https://doi.org/10.12697/JI.2020.29.06

Eneli Laurits

District Prosecutor[*1]
Visiting lecturer of IT Law, University of Tartu
Doctoral student, University of Tartu

Regulating the Unregulatable:

An Estonian Perspective on the CLOUD Act and the E-Evidence Proposal

In increasing numbers, criminal investigations are relying on electronic evidence that is not considered open-source data (i.e., material that is not publicly available). Electronic evidence is required in around 85% of criminal investigations. In two thirds of the investigations in that category, there is a need to obtain evidence from online service providers based in another jurisdiction.[*2] While criminals quickly move across borders – at least online – investigators do not, as their warrants are limited in jurisdictional reach. The current scale, scope, and challenges related to cybercrime and electronic evidence are such that cybercrime has become a serious threat to individuals' fundamental rights.[*3]

The jurisdiction of a state is deemed to be territorial. The state may not exercise it outside its territory except under a permissive rule derived from international custom or a corresponding convention. Law-enforcement and criminal-justice matters fall within this exclusive domain of the sovereign state – with the result that, traditionally, criminal jurisdiction has been linked to the geographical territory[*4] and, so far, cyberspace has not wrought much change in that concept. Accessing data stored on a server located in the territory of another state without the prior consent of that state constitutes a breach of the territorial integrity of said state and, thereby, a wrongful act.[*5]

The traditional instruments used for collecting evidence extraterritorially were designed at first for all manner of material apart from digital information, and the territory-based conception born in pre-Internet times made sense in that context. Since then, the Internet has evolved from a predominantly American network into a global one, both in usage and in infrastructure, and, because of these unforeseen developments, such laws (and the associated reasoning of practitioners) are no longer adequate for managing the current reality. In most cases involving digital data, an exclusive connection to one particular state is non-existent.

---

1 The author presents her personal views, which do not reflect the official position of the Prosecutor's Office.

2 Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters. https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf. (accessed 14 April 2020) (first page).

3 'Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY' 6. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e (accessed 14 April 2020).

4 'Comprehensive Study on Cybercrime' [2013] 184. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 14 April 2020).

5 B-J Koops and M Goodwin. *Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law* (Tilburg Institute for Law, Technology, and Society; Center for Transboundary Legal Development, December 2014) Tilburg Law School Research Paper 5/2016 9. DOI: https://doi.org/10.2139/ssrn.2698263.

There have been many efforts to regulate the extraterritorial collection of electronic evidence and also to enhance the co-operation between states in this connection. However, crucial problems related to jurisdiction and extraterritorial digital data collection are still unsolved. The latest attempt to address issues with extraterritorial evidence-gathering consists of the European Commission's E-Evidence Proposal[*6] coupled with the Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[*7]. These instruments are intended to simplify the procedure of requesting data from the relevant Internet service provider (hereinafter 'ISP'). In this, they represent a simplified version of traditional mutual legal assistance (referred to below as MLA also), imposing an obligation on the ISP to respond while not articulating an element of the requesting state's control (this aspect of traditional MLA is replaced with trust).

The CLOUD Act is a direct result of the so-called *Microsoft* case[*8], and discussions that were prompted by that case highlight that contemporary jurisdiction-oriented thinking has failed to address the challenges posed by the Internet adequately. Perhaps this is nowhere more evident than with regard to cloud computing in particular. Researchers have found that this failure may be blamed partially on the law's unwillingness to part with traditional categorisation schemes and equivalent thinking so as to recognise models and structures that better correspond to the new technological reality.[*9] States have begun efforts to rectify some of the problems that have arisen from cyber-territorial environments, which often involve discussions about allowing direct requests to ISPs. The latter approach still leaves critical issues unresolved, however – issues that various states face in the course of gathering data from foreign servers in the course of criminal proceedings.

