foreign governments (this appears to be the situation in most national regulations)[84], several laws explicitly obligate service providers to provide the requested information and even foresee a penalty for non-cooperation.[85] This leads not only to inconsistency – which is costly, particularly for service providers operating in multiple countries – but also to legal uncertainty, which is costly for society as a whole, especially if it diminishes criminal justice.

The case of *Belgium v Skype*[86] is very telling in this respect. In 2012, a Belgian judge discovered that two important suspects communicated with each other through Skype rather than using traditional communication channels. The judge requested Skype to assist in the interception of the suspects' communication, but Skype refused on the basis that the company is Luxembourg-based and that all users' data is saved in Luxembourg, hence precluding Belgium's jurisdiction.[87] Several subsequent requests did not alter Skype's view, and eventually Skype was convicted to a €30.000 fine for refusing to cooperate in the investigation.[88] Since Skype provides its communication services on the Belgian market and targets Belgian customers, the judge held that Skype should also ensure conformity with the Belgian criminal code. Skype's argument that Belgium should have submitted a request for MLA to Luxembourg was not accepted.[89]

83 This includes provisions under EU law, such as the GDPR (Reg. 2016/679) discussed further below.

84 According to the Commission's December 2016 Non-Paper, the majority of national legislations either do not cover or explicitly prohibit that service providers respond to direct requests from law enforcement authorities from another EU Member State or third country.

85 For example, under the revised Article 46bis of the Belgian criminal procedure code, all providers of an electronic communication network and all companies which – on Belgian territory and in whichever manner – make available or offer a service consisting of the transmission of signals through electronic communication networks or which allow users to obtain, receive or spread information through such network, have the obligation to cooperate. Penalties are not limited to fines but also encompass prison sentences.

86 See Judgment of Corr. Antwerpen (afd. Mechelen), 27 October 2016, *NjW* 2016, afl. 353, at p 921.

87 See also J. Flo, "Skype moet onderzoekers toegang geven tot communicatie verdachte", *Juristenkrant* 337, 9 November 2016, at p 4.

88 Skype has appealed this judgment, which was confirmed by the Antwerp Court of Appeal on 15 November 2017 (case 2016/CO/1006).

89 Indeed, Skype claimed that "*it does not possess or manage any infrastructure in Belgium*", arguing that its so called crime of non-cooperation could thus only have taken place in Luxembourg, hence barring Belgium's jurisdiction. This did not convince the Belgian Court of Appeal, who stated that "*the crime [of dereliction of duty] was committed on the place where the asked information should be received, not where the legal entity in question is located. Ac-*

Belgium's stance towards Skype stands in contrast with the approach taken by some other states using different connecting factors to subject foreign-based companies to their jurisdiction, and/or who foresee that direct cooperation between foreign authorities and service providers only occurs voluntarily. In that case, if a state wishes to obtain data from a foreign service provider on a mandatory basis, a request for MLA or the issuing of a EIO is required.[90]

According to the Commission's Non-Paper of December 2016, currently 14 Member States consider that service providers receiving a direct request from another state's authority can comply therewith voluntarily, whereas 7 Member States consider these requests to be mandatory.[91] Yet even when the cooperation mechanism is mandatory, it remains an open question whether Member States can legally enforce such requests.[92] Besides cultivating legal uncertainty amongst various stakeholders such as service providers and customers (i.e. European consumers), this situation also seriously hampers the efficacy of cross-border investigations.

The disparity of legislation entails another negative externality. When filing a criminal complaint against another entity, for example a multinational company, any clever legal advisor would try to find a way to bring such claim in a country where the authorities' competences are broad and the protection of the rights of defence less stringent. Based on the above, one would certainly be more willing to file a complaint in Belgium than in Germany, especially if it were known that some important evidence is digital, so as to avoid the unavailability thereof merely because it is located abroad. Yet such forum shopping is not to be applauded, especially in an area such as criminal law which touches upon the public order.[93]

It is thus no surprise that a uniform approach at EU level – and, ideally even on worldwide level[94] – is warranted in order to improve access to cross-border e-evidence in criminal matters. This need was picked up by the Council of the European Union who in June 2016 published its conclusions on improving criminal justice in cy-

cordingly, the duty to cooperate can be localised in Belgium, also for a legal entity established abroad which bears such duty. Dereliction of this duty is a Belgian territorial crime which can be committed by Belgians and foreigners alike." Notably, in a landmark judgment against Yahoo pronounced on 1 December 2015 (Nr. P.13.2082.N), the Belgian Supreme Court (Court de Cassation) already dismissed a similar argument, finding that an electronic communication provider (*in casu* Yahoo) actively participating to the Belgian economy and exercising its economic activities in Belgium targeting Belgian consumers, is subject to the Belgian criminal code. See in this regard also P. de Hert, M. Kopcheva, "International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! case", *Computer law & Security review* 27, 2011, at p 291.

90 Such as is for example the case in Germany pursuant to Article 110(3) of the StPO – see also supra.

91 Commission Non Paper (2016), at p 4.

92 *Ibid*.

93 See also S. Summers et al (fn. 1), at p 240; J. Ouwerkerk, "The Potential of Mutual Recognition as a Limit to the Exercise of EU Criminalisation Powers", *EuCLR* Vol. 7, 1/2017, at p 7.

94 Not only the European Union is planning to revisit the toolbox for the collection of e-evidence. As mentioned supra (fn. 24), the Council of Europe is currently undertaking a review of the Cybercrime Convention.

berspace.[95] The Council on the same occasion requested the Commission to prepare legislative action to accommodate the mentioned concerns. In what follows, the Commission's proposal for dealing with the above issues – and the new challenges generated thereby – are examined.

