Co-funded by the Justice Programme of the European Union
Project JUST-2015-JCOO-AG-CRIME-723150

THE EUROPEAN INVESTIGATION ORDER: CHALLENGES TO FUNDAMENTAL RIGHTS AND SOVEREIGNTY IN THE DIGITAL AGE

-ROUND TABLE-

Introduction

The intensive use of electronic communications such as webmail, messaging services apps or social media has led criminal investigations to increasingly rely on electronic evidence(e-evidence). While a formal definition of e-evidence has not yet been stablished, most interpretations seem to adopt broad approach to the same[1]. The fact that Internet Services Providers (hereinafter" ISP") and their infrastructures are often outside EU Member States, has led strictly local offences to increasingly acquire a cross border and international connotation. At the same time, the complexity of a networked society and the volume of information produced critically challenges the traditional mechanisms of evidence gathering by law enforcement authorities (hereinafter "LEA's").

LEA's requiring access to evidence during the investigation of a crime normally rely on a diverse set of mechanisms involving judicial cooperation, mutual legal assistance (MLA) or mutual recognition treaties. More recently the need for faster solutions has often set the spotlight on the cooperation of ISP upon receipt of evidence production orders and the possibility to directly access data.[2]

Since 22 May 2017, obtaining criminal evidence within the EU is governed by the Directive on the European Investigation Order (EIO Directive). The EIO is a judicial decision, issued or validated by a judicial authority of a member state, for the purpose of having one or more specific investigative measure(s) carried out in another member state to obtain evidence in accordance with the Directive (Article 1 of the EIO Directive). While the EIO had often been considered a milestone and "game changer" for judicial cooperation in criminal matters, as of January 2018, only eighteen Member States have transposed the EIO Directive into their national legislations, and differing views are raised on the risks and practical effectivity of the instrument[3].

---

[1] See for instance definition used by the European Commission https://ec.europa.eu/home-affairs/content/electronic-evidence_en.

[2] See for instance Microsoft / Ireland case or Yahoo! case

[3] The EU Member States were supposed to implement the Directive by May 22, 2017, however, at the time of the writing of this document (January 2018) only 18 of the states have transposed the Directive: Latvia (20 May 2017), Belgium (22 May 2017), France (22 May 2017), Germany (22 May 2017), Hungary (23 May 2017), Lithuania (15 Jun 2017), Netherlands (17 Jun 2017), Finland (3 Jul 2017), Estonia (6 Jul 2017), Italy (28 Jul 2017), United Kingdom (31 Jul 2017), Portugal (22 Aug 2017), Greece (21 Sep 2017), Slovakia (15 Oct 2017), Croatia (26 Oct 2017, Malta (24 oct 2017), Romania(17 Dec 2017) and Sweden (1 Dec 2017). Source: European Judicial Network **<** accessible at https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120 >

Mechanisms for the gathering of evidence such as the EIO faces important legal challenges in environments based in cloud computer architectures. Considering the EIO regime, the round table that took place on January 15th 2018, addressed cross border access to electronic evidence and judicial cooperation examining its fundamental elements and addressing some of its current and future challenges surrounding the notions sovereignty, territoriality and jurisdiction, individual´s fundamental rights and the work of law enforcement authorities in the digital era.

Speakers:

- Catherine Van der Heyning : Criminal lawyer at the Brussels bar, post-doctoral researcher at the University of Antwerp and visiting professor at VUB.

- Gloria Gónzalez Fuster: Research Professor at VUB's Faculty of Law and Criminology. Member of the Law, Science, Technology and Society (LSTS) Research Group and of the Brussels Privacy Hub (BPH)

- Paul De Hert: Professor at VUB, Associated Professor at Tilburg Institute for Law, Technology, and Society (NL) & Co-Director of LSTS, Human rights, privacy, data protection, European and international criminal law.

- Mireille Hildebrandt: Prof. dr. Mireille Hildebrandt is Research Professor on Interfacing Law and Technology, member of the Research Group for Law Science Technology and Society (LSTS) of the VUB. She is also Chair of Smart Environments, Data Protection and the Rule of Law institute of Computing and Information Sciences (iCIS) Radboud University Nijmegen.

Structure of the event:

The Round table was structed in two sections, the first of them leaded by Professor Mireille Hildebrandt who focused on the history of sovereignty and its practice. The second part was carried by Professor Catherine Van de Heyning and discussed Law enforcement and procedural elements of e-evidence gathering.

