DISSERTATIONES
IURIDICAE
UNIVERSITATIS
TARTUENSIS
63

ANNA-MARIA OSULA

Remote search and seizure of extraterritorial data

DISSERTATIONES IURIDICAE UNIVERSITATIS TARTUENSIS
63

DISSERTATIONES IURIDICAE UNIVERSITATIS TARTUENSIS
63

ANNA-MARIA OSULA

Remote search and seizure of extraterritorial data

UNIVERSITY OF TARTU
Press

School of Law, University of Tartu, Estonia

Dissertation is accepted for the commencement of the degree of Doctor of Philosophy (PhD) in law on February 20, 2017, by the Council of the School of Law.

Supervisor: Prof Jaan Ginter (University of Tartu)

Opponents: Dr Christoffer Wong (Lund University)

Commencement will take place on April 17, 2017 at 12.00 in the Faculty of Law, Näituse 20 room K-03.

Publication of this dissertation is supported by the School of Law, University of Tartu.

ISSN 1406-6394
ISBN 978-9949-77-363-3 (print)
ISBN 978-9949-77-364-0 (pdf)

University of Tartu Press
www.tyk.ee

TABLE OF CONTENTS

LIST OF ORIGINAL PUBLICATIONS

This dissertation is based on the following publications:

1. Osula, Anna-Maria (2015). Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data. Masaryk University Journal of Law and Technology, Vol 9, 43–64.
2. Osula, Anna-Maria (2015). Transborder Access and Territorial Sovereignty. Computer Law and Security Review, 31 (6), 719–735.
3. Minárik, Tomas; Osula, Anna-Maria (2016). Tor Does Not Stink: Use and Abuse of the Tor Anonymity Network from the Perspective of Law. Computer Law and Security Review, 32 (1), 111–127.
4. Velasco, Cristos; Hörnle, Julia; Osula, Anna-Maria (2016). Global Views on Internet Jurisdiction and Trans-Border Access. In: Gutwirth, Serge; Leenes, Ronald; De Hert, Paul (Ed.). Data Protection on the Move (465–476). Springer Netherlands. Law, Governance and Technology Series, 24.
5. Osula, Anna-Maria (2016). Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study. International Journal of Law and Information Technology, 24 (4), 343–373.

ANALYTICAL COMPENDIUM TO A CUMULATIVE DISSERTATION

I INTRODUCTION

1.1. Defining the research problem, its relevance and the current status of research in the area

Today, more than three billion users have access to the Internet,[1] and by 2020 the number of networked devices (the 'Internet of Things') will outnumber people by six to one.[2] This new digital reality exemplifies that current and future criminal investigations will have to take into account the unique characteristics of the Internet as well as evidence either stored on or transmitted via electronic devices. In the increasingly sophisticated realm of cybercrime, additional challenges related to accessing and employing digital evidence[3] in court arise since most offences involve actors, actions, or substantial effects that are wholly or in some part located or have been carried out in different jurisdictions,[4] and thereby, relevant evidence may not always be located on domestic territory.

For example, it is not uncommon for criminals to infect hundreds of thousands of computers worldwide as part of a malicious botnet. In such cases, the investigation would require the assistance of both industry and law enforcement (LE) partners from all over the world.[5] To make things even more complicated, due to the distributed nature of cyberspace the targeted evidence may be residing in multiple jurisdictions at once or it may be impossible to identify the location at all at a given time (also known as 'loss of location').[6] This may

---

1 International Telecommunication Union, 'ICT Facts and Figures 2016' (2016) <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf> (last accessed 4 January 2017).

2 United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime' (2013) xvii <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> (last accessed 4 January 2017).

3 This dissertation uses 'digital evidence' as a synonym for 'electronic evidence' referring to all '[evidence] that exists in electronic, or digital, form'. ibid xxiii.

4 E.g. according to the UN cybercrime study entailing the answers of 69 countries all over the world, 'more than half of responding countries /…/ reported that between 50 and 100 per cent of cybercrime acts encountered by the police involve a transnational element.' ibid 5.

5 E.g. the recent Zeus 'Gameover' botnet infected 500,000–1,000,000 computers worldwide, and its investigation included private industry experts and LE counterparts in more than 10 countries. United States Department of Justice, 'U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator' (2 June 2014) <https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware> (last accessed 4 January 2017).

6 'Loss of location' refers to a situation where it is not possible to identify the location of the data. See more at, e.g. Jan Spoenle, 'Cloud Computing and Cybercrime Investigations: Territoriality vs. the Power of Disposal?' (CoE 2010) Discussion paper <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df> (last

easily occur in cloud computing where, in order to provide the user with seamless interaction between multiple applications and services, different applications and servers across various locations are used at the same time and consequently, the identification of the location of certain data, or even data itself in cloud computing is more complex as data could be spread out across these applications and servers.[7] Another well-known option for concealing one's identity and geographical location is the use of the Tor network which allows its users to redirect their traffic through a distributed network of relays acting as proxy servers provided by a group of globally spread volunteers. Despite governments' alleged efforts to control or disable Tor, the software is freely available to criminals[8] and ordinary citizens alike and boasts over one and a half million users daily.[9]

Both previously mentioned conditions – the possibly extraterritorially located data and the inability to identify the exact location of the data – raise questions regarding the ability as well as the legal limits of LE's extraterritorial access to such data.

Naturally, the need for evidence in other jurisdictions is not new in itself. Usually, the exchange of evidence and other information in criminal and related matters is based on Mutual Legal Assistance (MLA). In the context of accessing extraterritorially located data, requests for mutual assistance are, in conjunction with relevant national legislation, mostly based on bi-lateral MLA treaties (MLATs), multilateral agreements such as the Council of Europe (CoE) Convention on Cybercrime (CoCC)[10], European Convention on Mutual Legal

---

accessed 4 January 2017); Joseph J Schwerha IV, 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"' (2010) Council of Europe Project on Cybercrime <https://rm.coe.int/CoERMPublic Common SearchServices/DisplayDCTMContent?documentId=09000016802fa3dc> (last accessed 4 January 2017). See also 'loss of knowledge of location' in Koops, B-J and Goodwin, M, 'Cyberspace, the Cloud, and Cross-Border Criminal Investigation' (2014) Tilburg Law School Research Paper 5/2016 9 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263> (last accessed 4 January 2017).

7 Mark Taylor and others, 'Forensic Investigation of Cloud Computing Systems' (2011) 2011 Network Security 4, 7.

8 Apart from being used as a tool bypassing censorship and protecting privacy in many countries, examples of criminal uses of Tor include the infamous Silk Road hidden service marketplace that was used for trading illegal drugs, prohibited weapons and even hiring assassins. Read more e.g. at Sam Thielman, 'Silk Road Operator Ross Ulbricht Sentenced to Life in Prison' *Guardian* (29 May 2015) <https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced> (last accessed 4 January 2017); Tomáš Minárik and Anna-Maria Osula, 'Tor Does Not Stink: Use and Abuse of the Tor Anonymity Network from the Perspective of Law' (2016) 32 Computer Law & Security Review 111, 1–2.

9 Tor Project, 'Tor Metrics – Direct Users by Country' <https://metrics.torproject.org/userstats-relay-country.html> (last accessed 4 January 2017). Read more generally at: Emin Çalışkan, Tomáš Minárik and Anna-Maria Osula, 'Technical and Legal Overview of the Tor Anonymity Network' <https://ccdcoe.org/sites/default/files/multimedia/pdf/TOR_Anonymity_Network.pdf> (last accessed 4 January 2017); Minárik and Osula (n 8).

10 Council of Europe, Convention on Cybercrime, ETS No. 185, RT II 2003, 9, 32 2001.

Assistance in Criminal Matters and other CoE treaties, United Nations (UN) and other international treaties, or reciprocity.[11]

According to a UN survey, approximately 70% of the respondents' currently employed means of international cooperation in cybercrime investigations are based on MLA mechanisms.[12] However, recent studies have indicated that these traditional means for accessing extraterritorial data may not satisfy modern criminal procedures in terms of time efficiency as it may take months for the extraterritorial evidence to reach the requesting state, and therefore these mechanisms are considered 'too complex, lengthy and resource intensive' and thus often abandoned.[13] One of the biggest flaws appears to be the lack of a uniform approach. This means that the content of and conditions for submitting as well as responding to the requests depend on the precise cooperation framework to be employed and the countries to be involved.[14] For instance, some countries may require the MLA request to be sent to a central authorising authority such as the Ministry of Justice, whereas others may allow these requests to be forwarded directly to relevant national authorities, or other channels such as International Criminal Police Organisation (Interpol) may be used.[15] Also, the national bodies that have the mandate to authorise, in response to a received MLA request, domestic access to stored computer data may vary according to the type of data to be accessed (such as subscriber data, traffic data or content data).[16] In some countries only the material received via the MLA mechanisms, as opposed to data obtained via alternative channels, can be used as evidence in court.[17] In others, domestic legislation offers more flexibility and

---

[11] Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (Cybercrime Convention Committee (T-CY) 2014) T-CY(2013)17rev 31 <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf> (last accessed 4 January 2017); Anna-Maria Osula, 'Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data' (2015) Vol 9 Masaryk University Journal of Law and Technology 43, 46–50.

[12] United Nations Office on Drugs and Crime (n 2) 201.

[13] For a comprehensive overview, see e.g. Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (n 11).

[14] ibid 31; Osula, 'Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data' (n 11) 3.

[15] Some countries also provide for more expedited procedures such as 'in cases of urgency, a request for assistance submitted through the International Criminal Police Organisation (Interpol) or a notice in the Schengen Information System may be complied with before the request for assistance is received by the Ministry of Justice with the consent of the Office of the Prosecutor General.' Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (n 11) 38; Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (RT I 2003, 27, 166; RT I, 20.05.2016, 7) 462.

[16] Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (n 11) 31–33.

[17] ibid 7.

requires accessing only certain types of data (such as content data) through a formal MLA request.[18] There are also examples of countries that do not put forward a detailed regulatory framework and only require the evidence to be gathered in accordance with the legislation of the other state and not to be in conflict with the principles of domestic criminal procedure.[19]

Additional challenges related to the use of MLA procedures for accessing extraterritorial data may include circumstances such as where MLATs do not cover the necessary investigative measures, MLATs have not been signed between these countries, the other state is simply uncooperative or where it is impossible to identify the location or the jurisdiction of the data altogether.[20] Further problems related to MLATs include refusals to cooperate on 'small' offences, lack of information from the requested country about the receipt or the status of the request, problems with the content of the requests (too broad, unclear criteria for urgent requests, problems with language, terminology) and differences in legal systems.[21] Indeed, in a recent case of *United States v. Microsoft Corporation* the appellant, Microsoft, claimed that instead of the search warrant being directed at Microsoft because it was headquartered in the United States (US), the US should have sent an MLA request to Ireland since the data was stored there in its servers. In response, the US Government argued that: '/.../ Microsoft's rosy view of the efficacy of the MLAT process bears little resemblance to reality. /.../ [A]n MLAT request typically takes months to process, with the turnaround time varying widely based on the foreign country's willingness to cooperate, the LE resources it has to spare for outside requests for assistance, and the procedural idiosyncrasies of the country's legal system. /…/ Moreover, there are many countries in the world that do not even have MLATs with the United States. /…/ [I]t is even conceivable that a provider could establish server locations at sea or otherwise beyond the territorial jurisdiction of any nation.'[22]

It is therefore understandable that states are looking for alternative ways to obtain extraterritorial evidence. Options for this include formal or informal cooperation between different countries' LE, establishing or maintaining national 24/7 point of contact networks, sending requests directly to third parties such as service providers (SPs), accessing data publicly available and undertaking

---

18 ibid.

19 Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (n 15) 65(1).

20 New Zealand and Law Commission, *Search and Surveillance Powers* (Law Commission 2007) 226 <http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R97.pdf> (last accessed 4 January 2017). MLA has also been compared to 'message in a bottle' – once you send it out, you never know who receives it or whether you will get a reply. 'Interview with Ms Imbi Markus, Estonian Ministry of Justice' (14 May 2015).

21 Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (n 11) 39–40.

22 Government's Brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within its Custody and Control, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp*., 13 Mag. 2814 WL 1661004 (S.D.N.Y. 2014) 25–26.

investigative measures (such as remote search and seizure, or others) to directly access the data notwithstanding its location or if the location cannot be identified. Regional organisations such as the European Union (EU) and the CoE have also introduced specific investigative measures to be transposed by its Member States or the Parties to its conventions such as the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (hereafter Directive on the European Investigation Order)[23] and the mutual assistance clauses in CoCC (in addition to other applicable CoE instruments). These alternative options will be further examined in Section 2.1.

Generally, countries may employ a number of technological tools that enable LE to collect data remotely from computer systems.[24] This dissertation is limited to the legal regulation of one of the most common investigative measures undertaken to collect digital evidence – search and seizure; and in particular, to the regulation of remote search and seizure of data not stored domestically. Given the legal ambiguity of the different quasi-legal terms found in literature, a few remarks on terminology are in order. Traditionally, the investigative measure 'search and seizure' (or 'search' as used in the Estonian Code of Criminal Procedure (hereafter CoCP))[25] signifies a coercive power used for accessing, copying, and seizing data stored in domestically located devices situated on the premises specified in a search warrant. The focus of this dissertation – remote search and seizure – entails searches that are either carried out by extending the initial search and seizure to devices accessible from the originally searched device or by remotely conducting search and seizure from other (such as the LE's own) devices.[26] Both of these approaches to remote search and seizure have been reported to be used in practice by investigators notwithstanding whether the physical location of the data is known or not.[27] An almost synonymous term

---

23 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters (OJ L 130, 1.5.2014).

24 United Nations Office on Drugs and Crime (n 2) 131.

25 Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (n 15) 91.

26 For example, reportedly, at least 36 countries have acquired surveillance software dubbed as 'FinFisher' which after infecting the target computer allows the user to record and access, e.g. keystroke data, screen recordings, Skype calls, connected USB drives, etc. Read more at Morgan Marquis-Boire and others, 'For Their Eyes Only: The Commercialization of Digital Spying' (2013) <https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf> (last accessed 4 January 2017); Wikileaks, 'SpyFiles 4' (2014) <https://wikileaks.org/spyfiles4/index.html> (last accessed 4 January 2017). Notwithstanding whether such software is employed under the search and seizure or surveillance domestic legislation, questions regarding the legality and conditions of transborder access to data still remain.

27 United Nations Office on Drugs and Crime (n 2) 216. Likewise, a CoE study suggests that LE of many states carry out transborder searches but that conditions and practices differ. For an overview of state practice, see also Council of Europe, 'Transborder Access and Jurisdiction: What Are the Options?' (Cybercrime Convention Committee (T-CY) 2012) 29–31 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8> (last accessed 4 January 2017).

'transborder access' has been coined by the CoCC Article 32(b) that signifies, based on the consent of a 'lawful authority', unilateral access (i.e., accessing, copying, seizing) to computer data stored in another Party's jurisdiction without previously seeking specific mutual assistance. Hence, CoCC's 'transborder access' may include search and seizure powers as well as other investigative measures. This dissertation employs the term 'transborder access' when discussing CoCC but prefers 'remote search and seizure' in the context of domestic procedural law.[28]

Remote search and seizure, and in particular, the difficulties in identifying the location of the data that is the object of the search, raise several legal issues both nationally and internationally. At the national level, the legislators should ensure that traditional search and seizure frameworks support the needs of modern criminal investigations that rely more and more on digital evidence. This includes addressing various challenges related to digital forensics, procedural effectiveness, legislative clarity and legal safeguards as well as specialised training for LE and judicial officers.[29] Given the increasing need to access data not stored domestically, domestic legal frameworks should be clear about the conditions and limits of remote search and seizure. If not regulated by law, or done so in an obscure manner, more uncertainty will be generated not only in respect of the application of investigative measures domestically, which may result in the routine breaching of rights and freedoms of individuals (such as privacy, secrecy of communication, right to a fair trial), but also regarding the legality of such state behaviour in general.[30] Examples of national law addressing remote search and seizure will be further examined in Sections 2.2 and 2.3.

Internationally, the legality of remote search and seizure of data not stored domestically should be analysed together with the accepted scope of jurisdiction to enforce, and territorial sovereignty. Despite these issues having been discussed by scholars and policy-makers for almost two decades, the legitimacy

---

[28] See, e.g. Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press 2007) 319; Council of Europe, 'T-CY Guidance Note #3: Transborder Access to Data (Article 32)' (Cybercrime Convention Committee (T-CY) 2014) T-CY (2013)7 E <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY (2013)7REV_GN3_transborder_V12adopted.pdf>; Anna-Maria Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (2016) 24 (4) International Journal of Law and Information Technology 343, 351.

[29] See for example, Orin S Kerr, 'Searches and Seizures in a Digital World' [2005] 119 Harvard Law Review 531; and about challenges in general, Orin S Kerr, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3rd Edition, Office of Legal Education Executive Office for United States Attorneys 2009) <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf> (last accessed 4 January 2017).