2. Commission's proposal for improvement – enabling direct access

Pursuant to the Council's call for concrete action based on a common EU approach, the Commission committed itself to report on intermediate results by December 2016 and to present deliverables by June 2017. An expert consultation process was launched which explored possible solutions, involving stakeholders from the private sector, practitioners from the Member States, and civil society organizations. A first Non-Paper was submitted to the Council in December 2016[96], followed in June 2017 by a second Non-Paper on the results of the expert consultation process[97] and a Technical Document containing the preliminary views of the Commission services.[98] It is in the latter document that the Commission set out a number of practical and legislative measures to be potentially adopted in order to tackle the issues set out previously.

The proposed practical measures constitute but a first step to buy some time, best compared to a tiny band-aid strapped to a gaping wound, not reaching the core of the issue and thus not discussed in what follows.[99] As to the proposed legislative measures[100], these are more far-reaching and aim to harmonise legislation on cross-border e-evidence by means of a directive enabling authorities' direct access to service providers and/or to e-evidence, even if located in another EU Member State. Three measures in particular are advanced.

First, the Commission suggests harmonizing the definitions of e-evidence, allowing for a better harmonization of the scope of the investigation measures available to obtain cross-border e-evidence.[101] A harmonization of the relevant definitions would also enhance legal certainty for the stakeholders addressed by the measures, including not

95 See at: http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/.
96 Commission Non-Paper (2016).
97 Non-paper from the Commission services, Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward, presented at the 8 June 2017 JHA Council meeting, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf.
98 Commission Technical Document (2017).
99 See pages 14 to 23 of the Commission Technical Document.
100 Note again that this paper focuses only on the measures concerning intra-EU cooperation, leaving aside proposals dealing with extra-EU cooperation.
101 See Commission Technical Document (2017), at p 18. In particular, the measure would define specific categories of electronic evidence by means of legislation, and include a library at technical level to facilitate a common understanding of the technical elements to be considered as part of those legal categories.

only the data-owner but also the service provider to which a request for data is addressed.

Second, the Commission proposes to enable direct cooperation between Member States and service providers located in another Member State, hence bypassing the intermediation of local authorities. In this respect, the creation of a common framework is envisaged, providing national authorities with the competence to make non-binding or binding production requests directly to foreign service providers to obtain cross-border e-evidence.[102] Service providers would in turn be allowed – or forced – to disclose e-evidence to foreign authorities on a direct basis. Consequently, the current uncertainty about the rights and obligations of service providers when confronted with a request from another Member State would be dissolved.

However, the parameters relating to such production requests or – when binding – orders still need to be defined. What type of data can be requested? Which service provider could be the subject of an order or request? What are the conditions to issue such request or order?[103] Furthermore, the delineation of jurisdiction would have to be carefully considered.[104] In any event, the jurisdiction of production orders would need to be limited to actors having a link with the EU. This in turn brings forth another parameter, namely the manner in which such link is established. As mentioned above, a variety of connecting factors exist and are currently used.[105]

A decision should also be made on whether the other Member State that could potentially be affected by the request – for example, if the data or the service provider were to be located on its territory – would need to be notified, including the legal consequences of such notification (does it concern a mere right to be informed or also a right to refuse access?[106]). From an individual right's point of view, namely the person whose data is being requested or to whom the data relates, the question of a potential notification and its implications likewise plays a critical role. In fact, notification ensures that procedural rights can be duly exercised.[107] Finally, the Commission suggests

102 See Commission Technical Document (2017), at pp 20-21.

103 *Ibid*., at p 21.

104 See also M. Kaiafa-Gbandi, "Jurisdictional Conflicts in Criminal Matters and their Settlement within EU's Supranational Settings", *EuCLR* Vol. 7, 1/2017, at p 30.

105 Such as the place of the service provider's main establishment, the place where the service provider has a significant presence, or simply the place where the service provider operates. See also Commission Non-Paper (2016), at p 4.

106 It can be argued that such right of notification depends on the manner in which the Member State is affected. E.g. if it merely happens to host the server on which the data is located, but has no link with the service provider, the data subject, or any other aspect of the investigation, it is difficult to justify why such State should nevertheless be notified, let alone have a right to refuse access.

107 See in this respect ECtHR, *Szabó and Vissy/Hungary* nr. 37138/14, 12 January 2016, § 86, where it is stated that: "*the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers*." See also the 2013 Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, at § 82.

that, to ensure compliance by the foreign service provider with the production order, a system of sanctions could be foreseen.[108]

Undoubtedly, the creation of a EU framework for production requests and orders would bring about a significant improvement. The often lengthy procedure of the EIO or MLA – whereby Member State A needs to request Member State B to request service provider C to provide the e-evidence – would be avoided. Furthermore, transparency for individuals on the level of cooperation by service providers with authorities will likewise improve, hence furthering legal certainty.[109] Indeed, service providers' customers would be able to assess beforehand what the service provider can do – or can be forced to do – with their data, regardless of its location.

Most far-reaching, the third proposed legislative measure goes beyond the assistance of service providers. It aims for the harmonization of direct access to e-evidence by means of an extended search. The typical scenario consists of an enforcement authority using its own computers to access data of a subject located elsewhere (often without the subject being aware thereof)[110] or an authority extending the search from a person's device (e.g. a suspect's computer) to a remote server.[111] The latter situation is exemplified by the German case mentioned earlier, where the German authority inspected the law firm's computers and accessed data stored not on the computer itself but on a remote server located abroad.

Such direct access to cross-border electronic evidence is a potential asset when other forms of access (such as through the assistance of a service provider) are not necessary[112], would undermine the investigation, or would be impossible/unfeasible.[113] In the context of a house search where a suspect's computer is inspected, this would allow the authority to directly access data stored remotely, regardless of whether the storage medium is located domestically or abroad, and without the need to request another State's assistance.

Today it is more likely than not that information is stored on a server located in a different Member State than the computer, hence increasing instances of cross-border e-evidence.[114] Moreover, the phenomenon of "*data sharding*", i.e. the storage of differ-

108 See Commission Technical Document (2017), at p 23. In a number of Member States which impose an obligation on service providers to cooperate, such sanctions are already foreseen (see also the above case of *Belgium v Skype*).