Each of both sections were also additionally discussed by Professor Gloria González Fuster and Professor Paul De Hert.

Summary of the discussion:

i. First section: Sovereignty history and practice

The round table was opened with Professor Mireille Hildebrandt´s remarks on the history of sovereignty and the conceptualization of territorial jurisdiction. By examining the origins and relation between both notions of sovereignty and territory, the theoretical framework to the relation of sovereignty and cyberspace was set. Professor Hildebrandt noted how the notion of jurisdiction preceded the notion of territoriality thus showing that jurisdiction has not always been strictly tied to land. In that sense, she argued that it was not until the emergence of cartography that a conceptualization of territorial jurisdiction appeared and explained how this new instrument allowed the production of "*a gapless map of mutually exclusive political territories*", this having fundamental implications to the notion of sovereignty and the way it was exercised.

Linking it to the matter of the EIO, Professor Hildebrandt questioned "*what does legal protection depends on?"* and stated that "*in the EIO citizens of one State are expected to trust their own authorities but also the authorities that their own authorities trust*". As result, according to Hildebrandt, it appears that the main question relies on the nature of such trust and to whether trust is ought to be transitive between citizens and states and then among states themselves. Hildebrandt reasserts that looking to sovereignty and territorial jurisdiction from this perspective, basically implies that effective and practical legal protection ultimately depends on national jurisdiction, which in turn relies on sovereignty and which is composed by an internal -principle of non-interference- and an external -equality of space- components. Professor Hildebrandt continued describing the relation between national jurisdiction, international law and national sovereignty, stating that insofar national jurisdiction is based on International law, this the one attributing national sovereignty, even when states are those determining the content of International law.

Finally, Hildebrandt concluded "*The whole idea of territorial jurisdiction in the sense of mapping contiguous pieces of land is over because of cyberspace. Cyberspace is not a different space from the land is not like the sea -defined by not being land-, cyberspace is always everywhere. If that is true, we must then rethink and reconstruct the borders of jurisdiction if we want legal protection*".

Elaborating upon Hildebrandt's explanations, Professor Gloria González Fuster begun her intervention questioning the existence of a unique notion of sovereignty, "*can we really say sovereignty in singular or should we use it in plural*?" She then continued connecting her remarks to the round table's title, and pointing out the existence of two types of data sovereignties. From one hand that related to legal protection, from the other, the sovereignty on the data in terms of ownership and processing capacities. Professor González Fuster stated that, while sometimes these different sovereignties can coincide, this might not always be the case. In that line, she referred to the fact that "*the relation of sovereignty's and territoriality might also not coincide.*"

In regard to relation between data protection and cartography, González Fuster claimed that both notions are often unrelated. Alluding to the particular case of the EU, the borderless nature of its data protection framework, and the freedom of data flows, she raised question upon how the different layers of sovereignty are to coexist. Continuedly Professor González Fuster examined the relation between data protection and the EIO, indicating that the same has at least two intersections with data protection, which are at the same time mutually interrelated. She explained how in order to be compliant with data protection rules, the EIO needs to provide legal grounds for the processing of data but additionally it also needs to provide the necessary safeguards for such processing. She concluded her remarks saying that "*from a Data Protection perspective the EIO looks better than one might expect*", and stressed positively the fact that while the EIO is inherently linked to an element of trust between member states, such trust is not

unconditional, "*the trust is there but is not blind trust, there is an issuing authority and then there is also an executing authority that has the chance not to execute on the grounds of data protection arguments*".

Professor Paul De Hert took the floor by mentioning the growing awareness of data protection within law enforcement cooperation mechanisms. Acknowledging that while the process to bring data protection in the international cooperation sphere has not been an easy task, in his view, the implementation of data protection rules in the field of police could be read as a rather successful story. A process that has often been based on a trade-off between police and law makers and that has resulted in the adoption by LEA's of data protection rules in exchange for more autonomy in the processing data.

Taking as an example INTERPOL´s constitution agreement, and how challenging it was for the sovereigns or law makers to regulate the role of police in the international sphere, Professor De Hert, stressed the historical importance of the Schengen Agreement in capturing the specific role of police and translating it into law. Conversely, he pointed out that the relation between magistrates and data protection has found significantly more difficulties. In that sense he explained how it was not until the EU convention on Mutual Legal Assistance from 2000, that collaboration between magistrates had introduced data protection provisions[4]. A first step however, that in his opinion has not adequately followed with further clarifications. In that sense he considered that such unclearness is evident when examining from one hand the cooperation treaties in the area of criminal law, and on the other from the soon in force Law Enforcement Directive which, in his view, hardly addresses its impact on the work of magistrates.