Although the discussions culminating in the E-Evidence Proposal and in the CLOUD Act that followed do show that a clear shift is taking place from the concept of location-based data as the determinant for jurisdiction and movement toward acknowledgement of the data-owner's citizenship status or registered domicile as the overriding feature with regard to jurisdiction, this still represents only half of the solution, especially for those states that lack clear and transparent regulation covering extraterritorial computer-system searches. The purpose and core aim stated for the CLOUD Act is to facilitate the fight against serious crime, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime. The question is this: while the United States is making efforts to streamline the handling of requests from foreign states, what should be the response on the part of other states? Are corresponding efforts warranted, or would the CLOUD Act and instruments under the E-Evidence Proposal suffice to ensure comprehensive legal grounds for appropriate extraterritorial data-gathering?

This article constitutes an attempt to assess the effects of the above-mentioned mechanisms on states' actions in the extraterritorial collection of evidence, from the perspective particular to a state that has no regulation in place for computer-system searches or extraterritorial data-gathering.[*10] Estonia is taken as an example of a state without regulation addressing searches of computer systems. I will highlight problems that states with this approach or a similar one are left to face even if there is an agreement in force with the

6 Related material is available: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en (accessed 14 April 2020).

7 Clarifying Lawful Overseas Use of Data Act or the CLOUD Act. https://www.congress.gov/bill/115th-congress/house-bill/4943 (accessed 14 April 2020).

8 In the case *United States v Microsoft Corp.*, the US court system had to consider the circumstances under which law-enforcement agents in the United States may obtain digital information from abroad. In December 2013, the US Government served a search warrant on Microsoft under the Electronic Communications Privacy Act of 1986, or ECPA. The warrant authorised the search and seizure of information associated with a specified Web-based e-mail account that was stored on premises owned, maintained, controlled, or operated by Microsoft Corporation ('Microsoft'). The physical location of the data that the government wanted Microsoft to turn over, however, was a server in Dublin, Ireland (accessible to Microsoft employees working in Redmond, Washington). The dispute ended with the Supreme Court when, on 30 March 2018, the Department of Justice moved to drop the lawsuit as moot and Microsoft filed to agree with the motion. The Supreme Court then dropped the case. Both the government and Microsoft maintained that the newly passed CLOUD Act had rendered the lawsuit meaningless, since that act of law creates clear new procedures for obtaining legal orders for data in cross-border situations of such a nature. See the opinion summary: https://supreme.justia.com/cases/federal/us/584/17-2/ (accessed 14 April 2020).

9 D Svantesson and F Gerry, 'Access to Extraterritorial Evidence: The Microsoft Cloud Case and Beyond' (2015) 31(4) *Computer Law & Security Review* 481. DOI: https://doi.org/10.1016/j.clsr.2015.05.007.

10 The seventh round of GENVAL mutual evaluations was dedicated to the practical implementation and operation of European policies with regard to preventing and combating cybercrime. Evaluations reveal that most states lack regulation pertaining to computer-system searches and for digital data-gathering carried out extraterritorially. States have declared that in cases of evidence obtained abroad, it is necessary to follow the procedures set forth under relevant international treaties while considering the domestic code of criminal procedure or the equivalent thereof. Reports from related evaluations are available: https://www.coe.int/de/web/octopus-old2019/blog/-/blogs/17449981?_33 (accessed 28 July 2020).

US that pertains to requesting data from a foreign ISP. For the analysis, I rely on practical expertise and apply traditional legal methods such as analysis proceeding from pragmatic concerns. However, on account of confidentiality requirements, several particulars are not revealed or addressed here.

It is my contention that the CLOUD Act and E-Evidence Proposal enhance the collection of data from foreign ISPs with respect to direct requests for data. However, states that have no regulation system in place for computer-system searches are still bound to face admissibility problems in court in connection with unauthorised extraterritorial data collection.