109 See also Commission Non-Paper (2016), at p 7.

110 Also referred to as 'government hacking'.

111 See Commission Technical Document (2017), at p 25.

112 The Commission's document provides the example of a victim offering his or her Facebook account information to the authority, which enables the latter to read messages sent thereto by the harasser/perpetrator.

113 This can for example be the case when the investigation has a covert nature, or when it concerns a complex cloud computing environment. See also M. Taylor, J. Haggerty, D. Gresty & R. Hegarty, "Digital evidence in cloud computing systems", *Computer law & Security Review* 26, 2010, at p 305.

114 See Commission Technical Document (2017), at p 25. See also C. Conings, *Een coherent regime voor strafrechtelijke zoekingen in de fysieke en digitale wereld*, KULeuven, Leuven, 2016, at p 546.

ent parts of a database across various servers that may be in different locations, has become increasingly common.[115] Obtaining the cooperation of all those different states beforehand – assuming these locations are actually known prior to the search – would be unworkable in practice. Hence, the establishment of a harmonised legal framework to enable direct access to cross-border e-evidence from an IT system would entail a substantial improvement.

The precise mechanism of such framework, however, still remains a question mark. It should be explored whether, how and when a potentially affected Member State should be notified of another State's access and, once again, what the legal consequences of such notification would be. Moreover, the connecting factor used to establish the status of an 'affected state' should likewise be determined.[116]

Finally, and most sensitively, in order to guarantee the protection of fundamental rights – in particular the right to privacy and defence – certain conditions and due process safeguards for direct access should be ensured. These can consist of, *inter alia,* the requirement of a prior judicial decision authorizing the search, notification of the individual whose data is targeted, and/or a certain severity of the offence investigated.[117] Crucial in this respect is also the transparency of the procedure, which – through a potential system of detailed reporting of the access and search activities of service providers and authorities – enhances legal certainty. Additionally, it must be ensured that the proposed investigation measures – as is also foreseen under the system of the EIO[118] – can be used both *à charge* and *à décharge*.[119]

This third and most far-reaching measure would offer a legal solution to most of the issues with the current framework and effectively adapt the Member States' toolbox to today's digital reality. While thus potentially entailing a big leap forward in the attainment of swifter criminal justice in the EU, the measure's invasiveness would also pose

115 See Commission Technical Document (2017), at p 25. See also J. Spoenle (fn. 6), at p 5; P. Ryan, S. Falvey, "Trust in the Clouds", *Computer law & Security review* 28, 2012, at p 520.

116 In this regard, it has convincingly been argued that when it concerns data in cyberspace, the focus in terms of connecting factor should be shifted away from the location of the object (i.e. the stored data) and move to the investigated subject (i.e. the person suspected of a crime). See for example C. Conings (fn. 81), at p 10; M. Simonato (fn. 2), at p 286; C. Leacock (fn. 76), at p 225. A subject-centered approach would also be consistent with the EIO Directive, which for the interception of telecommunications focuses on the location of the subject as opposed to the object in order to establish the connecting factor (see Article 30(2) of the EIO Directive).

117 Commission Technical Document (2017), at p 22.

118 See Article 1 (3) of the EIO Directive.

119 See C. Conings (fn. 81), at p 20; R. Boddington, "A Case Study of the Challenges of Cyber Forensics Analysis of Digital Evidence in a Child Pornography Trial", *ADFSL Conference on Digital Forensics*, *Security and Law*, 2012, at p 158; M. Simonato (fn. 2) at p 289. The right to use e-evidence *à décharge* is seen as part of the "quality of arms" principle as also enshrined in Article 6 of the European Convention on Human Rights.

a significant risk for breaches of fundamental rights,[120] and rely most heavily on Member States' mutual trust.[121]

The proposed legislative measures are still framed in relatively general terms and contain a number of policy choices that are yet to be made. Moreover, the measures must be translated into a proper proposal for a Directive – based on the Union's competence by virtue of Article 82 TFEU – which the Commission intends to prepare by early 2018. To this end, the Commission already conducted an Inception Impact Assessment in August last year.[122] Additionally, a (second) public consultation was held until the end of October 2017 to collect the views of relevant stakeholders. In what follows, the Commission's proposed legislative measures will be assessed and the main challenges they pose will be addressed.

IV. Challenges raised by the proposed harmonization

The Commission's legislative proposal[123] foresees far-reaching competences for national authorities and removes the impracticalities of the territoriality principle which today still reigns over cyberspace. However, it also leads to new challenges which should not be underestimated and deserve careful attention. These can be narrowed down to two points in particular: (a) maintaining an adequate level of protection of fundamental rights and (b) ensuring consistency with already existing relevant regulation on national, supranational and international level.

1. Challenges for the adequate protection of fundamental rights

a) Adequate protection of fundamental rights: necessity of a level playing field

The clash between the right to security and criminal justice versus the right to privacy and defence – each catering different needs – inevitably leads to a difficult balancing exercise for the legislator.[124] Moreover, such balancing is necessarily – and at times heavily – influenced by the contemporaneous political setting, as well as by national traditions and values. As mentioned above, many of the newly adopted national laws

120 Accordingly, a number of privacy advocates already uttered severe critiques. See for instance the paper prepared by privacy advocate group *Access Now*, authored by A. Stepanovich *et al*., "A Human Rights Response to Government Hacking", *Access Now*, 6 September 2016.

121 See also See V. Mitsilegas (fn. 27), at p 125.

122 See Inception Impact Assessment: Improving cross-border access to electronic evidence in criminal matters, Ref. Ares(2017)3896097 – 03/08/2017, available at: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en.

123 As noted above, this proposal has so far only been laid down in a Technical Document prepared by the Commission, and an actual legislative proposal in the form of a Directive can be expected in early 2018.