[30] Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 5.

of such searches under international law has not been universally agreed upon.[31] Commonly, the jurisdiction to take executive or judicial action in pursuance of laws and decisions is known as jurisdiction to enforce[32] and is normally seen to include LE activities such as investigation.[33] According to the Lotus Principle, no state may 'exercise its power in any form in the territory of another State' unless based on a permissive rule derived from international custom or from a convention.[34] Without basis under international law or consent for exercising its power on foreign territory, such actions would constitute a breach of international law such as a violation of sovereignty.[35] However, what are the limits of jurisdiction to enforce in regard to state activities in cyberspace?[36]

Imagine a situation where LE locates during a search and seizure of a house the suspect's computer, turned on with full and open access to the suspect's data (and it is critically important to access that data as soon as possible). What are the legal limits of the activities of the investigators if it is clear that the data is not stored in the suspect's desktop computer but in servers located in foreign territories? Does the fact that carrying out remote search and seizure does not require the state agents to leave their own territory have any legal weight? Or would territorial sovereignty of any state be breached at all if the accessed data were to be stored on a cloud and the exact location therefore difficult to determine?[37]

---

31 Examples of earlier scholarship include Jack Goldsmith, 'The Internet and the Legitimacy of Remote Cross-Border Searches' [2001] University of Chicago Law School, Chicago Unbound <http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1316&context=public_law_and_legal_theory> (last accessed 4 January 2017); Patricia L Bellia, 'Chasing Bits across Borders' [2001] U. Chi. Legal F. 35; Stewart M Young, 'Verdugo in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases' (Social Science Research Network 2004) SSRN Scholarly Paper ID 539942 <http://papers.ssrn.com/abstract=539942> (last accessed 4 January 2017); European Committee on Crime Problems and Council of Europe, *Computer-Related Crime: Recommendation No. R. (89) 9 on Computer-Related Crime and Final Report of the European Committee on Crime Problems* (Council of Europe, Pub and Documentation Service; Manhattan Pub Co 1990). More recently, CoE has investigated the issue in greater detail, see e.g. Council of Europe, 'Transborder Access and Jurisdiction: What Are the Options?' (n 10).

32 See generally, e.g. Malcolm N Shaw, *International Law* (Cambridge University Press 2008) 650–651; Antonio Cassese, *International Law* (Second Edition, Oxford University Press 2005) 49–50.

33 See also a proposal for separate 'investigative' jurisdiction at Dan Svantesson, 'Preliminary Report: Law Enforcement Cross-Border Access to Data' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2874238 6–8
<https://papers.ssrn.com/abstract=2874238> (last accessed 4 January 2017).

34 *The Case of the SS Lotus, Fr v Turk, 1927 PCIJ (ser A) No 10 (Decision No 9)* (Permanent Court of International Justice) [45].

35 Lassa FL Oppenheim, *Oppenheim's International Law* (9th Edition, Longman 1996) 385.

36 Anna-Maria Osula, 'Transborder Access and Territorial Sovereignty' (2015) 31 Computer Law & Security Review 719, 722.

37 ibid 720, 723.

International law is unclear about the regulation of accessing extraterritorially located data during an investigation. CoCC is the only international treaty specifically focusing on cybercrime. Although the CoE has attempted to regulate investigative measures such as remote search and seizure in CoCC Article 19 ('Search and seizure of stored computer data') and Article 32 ('Transborder access to stored computer data with consent or where publicly available'), an agreement between the Parties on the details of the extraterritorial application of these measures has not been reached.

Therefore, this dissertation focuses on the difficulties in regulating LE's time-critical access to evidence which is not stored domestically, while keeping in mind the requirements deriving from both national and international law as well as paying attention to the dissonance between actual practice and the current regulation. This research area is very relevant, since it touches upon the legal limits of an increasing number of investigations that need to make use of digital evidence not stored on domestic territory and demonstrates a wider need to review the procedures for the search and seizure of traditionally tangible items. These questions are increasingly receiving more consideration from scholars and practitioners alike but since little information is available about actual state practice, the already proposed academic and policy arguments have not been developed further or received wider international support. Apart from the CoE's work and the newly adopted EU documents, no other international organisations have tackled the issues related to the extraterritorial scope of search and seizure in detail. Also, the examples of domestic regulation examined in this dissertation do not reflect a standardised approach but rather illustrate different solutions to the same issues.

The research undertaken for this dissertation has been designed to complement the already existing scholarship as certain questions addressed here have been discussed by other authors only to limited extent. The conclusions of the articles that form the foundation of this compendium will hopefully have practical value to any legislator reviewing its criminal procedure regulation and the extraterritorial scope of domestic remote search and seizure provisions. In addition to assisting legislators in domestic reviews, the conclusions of the dissertation should also support the complicated process of moving towards a common understanding regarding the necessity and practicality of a multilateral or perhaps even global agreement on the scope and conditions of remote search and seizure of extraterritorial data.

1.2. Defining the objective of the research and research questions

The **objective** of the dissertation is to examine, building on the example of CoCC, the regulation of remote search and seizure in circumstances where the targeted evidence is extraterritorially located or where it is not possible to identify the exact location of the data. In addition to discussing the legality of

the possibly extraterritorial reach of remote search and seizure under international law, the dissertation will analyse CoCC Article 19(2) and Article 32(b) in light of the Estonian criminal procedure regulation, offer a comparative view on selected European countries' domestic approaches and analyse whether and how the current domestic regulation should be updated in order to enable LE to carry out operational investigation measures and at the same time not breach individual rights or international law.[38]

In order to achieve the objective, the dissertation focuses upon the following ***research questions***:

1. How has information technology and the increasing role of digital evidence impacted the choice of measures LE may undertake during an investigation in order to access data that is not stored on its domestic territory?
2. Is conducting remote search and seizure of data not stored domestically an extraterritorial application of jurisdiction to enforce and thus a breach of territorial sovereignty; and whether and how can 'loss of location' be seen as shaping the interpretation of the principle of territorial sovereignty?
3. Has Estonia transposed CoCC Article 19(2) and Article 32(b) to its domestic regulation, does the current regulation meet the regulatory challenges of remote search and seizure and, taking into account regulatory examples of selected EU states, whether and how should the current regime be updated?

The main body of argument of the dissertation is developed in five articles analysing aspects related to remote search and seizure of data not stored on domestic territory. **Article I** 'Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data'[39] examines how information technology and the increasing relevance of digital evidence have impacted the choice of measures LE may undertake during an investigation in order to access data that is not stored on its domestic territory. **Article II** 'Transborder Access and Territorial Sovereignty'[40] investigates whether investigation measures such as remote search and seizure or 'transborder access' as foreseen by CoE CoCC Article 32(b) can be seen as an unlawful application of jurisdiction to enforce, therefore breaching the territorial sovereignty of the state where the data is stored in. The article also discusses the role of 'loss of location' as possibly precluding the unlawfulness of remote search and seizure of extraterritorial data under international law. **Article III** 'Tor Does Not Stink: Use and Abuse of the Tor Anonymity Network from the Perspective of Law' (co-authored with

[38] Such an analysis appears timely as the Estonian Ministry of Justice has announced a thorough review of the Estonian CoCP. Justiitsministeerium, 'Kriminaalmenetlusõiguse revisjoni lähteülesanne', 2015 <http://www.just.ee/sites/www.just.ee/files/ kriminaalmenetluse_ revisjoni_lahteulesanne.pdf> (last accessed 4 January 2017).

[39] Osula, 'Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data' (n 11).

[40] Osula, 'Transborder Access and Territorial Sovereignty' (n 36).

Tomas Minárik)[41] scrutinises the technical and legal challenges brought along by the Tor network that allows its users to hide their digital footprints. The thorough analysis of the Tor network contributes to the discussion on whether 'loss of location' can be seen as shaping the interpretation of the principle of territorial sovereignty and how such technologies influence LE's work. **Article IV** 'Global Views on Internet Jurisdiction and Trans-Border Access' (co-authored with Cristos Velasco and Julia Hörnle)[42] connects the concept of jurisdiction with prevalent challenges of accessing transborder data such as the question of the overall legality of the SPs to provide data to foreign LE. Finally, **article V** 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study'[43] focuses on the development of the idea of transborder access in the CoCC Article 32(b) and puts forward a domestic case study with interviews with European practitioners. The article scrutinizes the issues surrounding the interpretation of CoCC's relevant articles, and also investigates whether Estonia has transposed CoCC Article 19(2) and Article 32(b) to its domestic regulation. The article asks whether Estonia's current regulation meets the regulatory challenges of remote search and seizure and, taking into account the regulatory examples of selected EU states, whether and how the current regime should be updated.

The author of the dissertation is the sole author of articles I, II and V and has contributed equally with the co-authors in articles III and IV. In article III the author of the dissertation contributed to formulating the research question, structuring the research results, producing analysis (author's prime responsibility was compiling Sections III and V) and drawing results. In article IV the author of the dissertation contributed to formulating the research question, structuring the research results, producing analysis (author's prime responsibility was compiling Sections 2 and 2.1) and drawing results. The author views the role of articles III and IV to support and further develop the principle arguments and conclusions put forward in articles I, II and IV.

The analytical compendium to this cumulative dissertation is structured as follows. After introducing the research problem, its relevance in the area and outlining the main research questions, the compendium sets forth the methods and resources used for the dissertation. The above-mentioned research questions and the author's corresponding main conclusions as can be drawn from the articles included in this compendium reflect the structure of the analytical summary presented in Chapter II. Each sub-section under Chapter II is arranged into three sections: 'Description of the problem' (the general background of the

---

41 Minárik and Osula (n 8).

42 Cristos Velasco, Julia Hörnle and Anna-Maria Osula, 'Global Views on Internet Jurisdiction and Trans-Border Access' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move*, vol 24 (Springer Netherlands 2016) 465–476.

43 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28).

problem area is to be found in the introduction, with more concrete comments under each sub-section), 'Statement set for defence' and 'Reasoning'.

1.3. Methods and resources

The principle research methods used for compiling the articles constituting this dissertation have been analytical, comparative and teleological methods.

The analytical method was used for the extensive research of literature, analysis of available case law and legislation. Specifically, I would like to mention the relevance of the research undertaken by the following authors: Prof Jack Goldsmith (limits of the changing nature of territorial jurisdiction in the light of transborder access), Prof Orin Kerr (remote search and seizure in the US), Prof Ian Walden (cloud computing and location, transborder access, limits of LE) and Prof Bert-Jaap Koops (transborder criminal investigations, domestic regulation of remote search and seizure, CoCC). In Estonia, to the best knowledge of the author, no specific research about remote search and seizure of extraterritorial data has been published, there is no case law on the issue and neither is it clearly regulated in domestic law. Estonian authors such as Prof Eerik Kergandberg, Tõnu Mets, Prof Uno Lõhmus and Jaanus Tehver have discussed issues related to the research area of this dissertation and their work has been valuable in understanding the challenges of accessing and employing digital evidence in Estonia.

Due to lack of original legal writing in Estonian on remote search and seizure of extraterritorial data, the comparative method was highly valuable in analysing selected countries' regulation reflecting the latest developments in the EU. For the purposes of this dissertation, the author has compared the remote search and seizure legislation of Estonia, Germany, the Netherlands, Belgium, and added additional relevant examples from countries such as the US and New Zealand. Comparison of regulation, relevant studies and articles have been complemented by semi-structured interviews with public prosecutors and public officers from Estonia, Germany, the Netherlands, and Belgium who are dealing with criminal cases on a daily basis.[44] These four EU countries were chosen on the one hand to reflect the approaches influenced by both Germanic and Romanic civil law traditions. On the other hand, the choice should illustrate the lack of a standard approach existing among four countries that might initially seem to have a somewhat similar profile: all of them have highly developed digital literacy, have all signed the CoCC and belong to the same supranational regional organisation.

[44] Please note that the conducted interviews do not necessarily reflect the official state policy but may rather point at some of the state practice and difficulties identified in approaching the above-mentioned issues. Please also note that the interview with Dr Oskar Gross from Estonian Police and Border Guard Board was conducted after the publication of the articles in order to add a more comprehensive view to the Estonian case study.

In addition, the teleological method was used in studying the historic development and early calls on the regulation of transborder access together with the following efforts made by the CoE in the form of CoCC Article 32(b) and the accompanying documentation and proposals published by the CoE since then. Particularly appreciated in this regard have been the work and publications of the CoE Cybercrime Convention Committee and its *ad-hoc* sub-group on jurisdiction and transborder access to data.

As a rule, the resources and regulation analysed for the purposes of this dissertation have been taken as of the date of the publication of the articles constituting this compendium. However, where deemed appropriate, the author has further explained some of the arguments proposed in the articles and referenced additional resources published at a later date such as examples of relevant case law, academic articles and studies. In particular, the author has updated the sections regarding the developments in the EU and the CoE which have occurred after the publication of the respective articles and which broadly support the conclusions put forward by the articles published as part of this dissertation.

II SUMMARY OF THE MAIN CONCLUSIONS OF THE PUBLICATIONS INCLUDED IN THIS COMPENDIUM

2.1. Measures available for law enforcement during an investigation in order to access data that is not stored on its domestic territory

Description of the problem

As explained in the introduction, despite the estimation that approximately 70% of the currently employed means of international cooperation in cybercrime investigations are based on MLA mechanisms,[45] recent studies continue to underline the lack of a uniform approach and numerous shortcomings of the MLA system.[46] In fact, it is concluded that the MLA process is considered to be inefficient in general, and with regard to obtaining digital evidence in particular, thereby hindering governments' role in fighting against cybercrime and other crime involving digital evidence.[47]

Besides not catering to the needs of time-critical investigations targeting volatile digital evidence residing abroad, traditional MLA procedures or other state-to-state arrangements would be of limited use in situations where it is not possible to determine the location of the data, such as may occur with the use of cloud computing or the use of anonymising techniques, e.g. Tor. With the increasing role of digital evidence and the growing sophistication and geographical fragmentation of virtual crime scenes, states are seeking for alternative cooperation measures in accessing extraterritorial evidence. However, since there is currently no commonly accepted approach to accessing extraterritorially located data, these procedures lack transparency and overview mechanisms.

Statement set forth for defence

Options for accessing extraterritorially located data can be divided into two groups: state-to-state approaches and those 'sidestepping' the central role of states regarding the data stored on their territory. Unless the identified inefficiencies of the MLA process are addressed or alternative state-to-state measures developed, the traditional focus on the territoriality principle and assuming that the other state should be the primary counterpart for carrying out

---

45 United Nations Office on Drugs and Crime (n 2) 201.

46 E.g. New Zealand and Law Commission (n 20) 226; Gail Kent, 'Sharing Investigation Specific Data with Law Enforcement – An International Approach' [2014] Stanford Public Law Working Paper 6–9 <http://ssrn.com/abstract=2472413> (last accessed 4 January 2017); Koops, B-J and Goodwin, M (n 6) 26–27; Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (n 11) 123.

47 Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (n 11) 123.

investigative measures requiring access to evidence stored on the other state's territory, will continue to gradually shift towards more operative mechanisms that do not necessarily require the prior authorisation of the state where the data is located before the investigative measure such as search and seizure is carried out. Consequently, conflicts and uncertainty between states may occur as states' activities in accessing extraterritorial data may be breaching both national and international law, and result in unsought escalation of retaliation measures.[48]

Reasoning

In order to offer reasoning for the statement defined above, the following section will begin by examining two examples of international organisations that have attempted to address the critique towards the MLAT system by adopting specific multilateral instruments. These and other state-to-state mechanisms will then be compared to alternative measures for accessing data not stored domestically. Due to the time-critical nature of accessing digital evidence as well as the increasing use of technologies which allow the user to anonymise their location and identity, the latter group of measures has become more relevant over time. Based on these observations, the section proposes two general avenues for development.

Examples of two organisations actively seeking to provide more effective options for transborder access are the EU and the CoE. In the EU, criminal assistance has been largely built upon the framework of the CoE Convention on Mutual Assistance in Criminal Matters[49], parts of the Schengen Convention[50], the EU Convention on Mutual Assistance in Criminal Matters[51] and its Protocol.[52] The EU has addressed the need for immediate mutual recognition of orders to prevent the destruction, transformation, moving, transfer or disposal of evidence,[53] further improved judicial cooperation by applying the principle of mutual recognition to judicial decisions for the purpose of obtaining objects,

48 Osula, 'Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data' (n 11) 59–60.

49 Council of Europe, European Convention on Mutual Assistance in Criminal Matters, ETS no. 030 1959.

50 The Schengen Acquis – Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at their Common Borders (OJ L 239, 22.9.2000).

51 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).

52 Council Act of 16 October 2001 Establishing in Accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 326, 21.11.2001).