Looking ahead, De Hert said that "*in the future we have to consider practical arrangements to complement Data Protection Authorities´ supervision of data processing through the supervision of magistrates controlling magistrates. If not, we will never get there*" he added. A path that he describes as unmapped territory, and that might need to be examined in order to achieve a proper implementation of data protection in judicial practice.

Going back to Professor Hildebrandt talk, he referred to the notions of sovereignty, territoriality and jurisdiction, stating that these concepts are *"rather vague, born in different mindsets, obviously prioritised by some and less prioritised by others"* and added, that nowadays their role is being contested in the sense that their precise implications remains unclear. As a result, he foresees State practice is going to end up giving them an interpretation, and highlighted in that regard the role magistrates -in particular the Belgian ones- who in his view, are unilaterally defining those notions of sovereignty, territoriality and jurisdiction through practice. Something that in his opinion, is silently supported by Member States and policy makers who are using mediatic cases to trigger debates and calibrate their position in the matter. In that regard, Professor De Hert alerted of the current role of magistrates in the policy making sphere, and the fact that their judgment in very specific and concrete cases might be dangerously extrapolated to scenarios beyond those that originated them.

To conclude, Professor De Hert warned "*we have a feeling that there is a call upon us to disregard sovereignty claims in the name of a higher interest but we don't know where to draw the line",* and continued by stating *"we are confused by what some might call liberal cosmopolitans, whenever there is injustice we send our troops and what magistrates are doing today is partly surfing on that wave of a certain benevolent attitude towards Human Rights* intervention, a *very dangerous game*".

[4] Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01) < accessible at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:197:0001:0023:EN:PDF>

ii. Second section: Law enforcement and procedural elements of e-evidence gathering

Professor Catherine Van de Heyning, started by expressing how in her opinion the EIO is a missed opportunity to provide guidance on what e-evidence means and refers to. In her view, while often the focus is put on content data, Law enforcement is on the other hand interested in accessing the other data related to communications. In that line she alerted of the fact that such other data (i.e, metadata) is often not protected under the same guarantees as content data might, this despite their processing effects might equally lead to interferences with fundamental rights.

Focusing on the EIO Directive, she stressed that Belgium was one of its main promoters and stated that behind such interest there was -among others-, the aspiration of facilitating access to e-evidence, more concretely, the possibility to obtain access to communication data in faster and easier way. However, in her analysis she described how the introduction of data protection layers of protection at EU level but also from national standards, might lead to a sentiment of failure in the expectations of the Member States and their judicial and law enforcement authorities, who now see the EIO as not being fast enough. In that sense, what LEA's were really looking forward prior the adoption of the text, was the possibility to obtain production orders against internet service providers (ISP), something that finally was not included. Secondly, Professor Van de Heyning pointed the existence of grounds of refusal for the executing state to provide data on the basis of data protection, a circumstance that very often has served as a ground for criticism over EIO.

This frustration is, according to Van de Heyning, visible in the lack of interest shown by Member States in duly implementing the EIO directive in time. Furthermore, the apparent failure of the EIO seems evident when looking at the current discussions on a possible e-electronic directive, which should now provide for production orders. In that regard she alerted on the possibility to end up with two standards to obtain the same data, one subject to the EIO based on high and very elaborated procedural rules and alternatively the production order with lower standards.

Professor Van de Heyning concluded by saying "*we should reassess whether the EIO will be practical and effective for LEA´s, because that will be one of the elements that will keep on triggering LEA's to push the boundaries further on, but on the other hand, to have some kind of balance with data protection but also with other fundamental rights such as professional secrecy and self-incrimination which are largely forgotten in this discussion*."

Commenting on Van de Heyning intervention, Professor González Fuster started by agreeing on the fact that some fundamental rights are given more attention than others, a circumstance that in her opinion is precisely based on the existence of different types of sovereignty. In that sense, she argues that at EU level, fundamental rights often focused on Article 8 ECHR, which enjoys of a higher level of harmonization, while, alternatively other rights are left to member states and their national perspective. In her view, that's a challenge when dealing with different layers of sovereignty.