Coping with lack of regulation extending to computer-system searches

The Estonian Code of Criminal Procedure[*11], or CCP, contains no regulation on conveying data across borders.[*12] Estonian law-enforcement agencies (hereinafter 'LEAs') see four possibilities for obtaining data from servers in foreign countries[*13]: 1) the suspect provides the material voluntarily, as is done quite often during a home search; 2) the person controlling the data (the ISP) supplies said data voluntarily in response to a request; 3) the location of the information is identified and a request for legal assistance is submitted to the corresponding state[*14]; or 4) data are collected by means of surveillance measures.[*15]

Data subjects' consent as legal grounds for data access

Estonian criminal procedure provides for an investigative measure referred to as inspection. According to the CCP (§83), the objective of an inspection is to collect information necessary for resolving the criminal matter, detect the evidentiary traces of the criminal offence, and confiscate objects that may have use as physical evidence. The object of inspection may be a scene where certain events took place, a body, a document, any other object or physical evidence, and – in the case of physical examination – the person and a relevant postal or telegraphic item. Considerable latitude for interpretation of inspection creates a large number of opportunities for the investigator.

Firstly, any object may be the object of inspection, and, for instance, the Estonian Supreme Court has found that an e-mail account is an object since it is a part of a server. Therefore, the account, as part of the server, may be inspected. The Supreme Court has adjudicated a matter wherein the main subject of dispute was whether e-mail messages held in a Google account could be seen as a 'thing'. The Court concluded that the relevant Google server itself, where the files containing the e-mail messages are stored, should be seen as the 'thing' and that, when inspecting an account on a Gmail server by utilising the username and password connected with the account in question, one is inspecting that part of the server (i.e., the portion

11 The Code of Criminal Procedure can be found at: https://www.riigiteataja.ee/en/eli/531052016001/consolide (accessed 14 April 2020).

12 See, generally: E Laurits, 'Criminal Procedure and Digital Evidence in Estonia' (2016) 13 *Digital Evidence and Electronic Signature Law Review*. DOI: https://doi.org/10.14296/deeslr.v13i0.2301; A-M Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (2016) 24(4) *International Journal of Law and Information Technology* 343. DOI: https://doi.org/10.1093/ijlit/eaw010.

13 These are described in the evaluation report on the seventh round of mutual evaluations: 'The Practical Implementation and Operation of European Policies on Prevention and Combating Cybercrime' [2016] *Report on Estonia* 36. http://data.consilium.europa.eu/doc/document/ST-10953-2015-DCL-1/en/pdf (accessed 14 April 2020).

14 This option is not discussed in the article, since the predominant opinion is that the current MLA system is not suited to meeting the requirements associated with effective co-operation between states in connection with collection of digital evidence. The MLA procedures are often slow and ineffective, irrespective of the need to obtain e-evidence rapidly for reason of its volatility.

15 For general discussion, see the final report from the seventh round of mutual evaluations: 'The Practical Implementation and Operation of the European Policies on Prevention and Combating Cybercrime' [2017]. https://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/en/pdf (accessed 14 April 2020).

where the account is)[*16]. In Estonia, inspection as a public investigative measure is conducted by the investigative body and does not require any higher authorisation (neither a prosecutor's nor a judge's).

In the hypothetical situation wherein a suspect is willing to co-operate and willingly reveal his or her Gmail, Facebook, or similar account credentials and offer assistance in the investigation, the revealing of the password and username would be considered to be the explanation for the inspection (rather than being testimony).

Data subjects'[*17] consent as sufficient legal foundation for the processing of sensitive personal data by competent authorities could prove highly problematic in light of the Data Protection Directive. The directive states that where the data subject is required to comply with a legal obligation, said data subject has no genuine, free choice and that, accordingly, the compliant reaction of the data subject could not be considered an indication of his or her wishes expressed freely.[*18]

On one hand, it is problematic to argue that the consent of the suspect or accused is genuinely free, or at least one would be taking a risk in so arguing (the presumption is that it is not). However, Article 32 b of the Budapest Convention could provide grounds for extraterritorial evidence-gathering of such a nature. On the other hand, it would be controversial to forbid or refuse freely and willingly offered help from the suspect or accused person wishing to co-operate with the LEA, since such co-operation is seen as a mitigating circumstance that would create grounds for reduced punishment under the Estonian Penal Code's Section 57.