124 See in this regard S. Manacorda (fn. 13).

facilitating the collection of e-evidence have been the subject of strong criticism from human rights organizations, not always without cause.

It was already noted that the standard of legal protection for fundamental rights in the context of access to e-evidence differs from one country to another.[125] Instruments based on mutual recognition nevertheless heavily rely on the idea that Member States can trust in the fact that the other states' procedural standards are sufficient to protect their own citizens. Accordingly, and to ensure the effectiveness of the cooperation system, the EIO mechanism only foresees a limited number of grounds which a Member State can invoke to refuse another state's request, given the mandatory trust in that State's system.[126] One of these refusal grounds concerns "*substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter*".[127] Given the different protection levels afforded by the national regulations, the use of such ground of refusal is not unimaginable.[128] While all Member States agree with fundamental rights in principle, the precise implementation of those rights is another story.

Returning to the Commission's proposal, mutual trust becomes even more crucial when allowing other states to directly obtain information from non-government actors such as service providers or remote computer systems.[129] In such situation the possibility for the affected state to conduct a legal check is entirely marginalised, if not absent, which has severe consequences for the exercise of procedural rights. Focusing on the third legal measure proposed by the Commission, the concrete impact thereof becomes clearer when drawing a hypothetical analogy with the mechanism of the European Arrest Warrant ("EAW"). In the context of the EAW, Member State A can request Member State B to execute an arrest warrant targeted at a subject located on B's territory. Should a hypothetical analogous provision to the abovementioned third legal measure proposed by the Commission be inserted in the EAW system, this would allow Member State A to simply enter B's territory and directly arrest the subject itself, without B – and B's procedural rights – being in the picture.

125 See J. S. Hodgson (fn. 31), at p 620; M. Simonato (fn. 2), at p 281; M. T. Schunke (fn. 73), at p 51; V. Mitsilegas (fn. 27), at p 130.

126 Listed in Article 11 of the EIO Directive.

127 See in particular Article 11(1)(f) of the EIO Directive and § 12 of the EIO Directive's preamble.

128 See however the Court's emphasis on the effectiveness on the principle of mutual recognition and its strictness in allowing for a ground of refusal based on fundamental rights, such as expressed in Case C-396/11, *Radu*, judgment of 29 January 2013, ECLI:EU:C:2013:39; Case C-399/11, *Melloni v Ministerio Fiscal*, judgment of 26 February 2013, ECLI:EU:C:2013:107. These judgments demonstrate that, as long as the EU rule at the basis of the request complies with fundamental rights, Member States are in principle not allowed to invoke "national" fundamental rights as a ground to dismiss mutual recognition. See also V. Mitsilegas (fn. 27), at p 135.

129 See M. T. Schunke (fn. 73), at p 49; J. S. Hodgson (fn. 31), at p 613; I. Zerbes (fn. 4), at p 309.

Certainly, the proposal at hand "only" concerns the access to e-evidence and not to an individual. Yet evidence plays a decisive role in criminal investigations, effectively making or breaking a case, and its proper handling is likewise crucial for the rights of defence. Can it hence not be argued that, before allowing state A to directly obtain e-evidence in state B and targeting an individual acting under the expectation that such data would be protected by the laws of B, an adequate level playing field of procedural rights across the EU should be established?

Admittedly, a number of steps have already been taken in the (minimum) harmonization thereof, pursuant to the Roadmap on Procedural rights adopted by the Council in 2009.[130] In the meantime, three measures have been adopted and implemented in national legislation: Directive 2010/64/EU on the right to interpretation and translation in criminal proceedings, Directive 2012/13/EU on the right to information in criminal proceedings, and Directive 2013/48/EU ensuring the right of access to a lawyer in criminal proceedings (including in the context of the EAW) and the right to communicate with a third party upon arrest. A next set of harmonizing measures has been adopted and implementation in domestic law is underway.[131]While constituting a step in the right direction and certainly to be applauded, these Directives, however, do not create a comprehensive level playing field in criminal procedural rights, and their piece-meal approach of harmonization is not always heartily welcomed.[132] Moreover, none of these measures are targeted at the specific due process issues arising in the context of e-evidence.

More tailored to that purpose is the 2008 Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[133] The Framework Decision, which was adopted prior to the depillarization by the Lisbon Treaty, is now being replaced by Directive 2016/680, which should be implemented into Member States legislation by 6 May 2018.[134] The legislation's objective is twofold: (i) ensuring – and harmonizing – individuals' right to pro-

130 See Resolution of the Council of 30 November 2009 on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings, OJ C 295, 4.12.2009, p.1–3. See also P. Hert, C. Riehle, "Data protection in the area of freedom, security and justice. A short introduction and many questions left unanswered", *ERA Forum* Vol.11 (2), 2010, at p 167; J. R. Spencer, "EU Fair Trial Rights – Progress at Last", *New J. Eu. Crim. L*, 2010, Vol.1 (4), at p 447; A. Tinsley, "Protecting Criminal Defence Rights through EU Law: Opportunities and Challenges", 4 *New J. Eu. Crim. L*., 2013, at p 461; V. Mitsilegas (fn. 27), at p 158.

131 The adopted directives on the presumption of innocence (2016/343), legal aid (2016/1919) and procedural safeguards for children (2016/800) should be implemented by Member States respectively by April 2018, May 2019 and June 2019.

132 See for example M. T. Schunke (fn. 73), at p 46.

133 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60–71.