53 Council Framework Decision 2003/577/JHA of 22 July 2003 on the Execution in the European Union of Orders Freezing Property or Evidence (OJ L 196, 2.8.2003) para 1.

documents and data for use in proceedings in criminal matters,[54] and adopted in 2014 a Directive on the European Investigation Order that outlines a framework for a judicial authority of one Member State to 'have one or several specific investigative measure(s) carried out in another Member State' in order to obtain evidence.[55] The Directive indicates a gradual shift in the EU criminal cooperation logic from the MLA mechanisms (where the requested Member State has a wide discretion to comply with the request of another Member State) into a mutual recognition mechanism (where each Member State must in principle recognise and execute a request coming from another Member State).[56] However, in the context of accessing data stored extraterritorially, the Directive still does not solve the need for time-critical access to data during an investigation because it foresees 90 days as the allowed timeframe for responding to such requests.[57] In conclusion it can be observed that the development of the EU's common approach for more effective investigation has progressed in stages and has certainly improved in general but falls short in addressing the previously outlined challenges. As it would currently most likely not be in the interest of the EU Member States for the EU to enforce a 'pan-European code of criminal procedure'[58], the proposed measures do not have the mandate to solve the issues outlined before nor provide for a harmonised regulation for remote search and seizure.

As a recent EU development, and not covered by the articles constituting this dissertation, the conference 'Crossing borders: Jurisdiction in Cyberspace' resulted in a report inviting the Member States' Ministers to provide political guidance on outstanding issues such as MLA procedures and difficulties in establishing jurisdiction in cyberspace and to adopt the conclusions at the Council of the EU in June 2016.[59] The following conclusions of the Council of

---

[54] Council Framework Decision 2008/978/JHA of 18 December 2008 on the European Evidence Warrant for the Purpose of Obtaining Objects, Documents and Data for Use in Proceedings in Criminal Matters (OJ L 350, 30.12.2008) 6.

[55] Importantly, as of 22 May 2017, this Directive will replace most of the existing laws in the area of transferring evidence between Member States in criminal cases. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 Regarding the European Investigation Order in Criminal Matters (OJ L 130, 1.05.2014) (n 23) 1(1).

[56] ibid 1(2); Steve Peers and Emilio De Capitani, 'EU Law Analysis: The European Investigation Order: A New Approach to Mutual Recognition in Criminal Matters' <http://eulawanalysis.blogspot.com/2014/05/the-european-investigation-order-new.html> (last accessed 4 January 2017).

[57] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters (OJ L 130, 1.5.2014) (n 23) 12(4).

[58] Samuli Miettinen, *Criminal Law and Policy in the European Union* (Routledge 2013) 176.

[59] Article II of this dissertation, Osula, 'Transborder Access and Territorial Sovereignty' (n 36) was indicated as suggested reading and point of reference for the Amsterdam Conference 'Crossing Borders: Jurisdiction in Cyberspace', 7th–8th of March 2016, the final report of which, in addition to offering a comprehensive background to the problem area, also invited the Ministers to adopt the 2016 Council of the EU conclusions. See, 'Crossing Borders:

the EU, on improving criminal justice in cyberspace, set out concrete measures for future follow-up and action in three main areas of work: improving MLA procedures, enhancing cooperation with SPs and examining possible connecting factors for enforcement jurisdiction in cyberspace.[60] The Council conclusions on the European Judicial Cybercrime Network concluded that the existing exchange between Member States' 'judicial authorities and experts in the field of cybercrime and investigations in cyberspace should be formalised and enhanced under the European Judicial Cybercrime Network supported by Eurojust' by facilitating the exchange of expertise, best practices and other relevant knowledge and experience on the investigation and prosecution of cybercrime.[61] These conclusions exhibit more concrete proposals for addressing the problem area described in this dissertation and support some of the conclusions of the articles constituting this dissertation. The proposals put forward by these two instruments will certainly be a step in the right direction and will hopefully lead the EU towards a more harmonized approach to accessing data extraterritorially.

CoE CoCC is the only international treaty that includes provisions regarding MLA specifically in cybercrime cases. As of 4 January 2017, CoCC had 51 ratified and 5 signed but not yet ratified Parties.[62] CoCC invites its Parties to provide each other mutual assistance to the widest extent possible (Article 23 and Article 25 p 1) and it further describes procedures to be used for mutual assistance requests in the absence of an applicable international agreement (Article 27 and Article 28). In order to underline the volatile nature of digital evidence, specific provisions also encourage 'expedited' means of communication (Article 25 p 3), use of 24/7 networks (Article 35) and sharing spontaneous information (Article 26). CoCC also prescribes options for expedited preservation of stored computer data where the other Party is requested to preserve information stored in its territory before the mutual assistance request has been formally submitted (Article 29). CoCC makes it easier for its Parties to share certain types of data (such as the expedited disclosure of preserved traffic data in Article 30) and foresees 'mutual assistance regarding accessing of stored computer data' (Article 31) among the Parties. Article 31 allows to request the other Party to 'search or similarly access, seize or similarly secure, and disclose

---

Jurisdiction in Cyberspace' (2016) Conference report 1–2 <http://data.consilium.europa.eu/doc/document/ST-7323-2016-INIT/en/pdf> (last accessed 4 January 2017); 'Crossing Borders: Jurisdiction in Cyberspace' (*The Netherlands EU Presidency 2016*, 7 March 2016) <https://english.eu2016.nl/events/2016/03/07/crossing-borders-jurisdiction-in-cyberspace> (last accessed 4 January 2017).

60 Council of the European Union, 'Council Conclusions on Improving Criminal Justice in Cyberspace' (2016).

61 Council of the European Union, 'Council Conclusions on the European Judicial Cybercrime Network' (2016) 2.

62 Council of Europe, 'Convention on Cybercrime, List of Signatories and Ratifications.' <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG> (last accessed 4 January 2017).

data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29' (Article 31 p 1). Importantly, the provision makes it possible to request for such assistance on an expedited basis where 'there are grounds to believe that relevant data is particularly vulnerable to loss or modification' or there are other legal grounds for providing for expedited co-operation (Article 31, 3a). Unfortunately, due to the increasingly decentralised nature of MLA where a growing amount of requests are sent or received directly between relevant judicial authorities and not only via central authorities, there are currently no statistics on the frequency of the use of mutual assistance to access stored computer data amongst the CoCC Parties.[63] Still, the CoE was able to conclude that CoCC Parties appear not to be making full use of the opportunities offered by CoCC and other specific agreements.[64] Therefore, the CoE has issued a set of recommendations for both Parties and other relevant entities on how to improve the MLA system in the context of accessing stored computer data.[65]

In addition to the MLA process, there are other (in some situations more expedient) state-to-state mechanisms that involve cooperation among the LE of two or more countries, and thus, require a formal or informal state authorisation in the provision of specific data to the requesting LE. Examples include informal cooperation between LE[66] and maintaining 24/7 liaison networks with standing points of contact.[67] For complex international cases, the frameworks of Europol, Eurojust or Interpol are employed, as well as Joint Investigation Teams, LE liaison officers or networks.[68] Such cooperation mechanisms are guided by the territoriality principle that focuses, as the principal counterpart of the investigation, on the country in whose territory the data being sought resides, and thereby allows for certain transparency and having a general overview of the activities of foreign LE targeting data stored on domestic territory.

However, there are two crucial challenges that these state-to-state mechanisms fail to address. These are the need for time-critical access to the evidence and the occurrence of situations where the location of the data cannot be determined. As was explained in the introduction, cloud computing and the Tor

---

63 Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (n 11) 6.

64 ibid 123.

65 ibid 125–127.

66 Generally, LE cooperation is aimed at exchanging intelligence that could lead to the commencement of criminal proceedings even if, in many cases, the information obtained through such alternative cooperation cannot be used as evidence in criminal proceedings. The distinction between police-to-police cooperation and MLA is not always very clear. ibid 7–8.

67 Except for the use of MLAs, however, these methods are under-utilised and handle only approximately 3% of the cybercrime cased confronted by LE. United Nations Office on Drugs and Crime (n 2) xxv.

68 Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (n 11) 91.

network are only a few examples of technologies that allow to hide one's location online. Besides re-directing the traffic to a network of relays acting as proxy servers and providing users with fake Internet Protocol (IP) addresses, Tor also provides its users 'hidden services' which allow websites to be published and other services to be offered without needing to reveal the location of the site.[69] The research undertaken on the Tor network suggests that even if governments would disregard the arguments of freedom of expression and rather ban the use of Tor and thereby be more in control of their residents' online activities,[70] due to technological reasons, it will most likely be impossible to fully ban the use of anonymising technologies. As long as the Internet remains a globally distributed network without a central governing body, there will technically be a way for Tor or other anonymity networks to exist and operate.[71] This means that options such as the Virtual Private Network (VPN), proxies, and Tor will continue to shape the virtual environment in which LE needs to operate.[72]

Thus, LE is in need of more flexible options for accessing extraterritorial data. However, such measures can be seen as 'sidestepping' the central role of the state and the principle of territorial jurisdiction as the determining factor for the location of the data. While employing these measures, investigators do not always seek formal authorisation from the relevant entities of the state where the data physically resides. This raises concerns about the extraterritorial application of these powers. Examples of such a way forward include contacting the SP directly, accessing publicly available data and undertaking investigative measures such as remote search and seizure (the latter may be based on CoCC Article 32(b); a more detailed analysis can be found in Section 2.3). Despite a lack of reporting on state practice and statistics regarding the frequency of the employment of such measures, recent case law indicates that these options are becoming more and more used by LE.

Domestically, LE may exercise coercive powers with the aim to force the disclosure of communications data and/or the simultaneous interception of data in transit, or searching certain devices under a warrant, but the extraterritorial application of the same powers becomes problematic.[73] Traditionally, if the SP would not be located in the state carrying out the investigation, an MLA system would require contacting the central authority of the SP's home jurisdiction

---

69 Tor Project, 'Tor: Overview' <https://www.torproject.org/about/overview> (last accessed 4 January 2017).

70 Banning Tor would most probably not be legally viable, at least in states that are party to the European Convention of Human Rights. Read more at Minárik and Osula (n 8) 5–7.

71 Bruce Schneier, 'Anonymity and the Internet' <https://www.schneier.com/blog/archives/2010/02/anonymity_and_t_3.html> (last accessed 4 January 2017).

72 In fact, LE is currently using Tor for its own benefits such as for online surveillance, sting operations and anonymous tip lines. Tor Project, 'Users of Tor' <https://www.torproject.org/about/torusers.html.en> (last accessed 4 January 2017). See also the discussion on the US Playpen case in Section 2.2.

73 Velasco, Hörnle and Osula (n 42) 469.

with a request for preservation and/or production of the computer data[74] and hence, the state-to-state approach would be used. However, current legal debates have come to focus on two aspects.

Firstly, whether LE has the power to directly request data from a foreign SP (established or headquartered in a foreign country) and whether there is an obligation for the SP to respond to such requests.[75] An example of the first scenario occurred in the series of Yahoo! Inc. court cases where Yahoo! Inc. was convicted for not communicating the data concerning certain email accounts used in Belgium to the Belgium Public Prosecutor.[76] Apparently, Yahoo! Inc.'s arguments which included Yahoo! Inc. not being based in Belgium, and not having a subsidiary office there, resulting in the position that requests with such extraterritorial effects should go through MLA, did not find support from the judge. According to the decision of the Court of Appeal of Antwerp on 20 November 2013, the fact that Yahoo! Inc. does 'not have an office or establishment in Belgium is irrelevant.'[77] The Court of Appeal's reasoning was at least partly confirmed in 2015 by the Belgium Court of Cassation which asserted that unlike Yahoo! Inc.'s opinion, Belgium's request for data was not extraterritorial since the request for disclosure was targeted at an operator of an electronic communication network or an electronic communications SP who was active in Belgium and does not imply any intervention outside the territory of Belgium, such as sending civil servants abroad.[78] Furthermore, it was concluded that notwithstanding where the operator is originally based, its refusal to comply with the Prosecutor's request constitutes an offence that takes place on the territory of Belgium.[79] The fact where the data to be sought was stored, was not discussed.

Secondly, it is debated whether LE has the power to request data from a local SP (established on domestic soil) in circumstances where the data is physically stored on a foreign territory.[80] In a recent case *United States v. Microsoft Corporation* the US Government requested Microsoft (headquartered in the US) with a warrant issued on the Stored Communications Act to produce the content of its customer's emails stored on a server located outside the US. Unlike the preceding decision of the District Court for the Southern District of New York[81], the 2016 decision concluded that the warrant 'does not authorize courts

---

74 United Nations Office on Drugs and Crime (n 2) 217.

75 See, e.g. Velasco, Hörnle and Osula (n 42) 470–475.

76 E.g. *Yahoo! Inc* [2013] Belgium Court of Appeal of Antwerp, 12th chamber for criminal cases 2012/CO/1054.

77 ibid.

78 *Yahoo! Inc* [2015] Court of Cassation of Belgium P.13.2082.N. It must be noted that this decision was made after the IV article had been published but did not change the general arguments of the Court of Appeal of Antwerp in 2013.

79 ibid.

80 See, e.g. Velasco, Hörnle and Osula (n 42) 470–475.

81 *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp*., 13 Mag. 2814 WL 1661004 (S.D.N.Y. 2014).

to issue and enforce against US-based SPs search and seizure warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers'.[82] Among other arguments, the court confirmed the possibility of an international disaccord, if the US Government were to seek the 'emails of an Irish national, stored in Ireland, from an American company which had marketed its services to Irish customers in Ireland'.[83] Despite ruling in Microsoft's favour, the judge reflects her scepticism regarding the absolute relevance of the 'location' of the data which would be able to put the data outside the reach of purely domestic regulation.[84]

In the opinion of the author, both of these cases illustrate how the development of information technology is influencing the effectiveness of the MLA procedures and the choice of measures employed on behalf of LE. In both cases we can see that the governments' first choice for accessing extraterritorial data was not an MLA procedure, but instead directly contacting the SP. In *United States v. Microsoft Corporation*, the US Government insisted on the legality of the warrant even after becoming aware that the data was stored extraterritorially, whereas in *Yahoo! Inc.* the actual location of the data was not a decisive argument at all for the court, and neither was it claimed that the data was stored in Belgium. These different legal approaches underline the fragmentation and lack of a common understanding on the legal limits of LE's mandate for accessing extraterritorially located data. Furthermore, these examples reinforce the argument that even if not officially admitted or supported by the majority of governments, technological change, the increase in sophisticated threats and the need to redress harmful local effects of malicious offshore activities can be seen as altering the extraterritorial influence of purely territorial action.[85]

The author concludes by predicting that unless the MLA system is reformed, the traditional assumption that the other state should be the primary counterpart for carrying out investigative measures requiring access to evidence stored on the other state's territory, will continue to gradually shift towards more operative mechanisms that do not necessarily require the prior authorisation of the state where the data is located before an investigative measure such as search and seizure is carried out.[86] The author suggests two possible courses of action that do not necessarily contradict each other.[87] Firstly, states may decide

---

82 *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp*., No. 14–2985 (2d Cir. 2016) 2.

83 ibid 15.

84 ibid 17.

85 Goldsmith (n 31) 111.

86 Osula, 'Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data' (n 11) 59–60.

87 ibid 58–59. Similar two strands of work with a list of proposals for further action were proposed by the Amsterdam 'Crossing Borders: Jurisdiction in Cyberspace conference in 2016: 'First, by looking into possibilities to speed up the handling of formal MLA requests, as well as to explore other ways of international cooperation. Second, to address the underlying and more fundamental question about how jurisdiction in cyberspace should be

to move towards finding consensus on the use of alternative measures for accessing extraterritorially located data, such as reflected in the extensive work undertaken by the CoE. This does not appear to be an easy task since it would require a wider discussion on a number of interrelated issues that broadly touch upon the '(re)-conceptualization of the extent to which "data location" can still be used as a guiding principle',[88] especially in circumstances where the exact location of the data cannot be identified. To begin with, states should find a common ground on the interpretation of the limits of jurisdiction to enforce which would allow for, under certain circumstances, direct access to the data or the SP without the prior authorisation of the other state. [89] This issue will be tackled in greater detail in the next sub-chapter. Foremost, more transparency is needed concerning state practice and official positions regarding the measures to be used for accessing extraterritorially located data. Without sharing domestic interpretations and practice with the international community, concrete agreements for further options for transborder access will be doubtful.[90]

Secondly, and assuming that this would be the preferred choice of states keen to protect its sovereignty, states may choose to invest in reforming the current MLA procedures.[91] This would certainly not be a smooth process, since, despite the clear need for more effective investigative tools and common criticism on MLA, states have largely refrained from open and constructive discussions on how to enhance these traditional frameworks. The reasons for this are ambiguous: in addition to lack of resources, one of the causes may be that the general lack of statistics related to cybercrime (lack of reporting and initiating prosecution as well as lack of statistics on the use of different cooperation measures) downplays the urgency of the issue on the political level. In order to overcome this, stakeholders should continue to underline the relevance of these issues for the successful fight against cybercrime, and propose options for reform. Clearly, regional organisations and multilateral agreements adopted by their members, or by a smaller group of like-minded states, may have certain

---

established.' 'Crossing Borders: Jurisdiction in Cyberspace' (n 59) 4. These proposals have also been echoed in recent Council of EU conclusions adopted in June 2016. Council of the European Union, 'Council Conclusions on Improving Criminal Justice in Cyberspace' (n 60); Council of the European Union, 'Council Conclusions on the European Judicial Cybercrime Network' (n 61).