There might exist a possibility for the LEA to conduct this investigative measure itself even when the credentials have been obtained in some other way than through their provision by the suspect or accused (in cases of surveillance activities, discovery during a home search, storage on a relevant device for automatic login or similar functions, etc.). However, it is essential to consider that such use of the username–password pair, such interference, could constitute commission of a criminal offence on the part of the LEA, under domestic and/or foreign jurisdiction, as in cases of illegal access under the Convention on Cybercrime[*19]. It should be quite clear that without the approval of the suspect, such an inspection carried out by the LEA (without the added weight of an authority such as a judge declaring a connection with a crime) would be illegal.

Searches of a computer system

One of the investigative measures provided for is 'search'. However, the search described in Estonia's CCP does not cover searching a computer system. The problem with the regulation of searches set forth in the CCP is that the provision gives a list of places that may be searched: buildings, rooms, vehicles, and enclosed areas. The list does not mention computer systems. I would suggest that the provision would be less restrictive and more up-to-date if it were not to include a list at all and instead search were defined only in terms of the objective (to find an object to be confiscated or used as physical evidence; a document, thing, or person whose discovery is necessary for resolution of the criminal matter; assets to be seized in criminal proceedings; or a body – whether a corpse or in apprehension of a fugitive). In practice, this means that if a potentially pertinent technological 'working device' is found during a search (e.g., of a house), the LEA would have to decide on inspecting that working device or creating an image of it on-site. Both of these actions are meant to guarantee the possibility of future procedural actions – namely, inspecting the storage medium. However, if 'live' inspection of the computer system or similar entity is not conducted there and then, at that

16 Judgment of the Criminal Chamber of the Supreme Court of 20.11.2015, 3-1-1-93-15, clause 92. https://www.riigikohus.ee/et/lahendid?asjaNr=3-1-1-93-15 (accessed 14 April 2020).

17 'Data subject' is defined as 'an identified or identifiable natural person [where] an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or [...] one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person', per Directive (EU) 2016/680, art 3(1).

18 Directive (EU) 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 data, and repealing Council Framework Decision 2008/977/JHA [2016] (OJ L119) s 35. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&qid=1556338292741&from=EN (accessed 14 April 2020).

19 Convention on Cybercrime (Budapest 23.XI.2001), at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (accessed 7 July 2020).

precise moment, a considerable quantity of data (what is held in RAM at the very least) and the connections established (e.g., to 'cloud' services) are bound to be lost.

Engaging in live inspection of computer systems without suspects' approval could be deemed illegal since the authorisation for a search typically does not extend to searching (inspecting) all the computer systems that are accessible from the space covered by the warrant. Judges are obviously reluctant to grant authorisation for computer-system searches. This scenario involves a weird hybrid measure wherein the LEA when carrying out one investigative measure, search, engages in another, inspection. Obviously, the following issue related to the suspect's rights rears its head also: while the person is subject to a given procedural action, such as search, a new measure arises from it wherein suspects' consent could provide grounds for several distinct legal actions.

Obtaining data through surveillance measures

This section of the paper focuses on gathering data by means of surveillance measures[*20] as another possibility for collection of data from servers on foreign soil. For these purposes, surveillance activities are defined as processing of personal data for the performance of a duty provided for by law with the objective of hiding the fact and content of the data-processing from the data subject. Such activities must follow the *ultima ratio* (last resort) principle: they are to be carried out only if collecting the data via other activities or obtaining the evidence through other procedural acts is impossible, cannot be done within the required time, or would be especially complicated or if employing other means might prejudice criminal proceedings in the case. Collection of digital data extraterritorially meets all those requirements.

The Advisory Guidelines on IT-Evidence, issued on 24 May 2016 as a co-ordinated effort of Estonian law-enforcement authorities, claim that in cases of public investigative measures (inspection or search) and covert surveillance, no request for legal assistance is needed with regard to data stored 'in the cloud' on foreign states' servers. The reason cited is that the action (i.e., copying of the relevant data) is performed in the territory of Estonia by an Estonian body conducting proceedings and the data can be received without anyone physically leaving the territory of Estonia. Accordingly, the guidelines state that Estonia has jurisdiction to copy the data.[*21]

The main argument seems to be that the actual location of the data (the material being copied) is not particularly relevant as long as the procedure itself is carried out within Estonian jurisdiction. In cases involving surveillance, further authorisation is needed either from the prosecutor (in cases of covert examination of a thing) or from a judge (for all other measures prescribed by law). The distinguishing properties of inspection are that, firstly, it is conducted in secret from the subject and, secondly, it requires higher authorisation. As for jurisdiction, one could argue that it is fundamentally of no importance, since the actions undertaken are the same wherever the data may be housed: the inspection of someone's account.