134 Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such

tection of personal data when processed by national authorities and (ii) ensuring and facilitating the free exchange of personal data by authorities within the Union.[135] The Directive foresees a number of rights for the data subject, including the right to be informed of those rights in a comprehensible manner.[136] It also introduces a stronger protection of data that are by their nature sensitive, such as data revealing racial origin.[137]

Nevertheless, Member States are able to adopt legislative measures delaying, restricting or omitting information to data subjects[138] or restricting access to their personal data to the extent that, and as long as, such a measure constitutes "*a necessary and proportionate measure in a democratic society*".[139] Any restriction of the rights of the data subject must, however, be decided on a case-by-case basis and comply with the Charter and the ECHR.[140] Directive 2016/680 thus aims to balance out the right of authorities to withhold notification if necessary for the success of the investigation against the right to receive an adequate protection of fundamental rights.[141] While the Directive can hence play a key role to ensure respect for such rights also in the context of (direct) access to cross-border e-evidence, it does not provide an overall solution.

Likewise of help, the future Directive which will harmonise access to cross-border e-evidence should – when implemented and used by national authorities – subject the latter's actions to the Court's competence to review conformity with EU fundamental rights. While the Charter is primarily addressed to the Union institutions, pursuant to its Article 51 it likewise applies to Member States when implementing EU law.[142] This would hence constitute an extra layer of protection.[143] Indeed, it is imaginable that a suspect would challenge the authority's decision to access data stored on a server abroad (based on the competences granted by the future Directive), and thereby in-

data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131. See C. Cocq, "EU Data protection rules applying to law enforcement activities: Towards an Harmonised Legal Framework?", *New Journal of European Criminal Law*, Vol. 7, Issue 3, at p 264.

135 See also P. de Hert and V. Papakonstantinou, "The New Police and Criminal Justice Data Protection Directive: A First Analysis", *New Journal of European Criminal Law*, Vol. 7, Issue 1, 2016, at p 15.

136 Those rights include information on the identity of the data controller, the existence of the processing operation, the purposes of the processing, the right to lodge a complaint and the right to request from the controller access to and rectification or erasure of personal data or restriction of processing. See § 42 and § 43 of the Directive's preamble.

137 See Article 10 of Directive 2016/680.

138 See Article 13 of Directive 2016/680.

139 See Article 15 of Directive 2016/680 and § 44 of the Directive's preamble.

140 See § 46 of the Directive's preamble.

141 See P. de Hert and V. Papakonstantinou (fn. 135), at p 18.

142 See in this regard C-617/10, *Åklagaren v Hans Åkerberg Fransson*, 26 February 2013, ECLI:EU:C:2013:105, indicating that such provision is interpreted broadly by the Court. See also F. Fontanelli, "The Implementation of European Union Law by Member States under Article 51(1) of the Charter of Fundamental Rights", *Colum. J. Eur. L.*, 2014, Vol.20 (3), at p 193.

143 See also See V. Mitsilegas (fn. 27), at p 10.

voke the Charter before a national court. This challenge may in turn trigger a reference for a preliminary ruling with the Court of Justice of the European Union ("CJEU"), so as to obtain an interpretation on – or even the potential invalidation of – the Directive.

In this respect, it can be recalled that only three years ago the CJEU, in its landmark judgment *Digital Rights Ireland*[144], spectacularly invalidated the Data Retention Directive.[145] Seized by the Irish High Court and the Austrian Verfassungsgerichtshof who requested a preliminary ruling on the Directive's validity, the CJEU found the latter to provide for a wide-ranging, serious and disproportionate interference with the fundamental rights to respect for private life and protection of personal data. And while a future Directive which would harmonise national competences to access cross-border e-evidence should meet the 'objective of general interest' test, it is less evident that the Directive would easily meet the 'proportionality' test.

The Commission is aware that respect for fundamental rights must be ensured and points to a number of potential safeguards for their protection in its proposal.[146] Yet the concrete implementation thereof remains an open question and requires further consideration.[147] Considering the above, and bearing in mind the critical eye of the Court of Justice on matters relating to fundamental rights[148], these issues should not be

144 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, ECLI:EU:C:2014:238.

145 Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications, OJ L 105, 13.4.2006, p. 54–63. National legislation implementing this Directive had already successfully been challenged before national courts, such as in Romania, Germany and the Czech Republic prior to the Directive's invalidation.

146 See the Commission Technical Document (2017), at p 6. One example is the requirement of a prior judicial decision authorizing the access rather than the mere initiative of the public prosecutor.

147 Note also that the Commission does not yet address what the consequences of a violation of those safeguards would entail, whereas it is crucial for the effective protection of fundamental rights to have such consequences be made explicit. Indeed, defendants must have legal certainty over the exact fate of the evidence which was obtained in breach of their rights (the law could for instance exclude such evidence pursuant to the "fruit of the poisonous tree" doctrine). This issue – along with a number of other concerns – is however not addressed in the Commission's proposal and merits further thought.

148 It can be noted that the CJEU has been at the forefront of protecting fundamental rights in the context of data collection and privacy, taking a strict approach against arguments relating to security. This is exemplified by the mentioned Digital Rights Ireland case, but also by a number of recent cases dealing with e-data. See e.g. Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650; Joined cases C-203/15 *Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others,* 21 December 2016, ECLI:EU:C:2016:970; Opinion 1/15 of the Court pursuant to Article 218(11) TFEU (Parliament's request) on the envisaged agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, 26 July 2017, ECLI:EU:C:2017:592.

taken lightly.[149] Any future harmonizing instrument must withstand the test of conformity with the Charter, as well as with the European Convention of Human Rights and fundamental rights forming an integral part of the general principles of law.[150] To illustrate the particular difficulties raised by this challenge, the consequences which the future Directive shall have on the right to legal privilege – recognised by the Court as fundamental – are used a case study and briefly examined below.

b) The right to Legal Privilege: an illustration of the harmonization's consequences

Articles 47 and 48 of the EU Charter of Fundamental Rights enshrine the right to an effective remedy and to a fair trial (including the right to be advised, defended and represented), as well as the presumption of innocence and the right of defence.[151] These two articles have been interpreted by the CJEU as also encompassing the protection of legal privilege, which is "*a recognised principle at EU level reflecting a delicate balance in light of the European Court of Justice's case law on the right to a fair trial – itself reflecting the principles of the ECHR as well as of the Charter*".[152] The CJEU has indeed stated that "*[a]ny breach of legal professional privilege during an investigation represents a serious interference with a fundamental right.*"[153]

A line of CJEU judgments – mostly emanating from the context of antitrust proceedings – has established and consistently confirmed the importance of legal privilege in the EU legal order.[154] Given its particular role in the context of criminal matters, the

149 See in this regard also the Article 29 Working Party Statement on the Commission's proposal, titled '*Data protection and privacy aspects of cross-border access to electronic evidence*' of 29 November 2017, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610177.