88 United Nations Office on Drugs and Crime (n 2) 223.

89 Especially as regards to new developments such as Brazil announcing that Brazilian data is under its jurisdiction regardless of where the data is stored Brazil, Law No. 12.965, April 23rd 2014.

90 Osula, 'Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data' (n 11) 58.

91 A comprehensive list of proposals has been put forward in e.g. Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (n 11); Andrew K Woods, 'Data Beyond Borders: Mutual Legal Assistance in the Internet Age' (2015) Global Network Initiative <https://globalnetwork initiative.org/sites/default/files/GNI%20MLAT%20Report.pdf> (last accessed 4 January 2017); Kent (n 46).

geographical restrictions when it comes to the territorial scope of their solutions but would nevertheless set an example of effective and transparent measures to other states and encourage them to follow the lead.[92]

2.2. Jurisdiction to enforce, territorial sovereignty and 'loss of location'

Description of the problem

As was explained in the introduction, the legality of remote search and seizure of extraterritorial data under international law has not been universally established. The Lotus principle sets a clear prohibition on expanding the territorial scope of jurisdiction to enforce:

> *'Now the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.'*[93]

Accordingly, every state has a duty to abstain 'from committing any violation of another state's independence or territorial or personal authority'[94] and 'persons may not be arrested, a summons may not be served, and police or tax investigations may not be mounted on the territory of another state, except under the terms of a treaty or other consent given'.[95] The general power of a state to exercise supreme authority over all persons and things within its borders is known as 'territorial sovereignty'[96] and extraterritorial application of jurisdiction to enforce can be seen as a violation thereof.[97] In fact, the meaning of territorial sovereignty relies on the assertion that both concepts – sovereignty and jurisdiction – can only be comprehended in relation to territory.[98] This has

---

92 Osula, 'Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data' (n 11) 58–59.

93 *The Case of the S.S. Lotus, Fr. v. Turk., 1927 P.C.I.J. (ser. A) No. 10 (Decision No. 9)* (n 34) [45].

94 Oppenheim (n 35) 385.

95 John Crawford, *Brownlie's Principles of Public International Law* (8th Edition, 2012) 479, quoting Lotus (1927) PCIJ Ser A No 10, 18; Service of Summons (1961) 38 ILR 133; 2 Repertoire Suisse de Droit International Public, 986–1017.

96 Oppenheim (n 35) 382.

97 ibid 385.

98 Shaw (n 32) 487.

led to claims that territory has become 'perhaps the fundamental concept of international law'.[99]

However, views regarding the accepted scope of jurisdiction to enforce and the threshold of breaching territorial sovereignty in cyberspace are fragmented. On the one hand, the technological developments that have evoked fears of a new borderless[100] world that would reduce the central role of territoriality in international law have not managed to undermine the foundational strengths of the territoriality principle completely.[101] This is mostly because none of the above-mentioned technical challenges fully 'deprive a state from its legal right to exercise jurisdiction over persons and cyber infrastructure located on its territory',[102] even though it can be concluded that they certainly increase the difficulty of doing so.[103] It has therefore been suggested that in the context of cyberspace, the principle of sovereignty upholds sovereign prerogatives, legal and regulatory controls over any cyber infrastructure located within a state's territory; similarly, a state's territorial sovereignty protects the infrastructure located on its territory, whether it belongs to the state, the private sector or an individual.[104,105]

On the other hand, it should be asked how domestic investigation measures necessary for fighting the increasingly sophisticated cybercrime fit the traditional concept of territorial sovereignty. In the context of this dissertation, the author has in particular examined whether carrying out remote search and seizure of extraterritorial data would entail an extraterritorial application of jurisdiction to enforce and whether this would consequently constitute a violation of the other state's territorial sovereignty. Given that anonymising techniques such as Tor render the notion of 'territory' untrustworthy in regard to the actual location of the data or the person behind the data, it should also be discussed how 'loss of location' influences the interpretation of territorial sovereignty in cyberspace. Examples of state practice unilaterally conducting remote search and seizure of data not stored on their domestic territory raise the

---

99 ibid 488, quoting D.P. O'Connell, International law, Second Edition, London 1970, Vol 1, p 403; see also 'Draft Convention on Jurisdiction with Respect to Crime' (1935) 29 The American Journal of International Law 439, Art 3.

100 Claims that territorial borders do not exist at all in cyberspace can easily be proved to be incomplete as the physical hardware and operating systems on which the Internet relies must ordinarily be based in the territory of a state. Read more at e.g. Michael Hirst, *Jurisdiction and the Ambit of the Criminal Law* (Oxford University Press 2003) 186.

101 Shaw (n 32) 488.

102 Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) 19.

103 Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' 89 Int'l L. Stud. 123 (2013) 134.

104 Schmitt (n 102) 16.

105 Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 4.

question whether the current legal assessment on the territorial scope of jurisdiction to enforce can indeed be based on a court decision written in 1927.[106]

Statement set for defence

In addition to possibly being illegal within the other state's domestic framework, conducting remote search and seizure of extraterritorial data without basis under international law entails an extraterritorial application of jurisdiction to enforce. Therefore, without the legal right deriving from an international treaty, consent or other grounds in international law, remote search and seizure of extraterritorial data could be considered as a breach of territorial sovereignty. Yet, such a strict interpretation of *lex lata* should be viewed together with emerging state practice, which indicates that rapid technological development and the need to counter sophisticated transnational crime will continue to influence the interpretation of the concept of territorial sovereignty, ultimately rendering the traditional understanding less relevant. Furthermore, circumstances such as 'loss of location' may be seen as precluding the wrongfulness of remote search and seizure under international law.[107]

Reasoning

In order to offer reasoning for the statement defined above, the following section analyses whether remote search and seizure of extraterritorial data without the other state's consent or other basis under international law would constitute an extraterritorial application of jurisdiction to enforce and thereby result in breaching the other state's sovereignty. The traditional interpretation of these concepts of international law will then be compared to selected developments in state practice and international organisations. Finally, the section will examine whether 'loss of location' can be seen as excluding the possibility of breaching territorial sovereignty.

Jurisdiction to enforce

While jurisdiction is linked to the concept of territory, it is not exclusively tied to it[108] which means that the principle of territoriality cannot always be applied in a straightforward manner.[109] For instance, a state could employ prescriptive or adjudicative jurisdiction over an extraterritorial matter. This could be done by using the nationality principle in order to extend its material jurisdiction to its

---

106 Paul de Hert, 'Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace – Whose Sovereignty Is at Stake' in Bert-Jaap Koops and Susan W Brenner (eds), *Cybercrime and jurisdiction: a global survey* (TMC Asser; Cambridge University Press 2006) 72.

107 Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 733.

108 Shaw (n 32) 646.

109 Oppenheim (n 35) 458.

citizen located in another country or maintaining that the subjective and objective territoriality principle are applicable when part of the offence has taken place in a foreign territory. Furthermore, some states support the controversial 'effects doctrine', the extraterritorial application of which would require a 'genuine connection between the subject matter of jurisdiction and the territorial base or reasonable interests of the state in question'.[110] Apart from the general challenges that fighting cybercrime poses to applying traditional notions of law, no extensive problems related to prescribing material jurisdiction have been reported.[111, 112]

Nevertheless, there is an apparent difference between the legally accepted territorial scope of different functions of jurisdiction. Even if it is accepted that a state could apply prescriptive or adjudicative jurisdiction over an extraterritorial matter, states generally lack the jurisdiction to enforce their decision on the territory of the other state.[113] As explained before, it would be illegal for a state to send police forces to another state's territory or to exercise an act of administration or jurisdiction on foreign territory without permission,[114] resulting in violating both international law (such as breach of sovereignty) and the domestic legal framework (e.g. provisions of national Penal Code),[115] and also possibly hindering peaceful relations between States.[116, 117]

However, the rules for the territorial scope of jurisdiction to enforce are not explicit in cyberspace. Unlike in the 'physical world' where exercising jurisdiction to enforce would generally mean physically being on another state's territory without prior authorisation and where the transgressing agents may be caught and convicted according to the domestic law of the captor state,[118] investigative measures such as remote search and seizure of extraterritorial data do not require the state agents to leave their domestic territory, rendering such

---

110 Crawford (n 95) 457.

111 United Nations Office on Drugs and Crime (n 2) xxv.

112 Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 723.

113 *Case concerning the arrest warrant of 11 April 2000 (Democratic Republic of Congo v Belgium): judgment of 14 February 2002, Dissenting Opinion of Judge van den Wyngaert* (International Court of Justice) 168.

114 Oppenheim (n 35) 386–387.

115 Example would be Article 271 of the Swiss Criminal Code that prescribes: 'Any person who carries out activities on behalf of a foreign state on Swiss territory without lawful authority, where such activities are the responsibility of a public authority or public official, any person who carries out such activities for a foreign party or organisation, any person who encourages such activities, is liable to a custodial sentence not exceeding three years or to a monetary penalty, or in serious cases to a custodial sentence of not less than one year'. *Swiss Criminal Code of 21 December 1937 (Status as of 1 October 2016) para 271 (1).*

116 Mireille Hildebrandt, 'Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace' (2013) 63 University of Toronto Law Journal 196, 223.

117 Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 723.

118 Cassese (n 32) 51.

national remedies largely unavailable.[119] Indeed, if the officers conducting the investigation do not leave their own territory, would there be any ground for discussing extraterritorial application of jurisdiction to enforce, and thereby a possible breach of sovereignty?[120]

Since much of the law regarding jurisdiction has developed through the decisions of national courts applying domestic laws, sometimes irrespective of their compatibility with international law, the influence of national jurisprudence has contributed to the uncertainty surrounding many matters related to jurisdiction.[121] Based on scarce evidence of state practice, available (and sometimes contradictory) case law and literature on the 'location' of remote search and seizure, three approaches can be distinguished. It has been discussed in literature that in situations where LE finds a networked computer which is displaying data, normally stored abroad, on the screen, and that has also stored the data in the interim memory of the computer, such a copy would be, strictly speaking, located on the domestic jurisdiction,[122] and hence, accessing such data would not entail an application of extraterritorial jurisdiction to enforce. Building on this reasoning, holders of the first view believe that an extraterritorial search is legal in circumstances where the agents, while surreptitiously installing data extraction software[123] or employing other investigative measures with an extraterritorial reach, do not actually leave the judicial district to obtain and view the information gathered from the target computer and, since the data will first be examined within their domestic territory, it becomes 'property located within the district'.[124] According to this logic, the LE could 'roam the world' in search of a 'container of contraband' so long as the data container is not opened until the 'agents haul it off to the issuing district'.[125] This is also consistent with the view that 'a search occurs when information from or about the data is exposed to possible human observation, such as it appears on a screen, rather than when it is copied by the hard drive or processed by the computer',[126] allowing the US District Court to conclude that since no exposure to the domestic LE takes place

---

[119] Note that there have been cases where individuals have been charged for illegal access or similar offences without being physically present on the territory of that state. See e.g. United States Department of Justice, 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage' (19 May 2014) <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor> (last accessed 4 January 2017); *United States v Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui*, 14–118 (W.D. Pa. 2014).

[120] Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 723.

[121] Oppenheim (n 35) 457.

[122] Nicolai Seitz, 'Transborder Search: A New Perspective in Law Enforcement' (2004) 7 Yale JL & Tech. 23, 28.

[123] *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753, 758 (S.D. Tex. 2013) 2.

[124] ibid 4.

[125] *In re Warrant to Search a Target Computer at Premises Unknown* (n 123) 5.

[126] Kerr, 'Searches and Seizures in a Digital World' (n 29) 23.

until the data is being reviewed in the US (i.e. the state accessing the information), 'no extraterritorial search has occurred'.[127] The second perspective suggests that such a search actually takes place in two locations: one, where the computer that is the target of the search resides, and another, where the data will actually be analysed by the other state's LE.[128] The third (and most prevalent) view, however, asserts that the collection of extraterritorially located data via investigative techniques such as remote search and seizure would indeed take place in foreign networks. This perspective was supported by a recent US District Court decision stating that '(s)uch search takes place, not in the airy nothing of cyberspace, but in physical space with a local habitation and a name,' and even when the search could be seen as two-fold, '(n)either search will take place within this district'.[129] The same approach has been echoed by Microsoft, which maintains that '[a] seizure of electronic mail occurs at the time it is copied and in the place where it is stored'[130] and by the recent US Second Circuit judgment asserting that 'the invasion of the customer's privacy takes place […] where the customer's protected content is accessed – here, where it is seized […]'.[131] Several recent court rulings in the so-called *Playpen* case which have focused on the legality of a certain investigative technique also concur that the property to be searched is the final destination i.e. the user's computer rather than the server where the investigative measures have been launched from.[132] Similarly, a number of scholars have concluded that during a transborder search the government action takes place outside the state which is conducting the search since what matters is the 'end result of the search'[133] and that a 'search of one's hard drive by a foreign [LE] agency from abroad […] has the same effects as a traditional search of premises' and therefore 'the consent of the territorial sovereign in which the target is located is required'.[134] It can therefore be concluded that even if we differentiated between 'search' and 'seizure' activities, the latter would still entail the act of 'copying the data', necessarily taking place in extraterritorial networks, and, consequently understood as an

---

127 *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp*. (n 81) 13–14.

128 Orin S Kerr, 'Fascinating New Case on Legal Standards for Searching a Remote Computer With Unknown Location' <http://volokh.com/2013/04/26/fascinating-new-case-on-legal-standards-for-searching-a-remote-computer-with-unknown-location/> (last accessed 4 January 2017).

129 *In re Warrant to Search a Target Computer at Premises Unknown* (n 123) 5–6.

130 Brief for appellant, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp*., 14-2985-cv (2d Cir. 2014) 31.

131 *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp*. (n 82) 39.

132 E.g. *United States v. Levin*, 15-10271-WGY, 2016 WL 2596010 (D. Mass. 2016) 14; *United States v. Arterbury*, 15-CR-182-JHP, 2016 BL 133752 (N.D. Okla. 2016) 16.

133 Young (n 31) 162–164.

134 Stephan Wilske and Teresa Schiller, 'International Jurisdiction in Cyberspace: Which States May Regulate the Internet' (1997) 50 Fed. Comm. LJ 117, 174.

extraterritorial application of jurisdiction to enforce. This approach was also recognised by the US Department of Justice cautioning that 'some countries may object to attempts by US LE to access computers located within their borders. Although the search may seem domestic to a US LE officer executing the search in the US pursuant to a valid warrant, other countries may view matters differently.'[135] Other countries have also implied that remote investigations do undeniably take place on the territory of the other state and therefore would require additional legal grounds such as MLA.[136] Given the scarcity of case law and lack of official state opinions asserting the opposite, the research concludes that according to *lex lata* remote search and seizure of extraterritorial data can be seen as involving the application of extraterritorial jurisdiction to enforce.[137]

However, at the same time it is clear from emerging state practice that investigational needs and the increasing sophistication of cybercrime are pushing countries towards slowly but steadily altering the level of acceptance for the limits of jurisdiction to enforce. This means that the traditional scope of jurisdiction to enforce and its territorial application is and should be evolving in time in order to best fit the requirements of LE and to avoid impunity for criminals. A common understanding regarding the accepted territorial scope of jurisdiction to enforce should be developed by states through state practice and legal frameworks which offer both certainty and transparency for the stakeholders involved in transborder investigation.[138]

Breaching sovereignty

Regardless of views that transborder access would generally be in line with territorial sovereignty,[139] neither individual countries nor international organisations have univocally supported such access without any additional legal grounds such as consent, nor is the legality of transborder access widely defended by scholars.[140] To the knowledge of the author, the best available

---

135 Kerr, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (n 29) 85.

136 E.g. 'According to international law (digital) research activities in the territory of another state can only be made through international legal assistance', Dutch Minister of Security & Justice, 'Letter to the Dutch Parliament, Cybercrime Legislation' (15 October 2012) <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2012/10/15/wetgeving-bestrijding-cybercrime/wetgeving-bestrijding-cybercrime-1.pdf> (last accessed 4 January 2017) 3.

137 Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 723–725.