In regard to the EIO and data protection, she stressed that the instrument has to include data protection safeguards, an added that in the case of the direct productions orders, there is also a need to make sure that those safeguards also exist in the international context. She warned on the possibility of having very strong MLA treaties with data protection safeguards, and simultaneously and parallelly, other police data access practices do not meet the same standards. Also in that line, she stressed that it is not enough to have data protection safeguards but also that there is a need to be proactive in preventive unlawful access, knowing that the temptation of unlawful access is there.

Going back to the question of authority in the context of the EIO and relating it to the notion of sovereignty, Professor González Fuster posed the following question "who has the authority to say what is compliant or not from a data protection perspective, what is legal or illegal?". And concluded "*when we have direct access there is always an authority that requests the data, we are thus not losing the notion of authority, but we have to ask ourselves whether that authority is enough*".

Recalling on the idea posed by Professor Van de Heyning on the possibility of having two mechanisms for accessing the same data, Professor Paul De Hert warned about ending up with this two-track system, one with high standards that is never used, and another with low standards becoming the routine, "*that is indeed something we should envisage and prevent*", he said.

Concerning the debate around production orders, he argues that the Prüm Treaty might be a good example on how the discussion should be addressed. From a legislative perspective he stressed the fact that Prüm was not negotiated at EU level but among a few neighbouring countries with a high level of trust, who leaded its drafting and who were then followed by others member states. He continued explaining that great part of Prüm's success was due to its very detailed and narrowly focused goal. In that sense he explained how, Prüm basically allowed MS to access vehicle plates data, and introduced a hit no hit system on biometric data, and it was this precise approach the reason why it was so well receipt by LEA's. "*Could we learn something from that*?" De Hert questioned and then said "*Yes, rather than shaping all the whole MLA with one practical need in our head, we should look at this one practical need and perhaps give it a status apart. If it is about knowing who is behind an email account then let's do something Prüm-like around this and no more and see what this brings us."*

On regard to the EIO and the possibility of a new E-evidence Directive, Professor De Hert remarked the fact that the EIO is still in its infancy and stated "*it is a simple wisdom of impact assessing new legislation, that you must have to assess whether new legislation is needed in the light of the experience of existent instruments, and we don't have that experience yet*" and concluded "*I can't see how impact assessments can say we need this new initiative (e-evidence Directive) upcoming now*". Referring to the results obtained in previous workshops carried by LIVE_FOR, De Hert stated that magistrates seem to take this need for new legislation for granted and reiterated his reluctance towards engaging new initiatives in a rushed manner "*we first need details on the functioning or not functioning of the EIO and I am simply not convinced that not functioning is crystal clear*". Finally, regarding the talks around the e-evidence Directive Professor De Hert concluded "*Let's use the Prüm experience but let´s also consider concerns for states and data subject interest and look at the way we have dealt with these different interests often conflicting but sometimes not conflicting in the past*".

References for further reading

- *Hildebrandt, M. 'Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace', (63) University of Toronto Law Journal 2013-2 [special issue Criminal Jurisdiction: Comparison, History, Theory], p. 196-224.*

- *Hildebrandt, M. 'The Virtuality of Territorial Borders', (13) Utrecht Law Review 2017-2, pp.13–27. DOI: http://doi.org/10.18352/ulr.380[4].*

- *De Hert, P., 'Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace – Whose Sovereignty Is at Stake?', in E.-J.KOOPS & S.W. BRENNER (eds.), Cybercrime and Jurisdiction. A Global Survey, The Hague, TMC Asser Press, 2006, 71-110.*

- *De Hert, P. & Sajfert, J., 'The role of the data protection authorities in supervising police and criminal justice authorities processing personal data', in C. Brière & A. Weyembergh (eds), _The needed balances in EU Criminal Law: past present and future_, Oxford: Hart Publishing, 2018, 243-255 (16p.).*

- González Fuster, Gloria (2016), 'Un-mapping Personal Data Transfers [3]', _European Data Protection Law Review, Vol. 2, Issue 2, pp. 160-168.

- *Van de Heyning, Catherine (2016) 'The boundaries of jurisdiction in cybercrime and constitutional protection: the European perspective' in the internet and constitutional law: the protection of fundamental rights and constitutional adjudication in Europe / Pollicino, Oreste. Routledge.*