150 See P. Ryan, S. Falvey (fn. 115), at p 518.

151 See also E. Symeonidou-Kastanidou, "The Right of Access to a Lawyer in Criminal Proceedings: The transposition of Directive 2013/48/EU of 22 October 2013 on national legislation", *EuCLR* Vol. 5, 1/2015 at p 68.

152 Quote from the Commission Staff Working Document of 26.6.2017 which accompanies the Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market.

153 See C-550/07, *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v European Commission*, 14 September 2010, ECLI:EU:C:2010:512 (hereafter 'Akzo'), at § 41.

154 See in particular case C-155/79, AM*&S Europe Limited v Commission of the European Communities*, 18 May 1982, ECLI:EU:C:1982:157 (hereafter 'AM&S'); C-550/07 *Akzo*; but also C-305/05, *Ordre des barreaux francophones et germanophone and Others v Conseil des ministers*, 26 June 2007, ECLI:EU:C:2007:383 (hereafter 'Ordre des barreaux'), not relating to antitrust. In this regard, the CJEU also frequently refers to the case law of the ECHR, such as *Golder v United Kingdom*, judgment of 21 February 1975, Series A No. 18, §§ 26 to 40; *Campbell and Fell v United Kingdom*, judgment of 28 June 1984, Series A No. 80, §§ 97 to 99, §§ 105 to 107 and §§ 111 to 113; and *Borgers v Belgium*, judgment of 30 October 1991, Series A No. 214-B, § 24. Not all lawyer-client communications are protected by the legal-professional privilege; the privilege applies only if both of the following conditions are fulfilled: (i) the exchange with the lawyer must be connected to 'the client's rights of defence' and (ii) the exchange must emanate from 'independent lawyers'. When a

right to legal privilege has been codified in Directive 2013/48/EU on the right of access to a lawyer in criminal proceedings.[155] The Directive's preamble clarifies that confidentiality of communication between suspects and their lawyers is key to ensuring the effective exercise of the rights of defence and is an essential part of the right to a fair trial.[156] Accordingly, Member States should respect the confidentiality of meetings and other forms of communication between the lawyer and the suspect and – pursuant to the Directive – without derogation.[157] Moreover, the Directive also brings questions on legal privilege in the context of criminal proceedings within the *acquis communautaire*, and hence open to potential review by and rulings from the ECJ.

Returning to the Commission's proposal enabling direct access to cross-border e-evidence, and bearing in mind the fundamentality of legal privilege in criminal procedures – how exactly will respect of this right be ensured? Pursuant to the EIO Directive, one of the grounds on which Member States can base themselves to refuse another state's request, is the fact that '*there is an immunity or a privilege under the law of the executing State which makes it impossible to execute the EIO*'.[158] The preamble clarifies that there is no common definition of what constitutes an immunity or privilege in Union law, and that the precise definition of these terms is therefore left to national law.[159]

Under the EIO's framework, Member State A must submit a EIO to Member State B, and it is the latter who formally verifies that no grounds for refusal are present, and thereupon gathers the requested evidence in its territory. This renders Member State B a *de facto* reviewer of the EIO's conformity with fundamental rights, on top of State A's own obligation thereof. Moreover, Member State B can also ensure that execution of the EIO does not hamper its national rules on privilege. However, under the newly envisaged framework, the step of contact between the two Member States is skipped, and Member State A would be able to directly enforce a production order with a service provider located in State B, or – more intrusively – directly access data which is virtually stored in State B. It can thus not be excluded that a situation occurs whereby, even though the data may be subject to legal privilege under the laws of State B, State A could nevertheless access such data directly. And while State A would most likely be required – based on its own legal privilege rules – to verify whether access to such data would infringe the privilege rights of the defendant, it may very well be that State A's rules on privilege are different than State B's.[160]

lawyer assists a client in the context of a criminal investigation, these conditions are typically met and the right to legal privilege as construed by the Court applies.

155 See Article 4 of Directive 2013/48/EU, OJ L 294, 6.11.2013, p. 1–12; E. Symeonidou-Kastanidou (fn. 151), at p 70.

156 See § 33 of Directive 2013/48/EU.

157 *Ibid.*

158 See Article 11(1)(a) of the EIO Directive. See also I. Zerbes (fn. 4), at p 310.

159 See § 20 of the EIO Directive's preamble. See also V. Mitsilegas (fn. 27), at p 178.

160 Indeed, EU Member States' legal privilege rules greatly differ in scope. See also J. Holtz, "Legal Professional Privilege in Europe: a Missed Policy Opportunity", *Journal of European Competition Law & Practice*, Volume 4, Issue 5, 1 October 2013, at p 405.

A simple hypothetical example can illustrate this scenario. Company A, headquartered in Belgium but with offices all over the world, including in Paris, is investigated by the French police for potential fraud in France. During an unannounced search in the company's Paris office, the police wishes to access data stored on the company's computers. The computer's server is, however, located in Belgium. So far so good: pursuant to the future Directive, the French police would in principle be able to access the data in Belgium without breaching the limits of its enforcement jurisdiction.

Let us now assume that the data which the French authority wishes to access concern communications between a company manager and the company's in-house counsel located in Belgium. Belgian law provides legal privilege not only to bar-admitted external counsels, but also to in-house counsels. By virtue of Belgian law, such communications would thus be legally privileged. France, however, does not acknowledge legal privilege for in-house counsels. A number of difficulties are immediately apparent. Which law prevails? How shall this be ascertained? Should the French authority be trained in the privilege rules of all Member States?