138 Velasco, Hörnle and Osula (n 42) 470.

139 E.g. Goldsmith (n 31) 115.

140 E.g. Koops, B-J and Goodwin, M (n 6) 9 on the strict interpretation of international law according to which transborder access without the consent of the foreign state constitutes a wrongful act under international law; Bellia (n 31) 100 generally concluding that unilateral transborder access would be prohibited by customary international law; Young (n 31) 161 reaching the conclusion that customary law regarding transborder access does not exist at all.

indication of different states' opinions regarding the matter derives from the already quoted UN study where two-thirds of the 69 responding countries perceived foreign LE's access to other countries' computer systems or data as impermissible, even if this may occur in practice either with or without the knowledge of the investigators.[141] At the same time there are well-known instances such as Gorshkov-Ivanov[142] and Bredolab botnet cases[143] where the employment of effective investigation techniques may be seen as challenging the traditional understanding of territorial sovereignty.

In assessing whether accessing data that is located in a foreign jurisdiction without sufficient grounds in international law would be a breach of sovereignty, two substantially different viewpoints have emerged.

The first is based on the strict interpretation of the ('vehemently criticised'[144]) Lotus case according to which any exercise of jurisdiction to enforce on a foreign territory should be considered as a violation of territorial sovereignty. According to this approach, unless on specific legal grounds, the territorial limitations of conventional investigative powers such as search and seizure do not allow for transborder access to servers located in other jurisdictions.[145] Should such access occur, it would constitute a breach of sovereignty even if the mere 'virtual presence' would not cause any damage to the transgressed state's networks.[146] However, as a consequence of such a low legal threshold, there

---

[141] This underlines the possible differences between states' official views and their actual LE practices. United Nations Office on Drugs and Crime (n 2) 220–223.

[142] *United States v Gorshkov*, 2001 WL 1024026 (W.D. Wash. 2001). According to commentators, this is the first openly known case where national authorities have used transborder access for investigation and where evidence obtained in such a way served as the basis for the conviction. Seitz (n 122) 27.

[143] Openbaar Ministerie, 'Dutch National Crime Squad announces takedown of dangerous botnet' (*Openbaar Ministerie*, 15 October 2010) <https://www.om.nl/actueel/nieuwsberichten/@28332/dutch-national-crime/> (last accessed 4 January 2017). Whereas it is unlikely that someone would bring the Dutch police to justice for the advisory messages they sent to computers worldwide, the action does draw attention to the legal limits of LE's activities in regard to computers located in foreign territories, especially since an act entailing 'illegal access' would most probably be illegal both in the Netherlands and other involved nations. Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 726.

[144] Cedric Ryngaert, *Jurisdiction in International Law* (Second Edition, Oxford University Press 2015) 34. See also de Hert (n 106) 72.

[145] E.g. Steven Chong SC, 'Keynote Address by the Honourable Attorney-General' (Criminal Law Conference, 17 January 2014) 10 <https://www.agc.gov.sg/DATA/0/Docs/NewsFiles/AG%20Speech_%20Criminal%20Law%20Conference_17%20Jan%202014.pdf> (last accessed 4 January 2017).

[146] Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (n 103) 129; Koops, B-J and Goodwin, M (n 6) 9, 61–62. However, the Tallinn Manual 1.0 experts were unable to concur whether a country's activity that does not cause any damage to another state such as planting malware for monitoring could be considered as a breach of sovereignty. Schmitt (n 102) 16. This conclusion should be separated from their legal assessment of conducting 'inherently governmental functions exclusively reserved to another state on the latter's territory', see footnote 147.

could possibly be thousands of breaches of sovereignty every day, and this could become very burdensome for states. Possibly, countries' decision not to respond to such breaches of sovereignty may be strategic as to allow a wide range of possible interpretations and 'room for action', and the legal uncertainty of the legal status under international law is similar to the often-quoted example of cyber espionage.[147, 148]

The second, alternative view emphasises that not every state conduct that has an impact on the cyber infrastructure of another state would necessarily constitute a violation of the principle of territorial sovereignty.[149] There are two ways of understanding this claim. Firstly, in order to be seen as a violation of the territoriality principle, the extraterritorial access must result in inflicting material damage to the cyber infrastructure located in the other state while an act resulting in mere minor material damage to the cyber infrastructure should not be considered as a violation of territorial sovereignty.[150] Supporters of this view maintain the general legitimacy of searches which do not inflict material damage and argue that 'remote crossborder searches fit into the long-accepted practice of officials in one nation acting within their territory (or from public spaces) to extract information from another' and that 'territorial sovereignty has

---

147 Robert D Williams, '(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action' (2011) 79 The George Washington Law Review 1175. It should be noted that there is general legal ambiguity regarding the crossborder collection of data. Over the years, nations have collected information from the territory of another nation with the help of e.g. binoculars, periscopes and orbital reconnaissance satellites without physically entering the territory and these activities, often labelled as 'espionage', appear not to be prohibited under international law. See, e.g. Goldsmith (n 31) 114. However, it is unclear whether the legal assessment for state activities aimed at collecting intelligence in the form of espionage can be equalled with state carrying out remote search and seizure procedures for collecting extra-territorial evidence for criminal proceedings. In the opinion of the author, the legal assessment of these activities should be distinguished since the latter is generally conducted under domestic rules for criminal procedure and, as has been argued in this compendium, may be seen as an extraterritorial application of jurisdiction to enforce, and therefore a violation of the other state's sovereignty. A similar conclusion has been put forward by Tallinn Manual 2.0 experts who concluded that a state may not conduct inherently governmental functions exclusively reserved to another state on the latter's territory. Therefore, for example, if a state would conduct a LE operation against a botnet in order to obtain evidence for criminal prosecution by taking over its command and control servers located in the other state without that state's consent, the former would violate the latter's sovereignty because 'the operation usurps an inherently governmental function exclusively reserved to the territorial state under international law'. Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second Edition, Cambridge University Press 2017) 22–23.

148 Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 725–726.

149 Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict* (NATO CCD COE Publication 2012) 11.

150 ibid.

never had a definitive content'.[151] Counterarguments to this viewpoint are that if transborder searches are to be declared legal under international law, they may be abused by states, or that such searches would foment reciprocity.[152] Secondly, as an alternative to the requirement to result in inflicting damage, it can be argued that any interference with an object enjoying 'sovereign immunity' such as diplomatic premises should be seen as a violation of the sovereignty of that state.[153] Such interference may also entail transborder access.[154]

As seen from above, international law remains seemingly unclear about whether transborder investigative techniques such as remote search and seizure would constitute a violation of sovereignty. In the opinion of the author, the unclear status of transborder investigative techniques without further legal grounds or consent cannot be considered today as a 'constant and uniform practice of states /…/ in circumstances which give rise to a legitimate expectation of similar conduct in the future',[155] such that it could be seen as a rule of international customary law. Furthermore, in the opinion of the author, according to *lex lata*, conducting remote search and seizure on the territory of another state can be viewed as a breach of territorial sovereignty of the other state. This conclusion is supported by the increasingly rich evidence of international organisations and states making an effort to identify legitimate grounds for transborder investigative techniques such as remote search and seizure, be it by means of treaty provisions or within domestic frameworks. In particular, interviews with practitioners confirmed that if the location of the data to be searched is known to be on the territory of a specific state, MLA procedures or other state-to-state mechanisms should be preferred.

International organisations and state practice

Examples of international organisations moving towards more concrete norms on transborder access are the EU and the CoE. As was discussed before, the Directive on the European Investigation Order is an example of moving from MLA to mutual recognition amongst Member States. Commentators have noted that since mutual recognition gives LE an extraterritorial reach,[156] such a tendency in the fast growing area of EU criminal law and police cooperation may raise concerns regarding these developments being in line with the protection of fundamental rights and the relationship between the state and the

151 Goldsmith (n 31) 108.
152 ibid 116.
153 Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (n 103) 130.
154 Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 726.
155 International Law Association, 'Statement of Principles Applicable to the Formation of General Customary International Law' 8 <http://www.ila-hq.org/download.cfm/docid/A709CDEB-92D6-4CFA-A61C4CA30217F376> (last accessed 4 January 2017).
156 Miettinen (n 58) 178.

individual on top of ensuring the non-violation of state sovereignty.[157] Also, even though not extensively discussed in the context of remote search and seizure, the Schengen Convention Article 40(2) allows under urgent circumstances for one Member State's LE to enter the territory of another with the purpose of continuing surveillance and permits engaging in 'hot pursuit' across the borders of another Member State if in the urgency of the situation, permission of the other state cannot be obtained.[158] Lastly, the issues related to improving MLA procedures, enhancing cooperation with SPs and examining possible connecting factors for enforcement jurisdiction in cyberspace are explicitly to be addressed and presented by the European Commission by June 2017, hopefully resulting in 'specific elements for a common EU approach and proposals for its realisation, including the possibility to pursue a legislative initiative in this respect'.[159]

Perhaps the most well-known example of the 'exception to the principle of territoriality'[160] and arguably CoCC's most controversial provision is Article 32 allowing access to extraterritorially located data without the authorisation of another Party to CoCC if it is publicly available (open source) or if the data is located in another Party and the accessing Party obtains the 'lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system'. Neither of the options for transborder access require the authorisation of the other Party *per se*, but rely on the consent of the Party as a signatory to CoCC. At first sight it may seem that the consent of the owner of the data would preclude the wrongfulness of any extraterritorial access to the data under international law, and a separate legal construct under CoCC Article 32(b) would be unnecessary altogether. However, in practice, determining the identity of the owner of the data (who may also be the suspect) and acquiring his/her 'lawful and voluntary consent' is often challenging, if not impossible. The author of the dissertation believes that the development of the CoE's regulation on transborder access in the form of CoCC Article 32(b), its extensive analyses and related initiatives are in itself evidence of states agreeing that transborder access without additional authorisation of the lawful authority or the state, or other legal basis, is not in accordance with law.[161] A more detailed analysis of CoCC Article 32(b) will follow in Section 2.3.

---

157 Maria Bergström and Anna Jonsson Cornell, *European Police and Criminal Law Co-Operation* (Hart Publishing 2014) 1.

158 Crawford (n 95) 481; The Schengen acquis – Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at their Common Borders (OJ L 239, 22.9.2000) (n 50) 41.

159 Council of the European Union, 'Council Conclusions on Improving Criminal Justice in Cyberspace' (n 60) 5.

160 Council of Europe, 'T-CY Guidance Note #3: Transborder Access to Data (Article 32)' (n 28) 3.

161 Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 728.

There are also several examples of states that have preferred regulating remote search and seizure over legal ambiguity or overall *laissez-faire* approach.[162] In Belgium, the traditional search and seizure which is based on a warrant issued by the investigative judge, covers copying, making inaccessible and removing data stored in an information system.[163] In situations listed in the law, for example if endangering the public order, morality or the integrity of the data or the information systems in question, the data can also be made inaccessible using appropriate technical means.[164] LE carrying out the seizure must notify the manager of the information system of their actions and submit a summary of the data that was copied, removed, or rendered inaccessible.[165] There is a clear difference between the search and seizure of data located on the premises specified in a search warrant, and remote search and seizure which employs initially searched information systems to access other information systems or data not located on the premises. In circumstances where there is a reason to extend the search further from the initial information system found on the premises, Belgium Code of Criminal Procedure (CCP) Article 88ter would apply, and an additional approval of the investigative judge would be needed. CCP Article 88ter § 1 allows the investigative judge, under certain conditions, for example if it is necessary to 'find the truth' in the investigation, only within the limits of the search warrant, and only if other measures are disproportionate or if there is evidence that the data would be lost otherwise, to issue a warrant to LE to extend a computer search to a computer system or part thereof, even if it is located in a place other than the location of the initial search performed. Therefore, when Belgian police officers are seizing an information system, they need to ensure before the search that the device does not automatically connect to other information systems not located on the premises of the initial search, notwithstanding whether they may have information about the location of these information systems or not.[166] CCP Article 88ter § 2 restricts the extension of the search, stating that only the parts of another computer system to which the

---

[162] Henrik WK Kaspersen, 'Cybrcrime and Internet Jurisdiction' (Council of Europe 2009) 26 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042b7> (last accessed 4 January 2017); Council of Europe, 'Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY' (Cybercrime Convention Committee (T-CY)) Adopted by the 12th Plenary of the T-CY (2–3 December 2014) 7 <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf> (last accessed 4 January 2017).

[163] Code d'Instruction Criminelle (Belgium Code of Criminal Procedure), Livre Premier, 17 November 1808 39bis.

[164] ibid 39bis 3.

[165] ibid 39bis 5.

[166] 'Interview with Mr Geert Schoorens, Federal Prosecutor's Office of Belgium' (28 May 2015).

users of the initial system have access (*autorisées*) can be retrieved.[167] If it turns out that the data is not situated in domestic territory, it can only be copied (and not, e.g., made inaccessible), and the reviewing judge should promptly (although retrospectively) communicate this information to the Department of Justice, who shall inform the competent authorities of the state concerned, if it can be identified.[168] In practice, it is very difficult to determine the exact location of the data, and therefore the option of informing the other state is rarely exercised, even if CCP Article 88ter is often used for accessing data not stored domestically.[169] There is no public information on whether Article 88ter could also be used for a search from LE's own computers.[170] Even if there may be concerns that Belgium is 'clearly acting on a unilateral basis'[171] and therefore possibly breaching the other state's sovereignty, there has so far not been any open conflict on these issues with other states.[172, 173]

In the Netherlands, traditional search and seizure powers also apply to computer searches, seizing data-storage devices and copying data. Article 125j(1) of the Dutch Code of Criminal Procedure allows for, if needed for disclosing the truth, the extended search and copying of computerised systems that are located elsewhere but can be accessed from the premises of the original search. Such investigatory procedures are restricted to searches that are carried out from the devices discovered on the premises to the extent that those persons normally working or residing at that place would have access, with the permission of its owner, to the computerised system in question.[174] According to the current interpretation, such a remote search 'can not go beyond the Dutch borders.'[175] To the extent necessary to terminate the offence or prevent new offences, data can also be made inaccessible.[176] However, these provisions do not provide an explicit legal basis for a remote search from the device of the investigators if the location of the data is unknown.[177] Therefore, the Netherlands has proposed an

---

167 See the summary of a contribution by Jan Kerkhofs and Philippe Van Linthout, Belgium, April 2012 in Council of Europe, 'Transborder Access and Jurisdiction: What Are the Options?' (n 27) 32–33.

168 Code d'Instruction Criminelle (Belgium Code of Criminal Procedure), Livre Premier, 17 November 1808 (n 163) 88ter 3.

169 'Interview with Mr Geert Schoorens, Federal Prosecutor's Office of Belgium' (n 166).

170 ibid.

171 de Hert (n 106) 108.

172 'Interview with Mr Geert Schoorens, Federal Prosecutor's Office of Belgium' (n 166).

173 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 364–366.

174 Wetboek van Strafvordering (the Netherlands Code of Criminal Procedure) 1921 125j(2).

175 Bert-Jaap Koops, 'Cybercrime Legislation in the Netherlands' (2010) Vol. 14.3 Electronic Journal of Comparative Law 18 <www.ejcl.org/143/art143-10.pdf> (last accessed 4 January 2017).

176 Wetboek van Strafvordering (the Netherlands Code of Criminal Procedure) (n 174) 125o.

177 'Interview with Mr Lodewijk van Zwieten, Dutch Cyber Crime Prosecutor' (28 May 2015). Please note that the interview was conducted in May 2015 and does not reflect

extensive reform of the Dutch Criminal Code and Code of Criminal Procedure,[178] which *inter alia* mentions the possibility of allowing for, regardless of the actual location of that data, activities against the data if rules of international law are complied with.[179] The Dutch proposal puts forward amendments that would allow, with the order of the prosecutor and the consent of the investigative magistrate, for a 'platform authority' to remotely access a computer system with the purpose of making data inaccessible, recording data or communications, and extended surveillance,[180] as well as installing software within a computer or network for the purpose of aiding an investigation.[181] Since in some instances it is not possible to determine the location of the specific data sought, the ability to conduct remote search and seizure should not always depend on being able to identify the physical location of the data.[182] Former Dutch Prosecutor Mr Lodewijk van Zwieten believes that the application of the principle of ubiquity[183] would allow one to proceed even if LE cannot always prove that a crime has occurred within the Netherlands.[184] Thus, even if the location of the offending computer could not be identified by reasonable measures due to the perpetrators having used anonymisation tools such as Tor, the principle of ubiquity would allow for the assumption that the computer system is in the

changes that have occurred after that date, and that Mr van Zwieten was an acting Prosecutor at the time of the interview but became later the Seconded National Expert for Cybercrime at Eurojust.

178 Ministerie van Veiligheid en Justitie, 'Van der Steur: nieuw wetboek krijgt vorm – Nieuwsbericht – Rijksoverheid.nl' (30 September 2015) <https://www.rijksoverheid.nl/actueel/nieuws/2015/09/30/van-der-steur-nieuw-wetboek-krijgt-vorm> (last accessed 4 January 2017).