The foregoing argument seems to run counter to prevailing opinion. Obviously, it manifests seeking justification for the claim that all the measures involved are conducted within the territory of Estonia. Although the latter is highly debatable from a technical standpoint, one can see the reasoning behind it: is there really any difference for the data subject when the data are collected via surveillance measures in Estonia as opposed to under an information request whereby the data are handed over or otherwise made available by, for example, a US-based ISP? I would claim that the answer is indeed 'no'. Collecting data from a digital account is considered covert inspection under the definitions applied in Estonian legislation and case law. Therefore, it requires a prosecutor's authorisation. If this measure involves accessing a computer system, authorisation from a judge too is needed. In essence, both authorisations are needed, as there is no other way to collect data from a foreign server apart from by accessing a computer system. Once the matter of authorisation is settled, the critical issue of jurisdiction remains. In this connection, the reasoning behind the argument presented above might be that Estonia has jurisdiction because the crime under investigation is subject to Estonian criminal jurisdiction and that access to the data could be achieved via the Internet

[20] CCP s 126^1 and the following provisions set in place the regulation for surveillance activities. In cybercrime investigations and for the collection of digital evidence, covert examination (s 126^5) and covert observation or examination of wire-tapping information (s 126^7) are the most commonly undertaken surveillance activities. For the former, the prosecutor grants authorisation, and judges' authorisation is needed for the latter.

[21] Per material in the author's possession: 'The Advisory Guidelines on IT-Evidence' [2016].

without any recourse to involving foreign authorities. After all, if the location of the data is largely irrelevant for the data subject, why should it pose an unimaginably difficult jurisdictional puzzle for the LEA?

The CLOUD Act and E-Evidence Proposal as a solution to MLA challenges

The CLOUD Act and E-Evidence Proposal lay the grounds for states to directly contact the relevant foreign service provider. Attention should be drawn to the fact that these instruments are foreseen not as giving any additional rights to foreign LEAs to collect data themselves (e.g., via surveillance measures as in the Estonian example) so much as introducing a fast-track form of MLA.

The United States CLOUD Act was adopted by the US Congress on 23 March 2018. Following from *Microsoft*, the CLOUD Act has two essential aspects. Its Part I clarifies the reach of US law enforcement to access data held extraterritorially by US-based providers. Part II authorises the executive branch of government to enter into agreements with foreign governments pursuant to which those foreign governments may bypass the otherwise applicable mutual legal assistance requirements in specified circumstances and in accordance with baseline substantive and procedural requirements. Recertification of partner nations' fulfilment of the agreement conditions is to take place every five years[*22]. The scope of the CLOUD Act's data coverage is delineated as encompassing both stored data and interception of wire or electronic communication, while the offences covered are 'serious crimes'.[*23]

With the above-mentioned agreements in place, foreign governments may issue wiretap orders or request stored data where the target persons are not located in the US or US citizens / legal permanent residents, regardless of where the data in question are located.[*24] To access data of US citizens or legal permanent residents and others within the US, the foreign government must continue to employ the process set forth in the mutual legal assistance treaty. The key difference from the *status quo* is connected with the common-sense notion, grounded in principles of democratic accountability, that governments have an interest in setting standards and rules regarding access to their own citizens' and residents' data. They seldom have a similar interest in setting rules regulating and moderating foreign governments' access to foreigners' data.[*25]