Moreover, even if the data concern documents exchanged not with an in-house but with an external counsel; are there sufficient safeguards in place to ensure that such communication is not looked into? While all Member States foresee a legal privilege for exchanges with external counsels, the definition, scope and application of the privilege still significantly differ from one state to another. Should we expect all authorities to be trained in each other's rules? Does our trust in the mutual recognition mechanism suffice, even if the scope of protection for the same type of data – and hence the scope of the rights of defence – substantially differ?

Furthermore, whereas the above scenario concerns the search of a company's premises, whereby it can be assumed that the subject of the search is present and can raise the confidentiality of the data (whether accepted by the authority or not), a number of complications can be added. What if, instead, the searching authority directly asks the service provider located in another Member State to produce the (privileged) communication? Should we expect the service provider to raise the issue of legal privilege? Begging the question even further, what if the authority conducts a remote search – from the police's own computer system – and accesses the data without a service provider's assistance (*i.e.* legal hacking)? More often than not such search occurs without notifying the data subject, as notification could hinder the search's success. Yet how can it then be ensured that the privilege applying to such communication is protected?

This conundrum is not a hypothetical one. In fact, in the German car manufacturer case mentioned earlier, where the authorities accessed documents at the suspect's law firm, the right of legal privilege played a fundamental role.[161] Clearly then, the question should be raised whether – before engaging in enhanced mutual trust which goes substantially beyond the trust at stake today by harmonizing Member States' competences to directly access cross-border e-evidence – first a higher level of harmo-

161 See supra under Part III, A, 1.

nization of procedural rights should be ensured to avoid such concerns.[162] Indeed, a unified approach to strong procedural rights – also encompassing fundamental rights such as legal privilege – to counterbalance intrusive investigation measures, seems both crucial and indispensable for the new instrument to withstand the fundamental rights test.

2. Challenges for ensuring consistency within a coherent system of rules

Conformity of the future Directive with fundamental rights is key, but is not the only major challenge the EU regulator will face. Importantly, the new instrument will belong to a framework of already existing regulations on various jurisdictional levels governing access to (electronic) evidence. Furthermore, this framework is in turn part of a broader system of procedural rules for which an ever-increasing number of EU instruments are being established. Consequently, it must be ensured that the new Directive will be consistent with, and be a coherent part of, the existing framework both vertically *(i.e.* consistency with existing laws on evidence collection on national, supranational and international level), and horizontally (*i.e.* consistency with existing laws on neighbouring issues which impact e-evidence collection).

a) Vertical Consistency

The lack of a specific set of rules regulating cross-border access to e-evidence, and the correlated difficulties to achieve swift criminal justice, needs to be – and is about to be – tackled. However, as was set out in Part II above, this does not mean that no framework is already in place which, at least in part, governs cross-border cooperation. Various instruments which are in force today are directly relevant in this respect, and it is precisely because of their multiplicity and/or their inadequacy that the need for a more coherent framework arose. Though the future Directive is meant to take over the role of some existing laws, it is unlikely that the former shall entirely substitute the latter. Rather, it shall exist as a supplement to and in symbiosis with other international, supranational and national rules, and must therefore aim to be consistent therewith.

As already discussed, on international level the most relevant legal instruments concern the Conventions of the Council of Europe, these being in particular the MLA Convention and the Cybercrime Convention. While the future EU Directive is aimed to go beyond the cooperation currently foreseen under these Conventions, they will co-exist, not only as concerns cooperation with extra-EU states but likely also within the EU if certain Member States opt out. The same can be said for the currently existing instruments on EU level, of which the most relevant ones for our purposes are the EU Convention on MLA in Criminal Matters and the EIO Directive.

162 See also M. T. Schunke (fn. 73), at p 53.

While a number of Member States never ratified the EU MLA Convention, apart from Denmark and Ireland all have implemented the EIO Directive.[163] It is not unthinkable that the same two countries will likewise refrain from participating to the new Directive regulating access to cross-border e-evidence. Both have, however, signed and ratified the MLA Convention of the European Council[164] and – except for Ireland and Sweden – all Member States have ratified the Cybercrime Convention. Accordingly, these instruments shall – at least to some extent – remain valid tools also in certain EU Member States. The co-existence of these different instruments warrants the striving for a coherent approach, in particular as regards concepts and definitions. Moreover, the interrelation between these instruments should likewise be articulated.

Turning to legislation on Member State level, the same considerations can be made. While the new instrument aims to harmonise and de-fragmentise the different national laws, it cannot be seen separate therefrom – being limited only to the subject of access to cross-border e-evidence. Moreover, the different national rules and their mechanisms can be used as a source of inspiration. Mapping the legal situation in the various EU Member States can be an enlightening exercise in the process of adopting new EU rules.[165] Furthermore, since it is after all the Member States' jobs to ultimately implement the new Directive into their laws, a thorough understanding of the States' existing rules could facilitate and smoothen the future implementation process.

Finally, the flaws contained in some of the national regulations that enable access to e-evidence and the heavy criticism formulated thereon must be born in mind. Indeed, it should be ensured that such flaws (in particular in the protection of fundamental rights, such as privacy and due process) are not simply extrapolated to the European level, but are anticipated and corrected in the harmonizing instrument.

b) Horizontal Consistency

Besides interacting with existing regulations on different jurisdictional levels, the new instrument will also interact with existing (or developing) regulations dealing with neighbouring subject matters. Accordingly, consistency also needs to be ensured from a horizontal point of view.[166] This is first and foremost the case for the above-mentioned 2008 Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, soon to

163 While Denmark has foregone the option to opt-in to the EIO Directive, for Ireland this question still remains open.

164 Not without reservations – for an overview see: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/030/signatures?p_auth=cg5n8Lid.