179 Rijksoverheid, 'Memorie van Toelichting Wetsvoorstel Computercriminaliteit III' (22 December 2015) 33–37 <https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/memorie-van-toelichting-wetsvoorstel-computercriminaliteit-iii> (last accessed 4 January 2017).

180 'Interview with Mr Lodewijk van Zwieten, Dutch Cyber Crime Prosecutor' (n 177).

181 See the draft of 2013, e.g. Article 125ja of the proposed bill and p 26 of the Explanatory Memorandum, Rijksoverheid, 'Opstelten Versterkt Aanpak Computercriminaliteit' (1 May 2013) <http://www.rijksoverheid.nl/ministeries/venj/nieuws/2013/05/02/opstelten-versterkt-aanpak-computercriminaliteit.html> (last accessed 4 January 2017); See also the final draft as was sent to the Parliament at Rijksoverheid, e.g. Article 126nba, Rijksoverheid, 'Wetsvoorstel Computercriminaliteit III' (22 December 2015) <https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/wetsvoorstel-computercriminaliteit-iii> (last accessed 4 January 2017).

182 'Interview with Mr Lodewijk van Zwieten, Dutch Cyber Crime Prosecutor' (n 177).

183 For example, in a case where computer systems are illegally accessed in Belgium but the computer systems in the Netherlands were used as a proxy or as a VPN to shield the origin of the attack, the Netherlands may, according to the principle of ubiquity, assume jurisdiction based on the fact that an integral part of the crime takes place in the Netherlands ibid; see also Michail Vagias, *The Territorial Jurisdiction of the International Criminal Court* (Cambridge University Press 2014) 17–24 where the author concludes that despite the critique that the doctrine of ubiquity may be too wide and flexible, it appears to be 'increasingly accepted as a manifestation of territorial jurisdiction under customary law'.

184 'Interview with Mr Lodewijk van Zwieten, Dutch Cyber Crime Prosecutor' (n 177).

Dutch jurisdiction unless it is proven that it is not.[185] For example, in cases where the Dutch authorities have fought against child pornography[186] accessible via the Tor network, it has been argued that Dutch law would be applicable for crimes committed through those websites because they could be accessed from within the Netherlands, some of the visitors could be Dutch, and it could be possible that the perpetrators were Dutch or there were other significant links to the Netherlands.[187] Otherwise, if the obligation to prove that the computer system or data is located in the Netherlands always remained with the domestic prosecutors, this would result in impunity for these crimes.[188] Mr. van Zwieten underlines that in situations where it would be possible to determine the location of the data such as would be the case with US-based Hotmail and Gmail accounts, unlike practices in many other European countries, the Netherlands would employ traditional MLA procedures.[189, 190]

The German Code of Criminal Procedure (StPO) allows searching computers for necessary data by means of a traditional search warrant, normally authorised by a judge.[191] StPO Section 110(3) is designed specifically to regulate the extended examination of an electronic storage medium. The law not only allows for the extension of the search at the premises of the person affected by the search, but also to carry out an extended search by police officers from their own devices after the initial search took place.[192] Without the need for a further warrant, the law allows, if there is a concern that the data sought would otherwise be lost, German LE to extend the search to cover also physically separate storage media insofar as they are accessible from the storage medium. Accordingly, the data that may be of significance for the investigation may be 'secured' (in practice: accessed, downloaded and copied).[193] Should it be possible to determine accurately that specific data is located in another country, MLA would be used. However, in practice, if a large international SP such as Google which uses cloud computing to store users' data is concerned, it is

---

185 The reasonable measures could also include actions that can be done after remotely accessing the computer system such as 'pinging' once there is an available 'ordinary' Internet connection. ibid.

186 See, e.g. National Rapporteur on Trafficking in Human Beings, 'Child Pornography – First Report of the Dutch National Rapporteur' (2011) 164–165 <http://www1.umn.edu/humanrts/research/Netherlands/Netherlands_child-pornography_report_2011_en.pdf> (last accessed 4 January 2017).

187 'Interview with Mr Lodewijk van Zwieten, Dutch Cyber Crime Prosecutor' (n 177).

188 ibid.

189 ibid.

190 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 366–369.

191 Search and seizure are generally, unless for exigent circumstances, authorised by a judge. See 105(1) for searches, and 98 (1) for seizures; 107 for notification. Strafprozeßordnung (German Code of Criminal Procedure), (7 April 1987; 23 April 2014) ch. VIII.

192 'Interview with Mr Rainer Franosch, Attorney General's Office of the German Federal State of Hessen' (28 May 2015).

193 ibid.

rarely possible to determine with any certainty in which foreign country the requisite data is being stored.[194] Therefore, according to Mr Franosch, the location of the data that is being accessed under StPO section 110(3) is always assumed to be (also) in Germany. The logic behind this assumption is that if the suspect accesses the data from Germany, it is almost always mirrored by one of the local SPs; and this conclusion has been reportedly confirmed by undergoing technical tests.[195, 196]

The above-quoted examples of efforts of international organisations and domestic legislations allowing for or proposing to domestically legitimise transborder access indicate a certain trend in state behaviour. Firstly, they show that these countries have deemed remote search and seizure a relevant investigative measure which should be clearly regulated in domestic law (or, these examples may be seen as pointing to an emerging consensus on the general legality of such measures). Secondly, these examples reveal that countries are increasingly looking for grounds for precluding, in a transparent manner, the wrongfulness of such searches under international law in order to make sure the activities would not be regarded as a breach of other states' sovereignty.[197]

Loss of location

Among the circumstances that have been proposed to be excluding the wrongfulness of remote search and seizure of extraterritorial data,[198] loss of location may be seen as the most prevalent justification for transborder access used by states in justifying their domestic regulation. States argue that while principles of territorial sovereignty should be recognised to the maximum extent possible, observation of such principles may not be possible where the identity of the relevant jurisdiction is unknown.[199] Furthermore, it is difficult to find workable parameters for crossborder searches in unknown jurisdictions[200] because it is not possible to consult with the interested state or request for official legal

---

194 E.g. Mr Rainer Franosch has never experienced such a situation during his career. ibid.

195 ibid.

196 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 369–371.

197 Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 731–732. For an overview of the exceptions under international law to the strict requirement of state consent as well as possibilities to broaden the international law understanding of transborder access, see Koops, B-J and Goodwin, M (n 6) 61–77.

198 Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 731–732. See also European Committee on Crime Problems and Council of Europe (n 31) 86–89; Koops, B-J and Goodwin, M (n 6) 61–77.

199 New Zealand and Law Commission (n 20) 227; Netherlands, 'Amendments to the Criminal Code and the Code of Criminal Procedure, the Improvement and Strengthening of the Detection and Prosecution of Cybercrime (Cybercrime III) – Explanatory Memorandum' 36 <http://www.internetconsultatie.nl/computercriminaliteit/document/727> (last accessed 4 January 2017).

200 New Zealand and Law Commission (n 20) 227.

assistance.[201] These concerns are illustrated by the recent Playpen case where the US Government began investigating a child pornography website ('Playpen') available only as a hidden service on the Tor network. As Tor hides the true IP addresses of its users, the Government decided to take over the website and install a piece of malware (a 'network investigative technique') on the Playpen's users' personal computers which would report back the information about the users' computers, such as the users' true IP address. However, as the use of Tor hidden services makes it impossible for investigators to know where the actual execution of the warrant would take place at, it becomes unfeasible for the Government to ensure that all of the targeted computers would be located at the US as well as sufficiently specify the target of the search warrant ('place to be searched'). As a result, there are several recent decisions arising from the same facts and circumstances demanding the evidence acquired in such a way to be regarded as inadmissible in court.[202]

Countries have found various approaches to dealing with 'loss of location' in their domestic regulations. The above-mentioned Belgian regulation is an example of domestic law allowing for unilateral access under CCP Article 88ter even if the location of the data is unknown. In the Netherlands some attempts have been made to explore the applicability of the principle of ubiquity that allows for the assumption that the computer system is in the Dutch jurisdiction unless it is proven that it is not, and therefore offering a solution to overcome the 'loss of location' issue. Also, the location of the data that is being accessed under the German StPO section 110(3) is always assumed to be (also) in Germany, thereby granting the state the necessary jurisdiction. As a recent development that took place after the publication of the articles presented in this compendium, US amended Rule 41 of the Federal Rules of Criminal Procedure, now allowing a judge to issue warrants to gain 'remote access' to computers 'located within or outside that district' in cases in which the 'district where the media or information is located has been concealed through technological means', i.e. with a possibly extraterritorial reach.[203] The amendments were target to a fair amount of criticism[204] cautioning that such transborder access might

---

[201] Dutch Minister of Security & Justice (n 136) 5.

[202] E.g. *United States v. Levin* (n 132); *United States v. Arterbury* (n 132); Orin S Kerr, 'Government "Hacking" and the Playpen Search Warrant' (*Washington Post*) <https:// www.washingtonpost.com/news/volokh-conspiracy/wp/2016/09/27/government-hacking-and-the-playpen-search-warrant/> (last accessed 4 January 2017). Please note that these decisions were taken before the amendment to US Federal Rules of Criminal Procedure Rule 41, see the next footnote.

[203] The previous wording of Rule 41 entailed a territorial limitation to the locations within the district. See, 'Current Rules of Practice & Procedure, Criminal Rules 4, 41, and 45, Redline of Amended Rules, Including Committee Notes' (*United States Courts*) 10–14 <http:// www.uscourts.gov/file/21315/download> (last accessed 4 January 2017).

[204] E.g. 'Rule 41 Coalition Letter' <https://noglobalwarrants.org/assets/Rule41Coalition Letter.pdf> (last accessed 4 January 2017); Rainey Reitman, 'With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government' (*Electronic Frontier*

result in serious diplomatic consequences, 'with short-term FBI investigations undermining the long-term international relationship building of the US State Department' and possible quick escalation of responses.[205]

Indeed, given the changed nature of threats and virtual investigations, and the complicating element of 'loss of location', we can observe state practice moving in the direction of establishing legal grounds under domestic law for conducting remote search and seizure of data in circumstances where the location of the data cannot be determined[206] or when criminals 'hide' in 'off-shore servers'.[207] This leads us to the same conclusion as de Hert who suggested that today's legal assessment on the territorial scope of jurisdiction to enforce should not be based on a court decision adopted nearly 90 years ago.[208]

However, there is no consensus opinion on this yet. There are also opposing views maintaining that state's mere inability to determine the location of the data at the moment of the access 'does not mitigate the wrong caused to the affected state of a breach of territorial integrity'.[209] These circumstances have also been compared to a situation where 'a state is not likely to accept that another state can arrest a fugitive present on the former's territory just because the former did not know of the fugitive's whereabouts'.[210, 211]

Notwithstanding these opposing ideas, this research concludes that even if we employ the territoriality principle as the basis for the interpretation and prescription of jurisdiction to enforce, rapid technological development and the

---

Foundation, 30 April 2016) <https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government> (last accessed 4 January 2017); Tor Project, 'Day of Action: Stop the Changes to Rule 41' <https://blog.torproject.org/blog/day-action-stop-changes-rule-41> (last accessed 4 January 2017) inviting the US Congress to support the 'Stop Mass Hacking Act'.

205 Ed Pilkington, 'FBI Demands New Powers to Hack into Computers and Carry out Surveillance' *The Guardian* (29 October 2014) <http://www.theguardian.com/us-news/2014/oct/29/fbi-powers-hacking-computers-surveillance> (last accessed 4 January 2017). Read more at e.g. Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 731; Richard M Thompson II, 'Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure' <https://www.fas.org/sgp/crs/misc/R44547.pdf> (last accessed 4 January 2017).

206 This condition would, however, also raise the question of the threshold of efforts that the LE needs to invest to the attempts to identify the location before being able to declare complete 'loss of location'.

207 *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp*. (n 127) 21.

208 de Hert (n 106) 72.

209 Koops, B-J and Goodwin, M (n 6) 61–62. This view is related to claims that not knowing the location of the data should not be an excuse for ignoring the law as this may be an open door for abuse in Mark Zoetekouw, 'Ignorantia Terrae Non Excusat' 1 <https://english.eu2016.nl/documents/publications/2016/03/7/c-mzoetekouw---ignorantia-terrae-non-excusat---discussion-paper-for-the-crossing-borders---jurisdiction-in-cyberspace-conference-march-2016---final> (last accessed 4 January 2017).

210 Ryngaert (n 144) 82.

211 Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 732.

need to counter sophisticated transnational crime is on the verge of making such arguments less relevant for modern states, fundamentally altering these concepts.[212] The latter can vividly be seen in the recent developments in the EU and the CoE. However, this would not mean that the concept of 'territorial sovereignty' would become less crucial in other aspects of international law. Instead, it would imply that future state behaviour will continue to shape the territorial limits of jurisdiction to enforce in outlining the exceptional circumstances for accessing digital evidence that would preclude the wrongfulness of activities that could otherwise be considered as a breach of other states' sovereignty.[213] These conclusions are also supported by the interviews conducted with practitioners suggesting that the criterion of 'location' is outdated[214] and that countries should join forces in agreeing on the common grounds of the collection of extraterritorial evidence even if this requires the relinquishing of some amount of sovereignty.[215] It has also been reasoned by some practitioners that there is already a development towards an international custom allowing transborder access but there is still a considerable lack of transparency since countries continue to deny their use of transborder access while practitioners confirm behind closed doors that this is actually standard practice.[216]

2.3. Regulation of remote search and seizure in CoE CoCC and in Estonia: uncertainty regarding law enforcement's extraterritorial powers

Description of the problem

Since many traditional criminal procedure provisions do not translate well to electronic data storage and real-time data flows,[217] CoE CoCC prescribes that 'each State Party is obligated to adopt such legislative and other measures as may be necessary, in accordance with its domestic law and legal framework, to establish the powers and procedures described [in Section 2] for the purpose of specific criminal investigations or proceedings.'[218] While Parties to CoCC are obliged to transpose certain provisions to their national legislation, the means

212 ibid 733 quoting Goldsmith (n 31) 108–109.

213 Osula, 'Transborder Access and Territorial Sovereignty' (n 36) 733 quoting Goldsmith (n 31) 116.

214 'Interview with Mr Geert Schoorens, Federal Prosecutor's Office of Belgium' (n 166).

215 'Interview with Mr Lodewijk van Zwieten, Dutch Cyber Crime Prosecutor' (n 177).

216 'Interview with Mr Rainer Franosch, Attorney General's Office of the German Federal State of Hessen' (n 192).

217 United Nations Office on Drugs and Crime (n 2) 122.

218 Council of Europe, Convention on Cybercrime (n 10); Council of Europe, 'Explanatory Report to the Convention on Cybercrime (ETS No. 185)' 141 <https://rm.coe.int/ CoERM PublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b> (last accessed 4 January 2017).

for establishing, implementing, and applying these powers and procedures within their legal system depend on the particularities of each Party's domestic law and procedures.[219] However, not all states have chosen to transpose and implement the complete set of proposed measures. For example, the Estonian Code of Criminal Law has been assessed to have satisfactorily adopted CoCC's provisions regarding substantive law, whereas not the same can be concluded about provisions regarding procedural law.[220] For instance, it is not entirely clear from the reading of the Estonian CoCP how the legal act subscribes to measures such as expedited preservation of stored computer data (CoCC Article 16) or expedited preservation and partial disclosure of traffic data (CoCC Article 17).[221] As the aim of these CoCC measures is to provide less coercive investigative techniques than traditional search and seizure, CoCC argues that it is 'essential' that states have in their domestic regulation alternative investigative powers for obtaining such data.[222]

Equally, it is unclear whether CoCC Article 19 ('Search and seizure of stored computer data') and CoCC Article 32 ('Transborder access to stored computer data with consent or where publicly available') have been transposed to the Estonian CoCP and how remote search and seizure is regulated in Estonia. This unclarity may have occurred due to the difficulties in interpreting the conditions and scope of application of CoCC Article 32(b). The lack of concrete and clear wording of the regulation draws attention to a number of possible consequences stemming from granting LE entities such broad discretionary powers. Such

---

219 Council of Europe, 'Explanatory Report to the Convention on Cybercrime (ETS No. 185)' (n 218) 145.

220 Eerik Kegandberg, 'Eesti kriminaalmenetlus: mõned rindeteated' Juridica IV/2013 256.

221 See for example, Council of Europe Cybercrime Convention Committee, 'Assessment Report: Implementation of the Preservation Provisions of the Budapest Convention on Cybercrime' (2012) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e722e> (last accessed 4 January 2017). It has been suggested that in Estonia these measures are left to be regulated by the general paragraph on the obligation to comply with orders and demands of investigative bodies and Prosecutors' Offices. See Council of Europe, 'Cybercrime Legislation – Country Profile Estonia' (2010) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042f4> (last accessed 4 January 2017); Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (n 15) 215. Expedited preservation of data as foreseen by CoCC Article 16 and Article 17 should be distinguished from the notion of 'data retention'. The former signifies the activity of keeping the already stored data secure and safe, and the latter the 'accumulation of data in the present and the keeping or possession of it into a future time period'. Council of Europe, 'Explanatory Report to the Convention on Cybercrime (ETS No. 185)' (n 218) 151. Data retention as SP's obligation is prescribed in Estonia by § 111^1 of Elektroonilise side seadus (Estonian Electronic Communication Act) (RT I 2004, 87, 593; RT I, 17.05.2016, 2). However, the current regulation is expected to be amended, see *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* (Court of Justice of the European Union).