Non-US parties would be expected to find partnership under a CLOUD-Act-based agreement especially beneficial with regard to obtaining the data requested; in the absence of such an agreement, there might be very little chance of receiving any content data (as opposed to metadata), on account of procedural factors and the like. The agreements foreseen by the CLOUD Act render it possible even to utilise real-time interception mechanisms as long as the investigation is related to 'transnational domestic crime'. For example, in cases in which the data needed by Estonia for criminal proceedings must be provided by a US-based ISP, being a party to such an agreement would simplify the proceedings significantly. Gaining access to a suspect's computer system is a huge challenge, and having this sort of agreement with the US would greatly simplify the work of the LEA. However, this is just a technical benefit. From the perspective of the Estonian data subjects' rights, nothing changes: the same judicial control applies as would when an Estonian LEA is conducting the surveillance measures.

It is yet to be seen how CLOUD-Act-based agreements will be handled with regard to the EU. Would there be a framework agreement? That would be extremely difficult to achieve, given the multitude of opinions within and among EU member states on the E-Evidence Proposal. Are individual Member States tempted to enter into their own agreements of the sort the UK has[*26]? Discussions of the E-Evidence Proposal already show a rocky start to efforts to establish common ground, and the pace is slow.

22 Clarifying Lawful Overseas Use of Data Act, §105(e). https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf (accessed 14 April 2020).

23 *Ibid*, §2(1).

24 See, generally, J Daskal, 'Setting the Record Straight: The CLOUD Act and the Reach of Wiretapping Authority under US law [2018]. https://www.crossborderdataforum.org/setting-the-record-straight-the-cloud-act-and-the-reach-of-wiretapping-authority-under-us-law/?cn-reloaded=1 (accessed 14 April 2020).

25 J Daskal, 'Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0' (2018) 71 *Stanford Law Review* 6. https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/ (accessed 14 April 2020).

26 Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crimes (3 October 2019).

Let us examine the proposal more closely. In April 2018, the European Commission tabled it as two proposals (one for a regulation and one for a directive) that together would establish a legal framework that renders it easier and faster for police and judicial authorities to obtain and secure access to electronic evidence in cross-border cases. Under the proposed terms, law-enforcement authorities in any of the EU member states would be allowed to force providers such as Facebook or Google to hand over the user's personal data even if the provider is based in a different country. The proposal and, even more so, the Council's draft entrust the mission of protecting human rights almost solely to the issuing authority and are, therefore, clearly rooted in mutual trust, in that the involvement of authorities in the executing state is, in principle, avoided – the orders pass directly from the issuing body in one Member State to the service provider in another Member State. The scope of the operations proposed is limited to stored data (both content and non-content data) and does not extend to real-time interception.*[27] In the latter, the proposal is in sharp contrast with the CLOUD Act, which, in allowing real-time interception (albeit subject to the rules specified in the act), conveys the idea that we trust each partner's judicial system and leave the evaluation entirely up to them. That said, since these instruments are articulated as for fighting serious crime, it could be difficult to reach said objective in the absence of an opportunity to use real-time information.

Both the CLOUD Act and the E-Evidence Proposal manifest the principle of mutual trust, in that the only judiciary-level control shall be by the requesting state. This creates obvious hurdles with regard to notification, data subjects' rights, and principles related to guaranteeing a fair trial, but it certainly expedites the collection of data from a foreign ISP. The main idea is that the judiciary's control should rest with the requesting state and that said state should be accountable for the lawfulness of the request. Neither the proposal on e-evidence nor the CLOUD Act is going to change the presumption of territorial jurisdiction – under these instruments, the participating states are just agreeing to trust each other's judicial system and are streamlining requests that would normally be subject to other procedural norms. Under these instruments, requesting states still are not granted a right to exercise their ability to collect data themselves without having asked.