165 Important initiatives have been taken in the EU to understand and map the diversity of national legislation relating to criminal procedural rules, also focusing on evidence. See for example the Evidence Project dedicated to the application of new technologies in the collection, use and transmission of e-evidence, and the E-Codex project, designed to improve access by European citizens and businesses to legal means across-borders.

166 See also the Article 29 Working Party Statement of 29 November 2017, referred to under fn.150 above.

be replaced by Directive 2016/680 adopted together with the General Data Protection Regulation ("GDPR").[167] Both Directive 2016/680 and the GDPR were adopted in the context of the Commission's reform of the EU data protection rules. While the GDPR strengthens citizens' fundamental rights in the business context,[168] Directive 2016/680 for the police and criminal justice sector aims to protect citizens' each time personal data is used by criminal law enforcement authorities. Both pieces of legislation will become applicable to EU Member States in May 2018.[169] Considering the establishment of this new and comprehensive mechanism for protecting personal data both in the public and private sphere, it is only normal to require that any new piece of legislation directly dealing with personal data – such as evidence in the form of electronic data – maintains consistency therewith. This implies consistency with the used legal terms and concepts, as well as – to the extent feasible – with the relevant procedures. Moreover, the relationship between the various pieces of legislation and their applicability in the context of e-evidence collection should be made explicit.

Other pieces of legislation are also relevant. Contrary to the invalidated Data Retention Directive, Directive 2002/58/EC on privacy in the electronic communications sector[170] (which was supposed to be amended by the former) is still alive and kicking. Accordingly, if the aim is to avoid a new invalidation of a Directive touching upon issues of privacy, the new instrument better ensures consistency therewith. Note that this Directive itself is currently undergoing a review in order to bring its provisions in conformity with the new data protection rules.[171] Furthermore, the Roadmap Directives mentioned above, harmonizing several procedural rights for individuals in the context of criminal proceedings, should likewise be considered. As for example already highlighted, Directive 2013/48/EU – ensuring access to a lawyer in criminal proceedings – inter alia contains an explicit reference to the right to legal privilege.[172] Such right should be consistently ensured in the new piece of harmonizing legislation.

Finally, besides ensuring consistency with legislation in similar areas, the quest for consistency can be taken a step further by asking whether additional steps should be

167 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('General Data Protection Regulation'), OJ L 119, 4.5.2016, p. 1–88.

168 Importantly, the GDPR also covers situations in which service providers collect/processes personal data to comply with a legal obligation to which they are subject (see also § 45 of the GDPR's preamble).

169 The Regulation becomes binding on 26 May 2018, and the Directive must be transposed by 6 May 2018.

170 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37–47.

171 A new proposal was adopted in the form of a Regulation on 10/01/2017. See Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD).

172 See Article 4 of the Directive.

taken to obtain a more coherent framework for (criminal) procedural rules as a whole. Indeed, it can be wondered more generally whether the piece-meal approach to harmonization in procedural rights is a desirable one[173], and whether this approach does not lead to important gaps in the protection of rights. One such gap identified is the lack of a level playing field in procedural rights granted to defendants whose electronic data are searched during a criminal investigation. Arguably, the upcoming Directive 2016/680 aims to fill such gap to a large extent, but is unlikely to solve all problems. For instance, it is entirely silent on the issue of the protection of legal privilege.

In sum, the new legal instrument will not be an isolated piece of legislation, but shall be part of a web of different conventions, regulations, directives and laws, governing the Member States' competences to access e-evidence and achieve criminal justice. The overarching framework should thus not be dropped out of sight, yet, given the proliferation of legislation, any attempt for consistency – indispensable as it may be – will inevitably pose a challenge.

V. Conclusion

In today's digital age, a large part of our lives has shifted from the physical to the virtual world. This holds true for the ordinary citizen and is not different as regards criminals. Consequently, in the context of criminal investigations, many pieces of evidence concern e-evidence, often located in another Member State. And while no one will deny that virtual borders are different than physical ones, due to the principle of territoriality, existing regulations still treat both in the same way.

Having provided an overview of the current legislative framework dealing with access to cross-border e-evidence, this paper subsequently exposed the framework's issues. It was argued that the inadequacy and inefficiency of the tools available to criminal investigators in cross-border scenarios is ridiculous at best, yet dangerous at worst. This is coupled with the fragmentation of national legislation dealing with such matters, in turn leading to a situation of legal uncertainty, likewise hampering the goal of swift criminal justice in the EU.

The Commission's envisaged solution to the problems, expressed in terms of legal measures to be translated into a new Directive expected in early 2018, addresses a number of the identified problems, but is not immune to criticism. Indeed, the proposal creates its own challenges, particularly in terms of the adequate protection of fundamental rights, and the maintaining of consistency and coherency with already existing regulation.

At present, searching a person's computer or smartphone can arguably be more intrusive than searching a person's home. It is, therefore, beyond question that enhanced cross-border cooperation, enhanced competences of investigation, and enhanced mutual trust, should be coupled with enhanced safeguards for the respect of fundamental rights. Finding the right balance between those rights on the one hand, and the right to

173 See M. T. Schunke (fn. 73), at p 46.

security and criminal justice on the other, is one of the most difficult tasks a legislator must fulfil. While in such situation it may be arduous for politics to withstand the emotional calls for action – particularly after the occurrence of specific threats to citizens' safety – history has taught that this balancing exercise deserves no shortcuts, and that the Court of Justice's vigilant stance can be counted on.

It would be a mistake to fall into the trap of the Nirvana fallacy and fantasise about a new legislative instrument which could perfectly accommodate all the concerns uttered by criminal enforcers and privacy advocacy groups alike. But it would be an even bigger mistake not to subject a new piece of legislation – which will have a significant impact on some of the most delicate issues of society – to constructive criticism and point towards the challenges such legislation must face. This paper aims to contribute to the latter.