222 Council of Europe, 'Explanatory Report to the Convention on Cybercrime (ETS No. 185)' (n 218) 170.

ambiguity may result in routine breaching of basic rights, as well as deficiency of legal certainty for individuals, which will likely need to be offset by introducing concrete remedies, legal clarity and control mechanisms over the activities of the LE.[223] Although a comprehensive analysis for specifying to what extent the procedural provisions of CoCC have been transposed to the Estonian domestic law would be appropriate and needed, this dissertation focuses particularly on the issues related to Article 19(2) and Article 32(b).

Statement set to defence

CoCC has been a visionary document in terms of foreseeing the need to harmonise cybercrime legislation and developing necessary procedural tools. However, due to the difficulties with interpreting and implementing CoCC Article 32(b), the provision is of limited assistance for CoCC Parties and for any other state attempting to address remote search and seizure of extra-territorial data domestically. The current Estonian regulation regarding remote search and seizure is unclear and in need of an update. Neither the powers prescribed in CoCC Article 19(2) nor Article 32(b) have been explicitly transposed to the domestic regulation. Given the difficulties with the inter-pretation and application of CoCC Article 32(b), the dissertation does not recommend direct transposition of the provision into Estonian law. However, the issues that have been aimed to be regulated by CoCC Article 19(2) and Article 32(b) are certainly relevant for modern LE and should therefore be considered by the domestic legislator. In particular, the scope of the current CoCP search and seizure regime should be assessed; the separation of search and seizure powers and the necessary powers for the covert collection of evidence should be analysed further; domestic law should introduce legal grounds for a remote search carried out either from the premises subject to the search warrant (extending the initial search as foreseen by CoCC Article 19(2)) or from LE's own devices; the domestic bodies suitable for granting the authorisation for accessing extraterritorially located data should be reviewed, and the difficulties in determining the location of the data that is being sought when carrying out a remote search and seizure should be domestically addressed.

Reasoning

In order to offer reasoning for the statement defined above, the following section analyses the requirements prescribed in CoCC Article 19(2) and Article 32(b), and scrutinises the difficulties regarding the interpretation of the latter. These provisions will then be compared with the regulation put forward in the current Estonian CoCP. The section will conclude with recommendations for updating the current Estonian regime regarding remote search and seizure of extra-territorial data.

---

[223] Uno Lõhmus, (2., täiend ja ümbertööt vlj, Juura 2014) 310, 313.

Remote search and seizure in CoCC

A careful reading of the CoCC's explanatory report reveals that even though Article 19 is clearly separated from Article 32 based on the territorial scope, these two articles describe very similar measures. The report notes that '[Article 19] does not address "transborder search and seizure", whereby states could search and seize data in the territory of other states without having to go through the usual channels of MLA', referring to the issue being discussed in the chapter on international co-operation.[224] Article 32 does not specifically mention 'search and seizure' but allows LE to 'access' and 'receive', thereby aiming to permit the use of accessed data for investigatory purposes but at the same time not being more specific regarding the coercive element of the allowed measures. To that end, the language used in Article 32 may have been intended to grant the Parties a certain degree of flexibility in deciding under which investigative measures transborder access as described in Article 32(b) should be transposed.[225]

Article 19(1) requires the CoCC Parties to adopt legislative and other measures as may be necessary 'to empower its competent authorities to search or similarly access a computer system or part of it and computer data stored therein, and a computer-data storage medium in which computer data may be stored in its territory,' similar to traditional search and seizure provisions in domestic legislation. Article 19's wording aims to ensure that traditional search and seizure powers that may have initially only targeted tangible objects, would also apply to search and seizure of stored computer data.[226] In addition, CoCC requires Parties to ensure that domestic provisions would allow for: the seizing or similarly securing of a computer system or part of it or a computer-data storage medium; making and retaining a copy of the data; maintaining the integrity of the data; and rendering inaccessible or removing the data in the accessed computer system.[227] Most relevant for the purposes of this dissertation is that Article 19(2) allows LE to 'extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system'. Since it is very common for individuals to store their data across a multitude of Internet-enabled devices (smartphones, tablets, laptops, personal computers, etc.) possibly through the use of additional storage mediums such as cloud services or hosting, Article 19(2) may be used to access these additional devices as long as the other computer system or part of it is 'in [the searching Party's] territory'.[228, 229]

---

[224] Council of Europe, 'Explanatory Report to the Convention on Cybercrime (ETS No. 185)' (n 218) 195.

[225] Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 351.

[226] Council of Europe, 'Explanatory Report to the Convention on Cybercrime (ETS No. 185)' (n 218) 178.

[227] Council of Europe, Convention on Cybercrime (n 10) 19(3).

[228] Council of Europe, 'Explanatory Report to the Convention on Cybercrime (ETS No. 185)' (n 218) 193.

Article 32 is not bound by the domestic territory of the Party initiating criminal proceedings and regulates extraterritorial access to stored computer data with consent or where publicly available, neither option requiring any additional authorization from the other Party. Article 32(b) allows to 'access or receive through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.' Unlike Article 32(a),[230] Article 32(b) continues to be subject to debates. In addition to doubts regarding the permissibility of such a clause under international law at all,[231] there are a number of concerns regarding its interpretation. Firstly, it appears problematic that the provision only allows to access 'stored computer data located in another Party'. Presumably due to the assumption that such access would require additional legal basis, Article 32(b) would not cover situations where the location of the data is unknown, or when it is determined that the data is located either in the territory of a country not a CoCC Party, or domestically. In fact, in such 'loss of location' situations, employing Article 32(b) in an investigation might be considered a procedural error even if there is the consent of the 'lawful authority'.[232] However, such rigid interpretation of the Article 32(b) renders it rather impractical for the use of investigation of transnational cybercrime where in practice it is not common that during an investigation and when in need to access data extraterritorially, a difference would be made between countries that are Parties to CoCC and those that are not.[233] Also, the relevance of Article 32(b) should be assessed in situations where data is indeed stored outside the territories of the Parties, or the location of data is unknown, but when there is explicit consent of the lawful

---

229 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 351–352.

230 Apart from some discussion on whether automated open-source investigations may affect the right to privacy and thereby require a legally codified basis to inform the citizens about such a possibility, transborder access to publicly available data appears to be largely uncontroversial. In fact, there is a general belief that access to open source material for criminal investigation purposes has become a commonly accepted practice and has resulted in no specific legal issues. See Bert-Jaap Koops, 'Police Investigations in Internet Open Sources: Procedural-Law Issues' (2013) 29 Computer Law & Security Review 654–655, 665; United Nations Office on Drugs and Crime (n 2) 133; Council of Europe, 'T-CY Guidance Note #3: Transborder Access to Data (Article 32)' (n 28) 4.

231 Marco Gercke, 'Understanding Cybercrime: Phenomena, Challenge and Legal Response' (International Telecommunication Union 2012) 277–278 <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf> (last accessed 4 January 2017). See also Russia refusing to sign CoCC due to this clause in Keir Giles, 'Russia's Public Stance on Cyberspace Issues' in C. Czosseck, R. Ottis and K. Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict* (NATO CCD COE Publications 2012) 67.

232 Spoenle (n 6) 8.

233 'Interview with Ms Eneli Laurits, Estonian Public Prosecutor' (6 April 2015); 'Interview with Mr Robert Laid, Estonian Assistant Prosecutor' (1 June 2015); 'Interview with Dr Oskar Gross, Police and Border Guard Board' (9 January 2017).

authority (e.g. the data subject) to disclose the data.[234] While not being able to offer Parties a concrete solution, the CoE advises the Parties in situations of loss of location to 'evaluate themselves the legitimacy of a search or other type of access in the light of domestic law, relevant international law principles or considerations of international relations.'[235, 236]

Secondly, there is a debate regarding who has the 'lawful authority to disclose the data'.[237] In this regard, the CoE remains relatively silent, except to confirm that the 'lawful authority' or being 'lawfully authorized' to disclose data may vary depending on specific circumstances, the nature of the person, and the applicable law concerned.[238] As will be discussed in the Estonian analysis below, some countries interpret the 'lawful authority' to be the domestic investigative judge. The CoE does not mention such a possible interpretation and it is unlikely that this option was foreseen when CoCC was adopted in 2001. In particular, there are controversies regarding the interpretation of SPs acting as a 'lawful authority' in disclosing data to LE. It can be argued that SPs may assume the role of 'lawful authority' and thereby provide foreign LE with requested data due to the contractual relationship between the SP and the individual.[239] At the same time, the CoE is reluctant to confirm that SPs would be able to 'consent validly and voluntarily to disclosure of their users' data under Article 32 since SPs 'will only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent'.[240] As was

---

234 The argument of the 'power of disposal' or the 'person in possession or control' as the connecting legal factor. See generally, Spoenle (n 6).

235 Council of Europe, 'T-CY Guidance Note #3: Transborder Access to Data (Article 32)' (n 28) 3.2.

236 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 352–353.

237 See generally about the arguments regarding 'lawful authority' and 'consent' in preparation of the CoE Guidance Note on Transborder Access in Micheál O'Floinn, 'It Wasn't All White Light Before Prism: Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe' (2013) 29 Computer Law & Security Review 610, 611–613.

238 An example is brought of a situation where a person's email is stored by himself or by the SP in another country, and in that case the person would have a 'lawful authority' to disclose the data to LE to permit access to the data. Council of Europe, 'Explanatory Report to the Convention on Cybercrime (ETS No. 185)' (n 218) 294.

239 Ian Walden, 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent' in Siani Pearson and George Yee (eds), *Privacy and security for cloud computing* (Springer 2013) 52; Simon Bradshaw, Christopher Millard and Ian Walden, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services' (2011) 19 International Journal of Law and Information Technology 187, 205–206; Kuan W Hon, Christopher Millard and Ian Walden, 'Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now' (2012) 16 Stanford Technology Law Review 107 <http://stlr.stanford.edu/pdf/cloudcontracts.pdf> (last accessed 4 January 2017).

240 Council of Europe, 'T-CY Guidance Note #3: Transborder Access to Data (Article 32)' (n 28) 3.6. Article 29 Working Party supported this approach by noting that private entities serving as data controllers 'cannot lawfully provide access or disclose the data to foreign law

discussed in Section 2.1, the debate regarding the issues surrounding LE's requests to SPs is of course much wider. It has long since moved on from Article 32(b)'s limited construct, and has come to focus on whether LE has the power to request data from either a foreign SP (established or headquartered in a foreign country) or a local SP (established on domestic soil), in case the data is physically stored in a foreign territory, and whether there is an obligation for the SP to respond to such requests at all.[241] In principle, if the SP is not located in the state carrying out the investigation, a traditional MLA approach would require contacting the central authority of the SP's home jurisdiction with a request for preservation and/or production of the computer data.[242] However, recent practice indicates that MLA requests may not even be sent to the country in which the data actually resides since international companies may be housing data in different data-centres located in various jurisdictions,[243] thereby again pointing at the unstable connection between the location of the data and the entity having the 'lawful authority' to provide access to such data.[244]

Thirdly, the term 'consent' is not understood exactly the same way in all legal systems. In many countries, cooperation in a criminal investigation would require explicit consent, whereas the general agreement by an individual to terms and conditions of an online service might not constitute explicit consent even if the provisions of the terms and conditions indicate that data may be shared with LE.[245] The meaning of 'voluntary' may also raise questions. For example, the EU Data Protection Regulation 2016/679 warns that 'consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.'[246] At the same time,

---

enforcement authorities that operate under a different legal and procedural framework from both a data protection and a criminal procedural point of view.' Article 29 Working Party, 'Article 29 Working Party's Comments on the Issue of Direct Access by Third Countries' Law Enforcement Authorities to Data Stored in Other Jurisdiction, as Proposed in the Draft Elements for an Additional Protocol to the Budapest Convention on Cybercrime' (2013) 3 <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf> (last accessed 4 January 2017).

241 See, e.g. Velasco, Hörnle and Osula (n 42) 470–475.

242 United Nations Office on Drugs and Crime (n 2) 217.

243 ibid 217–218; See also *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp*. (n 127), *Yahoo! Inc* (n 76).

244 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 353–354. See also generally CoE's most recent analysis regarding LE's access to evidence in the cloud in Council of Europe, 'Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY' (2016) T-CY (2016)5 Provisional <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e> (last accessed 4 January 2017).

245 Council of Europe, 'T-CY Guidance Note #3: Transborder Access to Data (Article 32)' (n 28) 3.4.

246 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) s 42.

the meaning of 'consent' differs in the context of processing personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties since the EU Data Protection Directive 2016/680 puts forward that 'where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes' and therefore the consent of the data subject, as defined in Regulation (EU) 2016/679, 'should not provide a legal ground for processing personal data by competent authorities' in the context of Directive 2016/680.[247] Moreover, in practice, the requirement of obtaining consent may not be tenable in extremely time-sensitive situations[248] and if the suspect does give explicit consent for remote access to his/her online accounts, LE would probably proceed despite the fact that the country on whose territory the data is located is not a Party to the Convention.[249, 250]

In conclusion, even though the aim of Article 32(b) – to provide investigatory access to extraterritorially located evidence – is certainly justified by the practical needs of today's LE, the legal construct of the provision contains a number of problems that preclude Parties from effective implementation. The CoE has attempted to clarify the exact meaning of the terms and concepts put forward in the clause, but has also finally concluded that Article 32(b) offers 'very limited possibilities'.[251] Furthermore, the CoE notes that in the absence of a clear and feasible international legal framework, governments have increasingly pursued unilateral solutions with risks for international relations and the rights of individuals.[252] The CoE has attempted to address these matters by proposing the adoption of a CoE Additional Protocol on Transborder Access[253] but further discussions were halted in 2014[254] due to a lack of

---

247 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 (OJ L 119, 4.5.2016) s 35.

248 Schwerha IV (n 6) 18.

249 'Interview with Mr Lodewijk van Zwieten, Dutch Cyber Crime Prosecutor' (n 177).

250 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 354–355.

251 Council of Europe, 'Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY' (n 244) 44.

252 Council of Europe, 'Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY' (n 162) 7–8.

253 Council of Europe, '(Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data' (2013) T-CY (2013) 14 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e70b6> (last accessed 4 January 2017).

254 Council of Europe, 'Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY' (n 162) 13.

consensus. In 2016, the CoE Cloud Evidence Group recommended starting negotiation of an additional Protocol to the CoCC in order to 'allow for more effective MLA, to facilitate direct cooperation with service providers in other jurisdictions when needed and subject to conditions and safeguards, to frame and establish conditions and safeguards regarding existing practices of transborder access to data and to establish data protection requirements.'[255] Unless solved by the Additional Protocol, the overall uncertainty regarding the implementation of Article 32(b) will continue and render the direct transposition of the wording of Article 32(b) impractical for Parties. Subsequently, this has resulted in a lack of harmonized regulation of such transborder investigative measures, or no regulation altogether, among the Parties to CoCC.[256]

Remote search and seizure in Estonian CoCP

The subsequent section will draw conclusions from the following issues related to the Estonian regulation: principles of Estonian criminal procedure in light of collecting digital evidence and the applicability of traditional search and seizure powers to collecting digital evidence, employing surveillance powers in order to remotely access data and CoCC Article 19(2) and Article 32(b) in Estonian law.

a. Principles of Estonian CoCP in light of collecting digital evidence and the applicability of traditional search and seizure powers

Generally, the Estonian CoCP applies to all criminal proceedings undertaken on the territory of the Republic of Estonia.[257] Evidence collected abroad or gained through MLA can be used in the Estonian criminal proceedings if evidence is collected in accordance with the principles provided in the Estonian law,[258] even though it remains unclear what exactly the principles of the Estonian criminal procedure are.[259] The Supreme Court asserts that the mere fact that another state's regulation of criminal procedure does not include all the rules that are required by Estonian law does not render evidence inadmissible in an Estonian court if they have been collected in accordance with their own domestic legislation.[260] However, neither the CoCP nor its supporting materials include

[255] Council of Europe, 'Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY' (n 244) 40.

[256] Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 355–356.

[257] Unless the extraterritorial application would arise from an international agreement or if the object of the criminal proceeding is an act of a person serving in the Defence Forces of Estonia. Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (n 15) 3(1).