Concluding discussion

Data collection is an urgent issue today, and the options offered under the CLOUD Act seem to mark the end to a long wait for many states (one exception being the UK, which has already entered into an agreement with the US). For the time being, the Estonian standpoint in a nutshell is this: the data are not seized but copied (not an uncomplicated issue and one best examined elsewhere), and the actions (copying) are carried out in Estonia, in accordance with Estonian legal norms; therefore, Estonia has jurisdiction. Although interpretations of this nature have received criticism ever since the *Gorshkov and Ivanov* case*[28], indications of domestic courts allowing such self-authorised digital data collection are rising. One example is the Danish Supreme Court's reasoning whereby the crime with which the accused is charged is subject to Danish criminal jurisdiction. If the matter is under investigation by Danish authorities and if the relevant interventions can be implemented without involving foreign authorities (on Danish territory), Denmark has jurisdiction.*[29] In those circumstances in which it is technically possible for the investigating state to gather the data, where the quantities of data so allow, the preferred method should be 'self-help' that may take the form of surveillance activities subject to the control of local judicial authorities.

https://www.justice.gov/ag/page/file/1207496/download#Agreement%20between%20the%20Government%20of%20the%20United%20States%20of%20America%20and%20the%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland%20on%20Access%20to%20Electronic%20Data%20for%20the%20Purpose%20of%20Countering%20Serious%20Crimes (accessed 14 April 2020).

27 Article 2 (7–10) of the proposed E-Evidence Regulation distinguishes among four types of data: (i) subscriber data, (ii) access data (related to the commencement and termination of a user access to a service, (iii) transaction data (context or additional information about the service, such as data on the location of the device used to access the service), and (iv) content data (any data stored in digital form – text, voice, videos, images, sound, etc.).

28 *United States v Ivanov* [2001] 300CR00183AWT, case brief. https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/2001/united_states_v._ivanov.html?lng=en&tmpl=sherloc (accessed 14 April 2020).

29 Case translation: Denmark. U 2012.2614 H (10 May 2012). See the commentary by Professor Lars Bo Langsted (2013) 10 *Digital Evidence and Electronic Signature Law Review* 162. https://journals.sas.ac.uk/deeslr/article/view/2038/1975 (accessed 14 April 2020).

As the Estonian example illustrates, the level of judicial control over digital data collection is remarkably high when access to a computer system is involved, with such actions necessitating judges' authorisation. Estonia's regulation of surveillance measures is strict, and both the *ultima ratio* condition must be met and the crime investigated has to be serious enough to warrant the measures[*30]. It seems that since *Gorshkov and Ivanov*, states have grown more willing to admit – and domestic courts readier to go along with – reasoning whereby digital data collection should be possible without the need for *pro forma* help from another state. Of course, such actions may be necessary in part because advanced technical knowledge cannot and should not be expected. For instance, should the agents involved have to know that, even though the copying of digital data is performed in Estonia, the data undergoing the copying are still retrieved from a foreign server? Likewise, should lawyers really need to possess such in-depth knowledge of technology that they can (and do) determine where exactly the copying action is completed, and should this determine jurisdiction? Does one really have to go so far with the demand for understanding of the reality of a given case that knowing which jurisdiction and legal norms are applicable would necessitate lawyers consulting IT experts case-specifically?

First of all, there should be a shift in our understanding of data and in how legal norms are applied on that basis. When applying the law, those involved in the relevant processes are still drawing parallels with physical things. This can be seen in the reasoning behind the Estonian Supreme Court's decision that part of a server was being inspected, not the piece of data itself. It seems to be very difficult to see the digital network as 'space' rather than as 'place'. For digital data to be transformed into a human-readable form, there must be a 'place', a storage medium. If digital data could be understood without reference to a storage medium, would different solutions result? If it were possible to pick up the pieces of information in transit and put them together in some other way, would the legal norms have to be changed again? Or the concept behind them? Also, the same digital data might be stored by a given user on multiple systems, which could be in different jurisdictions (as in the case of using two 'cloud' service providers for redundancy). The diversity that is created by the non-territorial nature of data is leading to confusing legal decisions, in the course of which the data subjects' rights might end up protected even less than they would if the rights offered by the investigating state were honoured by all parties in all cases.

By passing the CLOUD Act, the US has already declared that, when certain criteria are met, democratic states are eligible to receive the data they request. Allowing or tolerating 'self-help' for data in the same categories should be likewise legally accepted, in light of the fact that, in reality, it is no longer important where the data are, in contrast against the nationality and location of the data-holder. Again, it is worth remembering that governments have an interest in setting standards and rules regarding access to their own citizens' and residents' data while they do not have an equivalent interest in setting rules pertaining to foreign governments accessing foreigners' data.

For European Union countries, one of the options would be to define the rules for extraterritorial evidence-gathering in national laws and let the relevant disputes be addressed at national level: as courts start issuing decisions, states will begin finding it easier to form legal interpretations. The greatest benefit in this would lie in having transparent, precise requirements, which should be coupled with an explicit requirement to notify (or receive consent from) the foreign government in question (when this information is known). Today, in contrast, many states lack regulation of e-evidence collection and are simply waiting for this field to be regulated at a higher level. This could well result in rigid norms and excessively slow movement or in undesirable regulation, since, for instance, negotiations involve too many parties (data-retention disputes serve as a case in point). There should exist a possibility of legally using digital data that, for reason of the digital data's non-territoriality, are gathered extraterritorially. However, the conditions for said use should be abundantly clear.

The above-mentioned reluctance to tackle this complicated issue is evident in Estonia also. Therefore, it is worthy of note (though not surprising) that neither the circuit court system nor the Supreme Court[*31] raised the issue of jurisdiction when given the opportunity. One of the issues in the case in question was covert examination of a server of a foreign private company located in a foreign territory – an issue that definitely requires legal analysis. I am aware that the courts did not have an obligation to say anything on that subject, as the question of jurisdiction was never really raised, since it was not a governmental entity

30 The CCP's §126-1 sets the general conditions for conduct of surveillance activities, and §126[2]'s Subsection 2 enumerates the list of crimes in the event of which surveillance activities are allowed.

31 Judgment of the Criminal Chamber of the Supreme Court of 20.11.2015, 3-1-1-93-15.

collecting digital data from the foreign computer system. However, the Supreme Court has, on numerous occasions, exercised its powers of making statements on important issues in the form of *obiter dictum*. Hence, the silence on the matter was interpreted as acceptance of the 'copying' argument, with the Advisory Guidelines on IT-Evidence for LEAs getting prepared in the wake of that decision.

The critical issue for Estonia and states that are lacking in computer-system search regulations is that there is no justification for such actions to be found in the international agreements in place, and neither is justification offered in domestic rules. In this light, the silence of the Estonian Supreme Court might be intentional and does not necessarily imply the Supreme Court's acceptance of such interpretations of jurisdiction. It might also mean that the Supreme Court leaves this issue for the legislator to regulate. In fact, the latter is much more likely.

It can be concluded that European countries are a far cry from clarity on the subject, and in the absence of national rules, clarity will never come about. It remains to be seen whether EU members can agree at all on joint principles (even when real-time interception is not under consideration). Inevitably, the slow and uncertain movement toward regulating requests for data from foreign ISPs leads to states using alternative methods, as seen in the Estonian example. Because the debate about how cyberspace should be regulated is highly politicised, one should not be surprised that states are actively pushing for norms and legal interpretations that coincide with their strategic and ideological preferences. Since legal environments can differ significantly between states, the wait for a solution might be a long one indeed. The discussion surrounding the E-Evidence Proposal has already shown clear signs of this.

In the future, when the EU has a suitable agreement in place with the US, it should be simpler for an LEA to obtain the necessary content data, since it would not have to access computer systems itself and would receive the data by merely making a request. States such as Estonia, which do not have any legal norms for extraterritorial data-gathering or computer-system searches at present, are going to continue facing problems when data are needed anywhere other than from a US or European ISP or when data are collected via methods (e.g., surveillance measures) that do not involve recourse to assistance, since no justification is provided for such extraterritorial digital data collection. The CLOUD Act should be a clear sign of new thinking – the state with the world's largest ISPs is declaring that location is not the centre of gravity in digital data collection; rather, the citizenship of the data-owner is the deciding factor. This should supply encouragement to start thinking in a manner that acknowledges the data's non-territoriality and should be a nudge for states such as Estonia.