[258] Eerik Kergandberg and Priit Pikamäe, *Kriminaalmenetluse seadustik: kommenteeritud väljaanne* (Juura 2012) 225; Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (n 15) 64, 65.

[259] Kergandberg and Pikamäe (n 258) 226.

[260] *3-1-1-84-09* (Estonian Supreme Court) [10.1].

distinct principles for collecting digital evidence.[261] Some of these principles may be deduced from CoCP § 64 but offer limited guidance for such investigative measures as remote search and seizure. For example, the CoCP includes an obligation that 'If technical equipment is used in collecting evidence, this must be communicated in advance to the parties involved in the procedure and they will be explained the purposes of using such technical means'.[262] Nevertheless, it remains ambiguous whether LE officials should follow this requirement in all instances of collecting evidence, such as when using technology like the Internet for collecting public source information as outlined in CoCC Article 32(a).[263]

While it can generally be concluded from case law and legal commentary that evidence in digital form is accepted in Estonian courts like any 'tangible' evidence,[264] it is not apparent whether CoCP § 91 which stipulates the traditional coercive powers for search and seizure would also cover the search of the devices found on the premises subject to a search warrant.[265] This is because the strict reading of CoCP § 91(1) prescribes an exhaustive list of possible premises subject to a search: 'The objective of a search is to find an object /…/ in a building, room, vehicle or enclosed area'. The provision has thus been interpreted as not to allow the digital environment or a computer system as an objective of a search.[266] However, when applied together with 'Inspection' (CoCP § 83, 86(2)), it is clear that CoCP § 91 may be used to access data stored on electronic devices.[267] LE may also determine that an immediate examination of the evidence found on a search premises is not reasonable due to the amount of data and the time needed for listing all the documents in the search protocol, and therefore decide that the evidence should be seized for later inspection.[268]

---

261 For discussion on the same conclusion, see Jaan Ginter and others, 'Analüüs isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses' (2013) 130–132 <http://www.kriminaalpoliitika.ee/en/analuus-isikute-pohioiguste-tagamisest-ja-eeluurimise-kiirusest-kriminaalmenetluses> (last accessed 4 January 2017).

262 Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (n 15) 64(3).

263 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 356–357.

264 CoCP's lack of clarity regarding digital evidence has been subject to critique in recent research. See, Jaan Ginter and others (n 261) 148–151. See also comments about the difficulties of qualifying digital evidence under Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (n 15) in Jaanus Tehver, 'Digitaalsete tõendite kasutamise võimaldamine' (2016) Kriminaalemetluse revisjoni töörühm 2 <http://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf> (last accessed 4 January 2017).

265 Lõhmus (n 223) 312–313.

266 Kergandberg and Pikamäe (n 258) 269. The need to interpret the search and seizure provision in order to apply to a wider range of objects may prove problematic. This is due to the principle according to which, when dealing with a possible breach of basic rights, such interpretation should only be more restrictive as opposed to more permissive. Lõhmus (n 223) 313.

267 Kergandberg and Pikamäe (n 258) 269.

268 ibid 253.

Beyond special cases such as inspecting postal deliveries, an inspection does not usually require a special warrant.[269] When analysing the content of these devices, the information relevant for the case must be identified and details of the inspection recorded.[270] There is no specific provision under the search regime allowing the LE to alter the data or make it inaccessible, which may in practice be necessary for preventing an offence or the continuation of the offence.[271] Neither does the current law include clear regulation regarding LE's possibilities for accessing devices when access is hindered for example, by the use of encryption.[272] Even if a standard procedure for this may have developed in practice, the law also does not seem to have a clear regulation in place for situations where the computer is protected by a password unknown to the investigators.[273] Overall, besides the Supreme Court's guidance on following the principle of proportionality,[274] the law sets no additional limits for seizing devices.[275] Also, it is not clear from the law whether a search warrant would grant LE the right to access or copy data from a device on the premises of an initial search – since this may facilitate determining whether all data is relevant for the investigation – or only seize a device for inspection.[276] The critique regarding the authorization for conducting search under CoCP § 91[277] has been addressed by recent CoCP amendmets.[278, 279]

The author therefore concludes that the scope of the current CoCP search and seizure regime as well the general approach for collecting digital evidence and how the principles of the CoCP would apply to this, should be reviewed. The legislator should clarify whether and under which conditions the traditional search and seizure provision CoCP § 91 can be used for searching devices on the premises identified in the search warrant or after seizing it by LE.[280] While it is certainly possible to draw up specific provisions focusing on collecting digital

---

269 Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (n 15) 89.

270 Kergandberg and Pikamäe (n 258) 257.

271 'Interview with Dr Oskar Gross, Police and Border Guard Board' (n 233).

272 ibid.

273 See a proposal for a possible solution in Tehver (n 264) 9.

274 *3-1-1-57-12* (Estonian Supreme Court) 16.

275 The 'plain view' doctrine that allows to seize objects that were discovered during the search in a 'clearly visible place' or during 'reasonable searches' was included in the current law with the September 2016 CoCP amendments as part of Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (n 15) 91(10).

276 Except for specific circumstance where seizing the whole device is necessary, a forensic copy of the device should be preferred. Jaan Ginter and others (n 261) 152. See also comments on the lack of safeguards for individuals when seizing the device and uncertainty about using copies of data stored on devices as evidence in court in Tehver (n 264) 3, 6–7.

277 Jaan Ginter and others (n 261) 102–103.

278 ibid 94–113. See Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seadus, RT I, 19.03.2015, 1 2015 RT I, 19.03.2015, 1.

279 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 357–359.

280 See more concrete proposals on the same conclusion in Tehver (n 264) 8–9.

evidence, state practice examined in this dissertation shows that traditional search and seizure powers may also be employed and appropriately expanded in order to develop or extend the capability for the collection of computer data. A separate regime for collecting digital evidence may need to be established, but the search and seizure of intangible material should not be rendered less stringent than the regime addressing the search and seizure of tangible materials since this would create an incentive for criminals to prefer the use of digital devices. While advancing domestic regulation, a balance should be struck between legal certainty and transparency regarding the proposed investigative measures and the level of scrutiny levied by regulators over an investigation which must be careful not to hinder the flexibility of investigators to keep pace with the ever-evolving digital environment.[281]

b. Employing surveillance powers to remotely access data

Besides employing search and seizure, evidence on electronic devices may also be accessed as part of 'Surveillance activities' (CoCP Chapter 3^{1}).[282] The broad distinction between covert actions directed at real-time data (such as prescribed in CoCC Article 21) and search and seizure powers to be used for accessing stored data was pointed out by the Supreme Court when stating that accessing messages (such as emails) that have reached the addressee should be done under search and seizure and inspection, whereas those still 'in transmission' should be accessed based on the authorisation of the court since they require protection under the principle of the secrecy of communication of the Constitution.[283] In practice, however, drawing the line between these two approaches has not always been so straightforward,[284] and recent case law has only partly managed to make matters clearer. In particular, different instances of the court system disagreed on whether CoCP § 126^{5} ('Covert surveillance, covert collection of comparative samples and conduct of initial examinations, covert examination and replacement of things') can be employed at all to access digital evidence such as emails stored by SPs such as Google. The Circuit Court found that CoCP § 126^{5} would not be applicable because 'emails were not [tangible] things' in the sense of the paragraph.[285] The Supreme Court, however, was of the opinion that a Google mail server itself, where the files with the emails were stored, should be seen as the 'thing' that was covertly examined.[286] It is peculiar that the questions regarding jurisdiction were not mentioned in the judgment as

---

281 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 372.

282 Kegandberg (n 220) 256.

283 *3-1-1-14-14* (Estonian Supreme Court) 816–817; Kergandberg and Pikamäe (n 258) 322.

284 'Interview with Ms Eneli Laurits, Estonian Public Prosecutor' (n 233).

285 *1-14-3029/61* (Estonian Circuit Court) 27.2.

286 *3-1-1-93-15* (Estonian Supreme Court) 89.

if 'covert examination' of a server of a foreign private company located in a foreign territory would not require any additional legal analysis.[287]

Moreover, there was confusion regarding whether covertly accessing emails stored on a SP's servers should fall under CoCP § 126^7 ('Wire-tapping or covert observation of information'). The Circuit Court asserted that emails stored on a SP's servers are still 'in transmission' because they are not solely in the possession of the addressee and therefore the addressee cannot wholly protect them from third parties.[288] However, the Supreme Court stated that since these emails are 'stored' on the server, they cannot be seen as 'in transmission', and thereby covert observation of information in the sense of CoCP § 126^7 did not take place.[289] According to this approach, covert examination of emails stored on an email account would not require the permission of the preliminary investigative judge (as prescribed in CoCP § 126^7), but can be carried out based on the authorisation of the prosecutor (as prescribed in CoCP § 126^5).[290]

The general practice of using surveillance powers to access stored data has sparked criticism. Firstly, it has been argued that the previously quoted Supreme Court ruling narrowing the interpretation of the protections afforded by the principle of secrecy of communication may be seen as contradicting the opinion of the European Court of Human Rights in regard to messages that have been received or have been prepared to be sent.[291] We can see the relevance of such protections in situations where an email is stored by a SP, having just arrived in the user's inbox of received emails but has yet to be opened or read by the addressee. Another well-known situation is where the email has been prepared but never sent, and it remains instead as a draft in the mailbox where anyone with appropriate credentials may enter to read the email without it ever being 'in transmission'.[292] Secondly, the insufficiently outlined requirements for the documentation of such surveillance have been brought out by recent research, and it has been claimed that more specific rules regarding documentation would allow the integrity of the collected data to be evaluated better.[293] Thirdly, due to the *ultima ratio* principle which advocates for surveillance measures only to be used in cases where the collection of data by other activities or taking of

---

287 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 359–360.

288 *1-14-3029/61* (n 285) 27.3; Kergandberg and Pikamäe (n 258) 258–259.

289 *3-1-1-93-15* (n 286) 92–93.

290 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 360.

291 Lõhmus (n 222) 333–334; Eerik Kergandberg, 'Eriarvamus Riigikohtu kriminaalkolleegiumi 20. novembri 2015. aasta otsuse 3-1-1-93-15 juurde' <http://www.riigikohus.ee/?id=11&tekst=222579511> (last accessed 4 January 2017).

292 E.g. Max Fisher, 'Here's the E-Mail Trick Petraeus and Broadwell Used to Communicate' *Washington Post* (12 November 2012) <https://www.washingtonpost.com/news/worldviews/wp/2012/11/12/heres-the-e-mail-trick-petraeus-and-broadwell-used-to-communicate/> (last accessed 4 January 2017).

293 Jaan Ginter and others (n 261) 153.

evidence by other procedural acts is impossible due to time constraints, unreasonable complicating factors or is especially damaging to the interests of the criminal proceedings,[294] the authorisation of surveillance activities should at all times be measured against the breach of individuals' basic rights and the potential use of other investigative measures such as inspection, and search and seizure should be considered. A concrete reasoning based on the facts of a specific case should be included in any warrant authorising such surveillance activities.[295] Taking into account the above, the author agrees that the application of surveillance powers in the context of accessing stored computer data merits further research, especially given the immediate risk to individuals' fundamental rights arising from the current lack of legislative clarity.[296] In particular, the author suggests examining the difference between the authorization needed and the application of search and seizure powers and the necessary powers for the covert collection of evidence, since the current Estonian regulation and practice do not make it evident under which circumstances these separate procedures can and should be employed, especially when it comes to accessing data that is stored extraterritorially.[297]

c. CoCC Article 19(2) and Article 32(b) in Estonian law

Searching or accessing an associated computer system or storage device that may be connected with a device located on the premises of a search and seizure site as foreseen by CoCC Article 19(2) is currently not regulated clearly in the Estonian legislation. While not unequivocally accepted, there have been discussions regarding a possible work-around to this legal void by using an analogue: should such a situation arise, the investigator should ask the permission of the preliminary investigation judge for the 'seizure and examination of postal or telegraphic items.'[298] While this approach may seemingly satisfy the legal grounds necessary for certain investigative measures, it also highlights the possible problems related to a lack of a clear regulation, the obscuring of the conditions and limits of such an extended search as well as the control mechanisms over which such coercive activities would be balanced against citizens' rights and freedoms. Equally, such an interpretation would probably not be in accordance with the previously quoted Supreme Court decision according to

294 Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (n 15) 126^{1}(2); Kergandberg and Pikamäe (n 258) 304.

295 E.g. *3-1-1-14-14* (n 283) 775.

296 Kegandberg (n 220) 255.

297 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 360–361, 372.

298 Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (n 15) 89; 'Interview with Ms Eneli Laurits, Estonian Public Prosecutor' (n 233).

which emails stored on a SP's server should not be considered as being 'in transmission'.[299]

Neither does the current law address situations where the data to be accessed is stored in the territory of another state (the situation prescribed in CoCC Article 32(b)), or where the location of the data cannot be determined altogether. Interviewed experts asserted that formal guidelines for dealing with such situations have not been developed, and that, in practice, investigators do not distinguish between data stored in Parties or non-Parties of the CoCC.[300] Interviews conducted for this dissertation reveal that there may be different approaches to accessing such data. For example, it was suggested that if the device that was to be searched under the search warrant was connected to a Google account, for example, then the data stored on SP's servers and accessible from the original device may be directly accessed and copied (without a separate warrant) since the exact location of the data cannot be determined.[301] However, before the previously quoted Supreme Court's decision, another option to gain access to such data was reported to be legitimate under warrants granted by a preliminary investigation judge under 'wire-tapping' provisions even if it was known in advance that the data would not be physically stored in Estonia.[302] This approach was reasoned by claims that the person owning the data and the devices employed to access the data were located in Estonia and that the data itself was collected and analysed also in Estonia, both activities undertaken in accordance with domestic laws;[303] and that the consent of the 'lawful authority' required by CoCC Article 32(b) may be interpreted as the authorisation of the preliminary investigation judge.[304] However, the recent Supreme Court decision may have changed this approach by claiming that only data in transmission may be accessed by the wiretapping provision, and that stored data, if surveillance activities are justified, may be covertly accessed under the authorisation of the prosecutor (as prescribed in CoCP § 126[5]). The author finds it questionable whether the authorisation of a prosecutor in cases where the data is known not to be stored on domestic territory offers sufficient control mechanisms to assess the suitability and legality of such investigative measures.[305]

The author therefore suggests that domestic law should introduce legal grounds for remote search and seizure carried out either from the premises subject

---

[299] Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 361–362.

[300] 'Interview with Ms Eneli Laurits, Estonian Public Prosecutor' (n 233); 'Interview with Mr Robert Laid, Estonian Assistant Prosecutor' (n 233); 'Interview with Dr Oskar Gross, Police and Border Guard Board' (n 233).

[301] 'Interview with Dr Oskar Gross, Police and Border Guard Board' (n 233).

[302] 'Interview with Ms Eneli Laurits, Estonian Public Prosecutor' (n 233).

[303] 'Interview with Dr Oskar Gross, Police and Border Guard Board' (n 233); 'Interview with Ms Eneli Laurits, Estonian Public Prosecutor' (n 233).

[304] 'Interview with Ms Eneli Laurits, Estonian Public Prosecutor' (n 233).

[305] Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 362–363.

to the search warrant (extending the initial search as foreseen by CoCC Article 19(2)) or from LE's own devices. A more transparent regulation should determine the scope and limits of searching data in electronic form, require a justification for using particular measures, include concrete remedies for individuals, regulate alternative measures to be used by LE in gaining access to the devices in the absence of access codes or if other technologies for hindering access have been used as well as include more concrete control mechanisms over LE's activities that would also allow the evaluation of the integrity of collected evidence. Given the possible breach of both the basic rights of individuals and the sovereignty of other countries, it should be reviewed which domestic bodies, and under which conditions, are suitable for granting the authorisation for remote search and seizure. According to the examples examined in this dissertation and in order to support the control mechanisms over LE's activities, powers for remote search and seizure of extraterritorial data should be granted under judicial supervision. It should be evaluated whether search and seizure powers could include the ability to access and copy data as well as possibly secure, remove or render data inaccessible and, under which conditions certain technical equipment such as software can be employed. If the regulation foresees the option to invite an expert to assist with the search (such as CoCP § 83(3) which prescribes the possibility for an expert to partake inspection), the powers and obligations of such experts should be clearly outlined in the law.[306] Also, the conditions for notification regarding the remote search and seizure measures (as currently foreseen by CoCP § 91(6)) should be established both for targeting data stored on the domestic territory as well as extraterritorially.[307] As such a notification before the search may prejudice the investigation, the legislator should consider allowing for the option of notifying the persons concerned after the search has been carried out (the so-called 'delayed notice').[308]

Finally, the author would like to point out that the difficulties in determining the location of the data that is being sought when carrying out a remote search and seizure should be acknowledged and addressed domestically by appropriate authorities. Specifically, formal guidelines regarding situations where the location of the data cannot be identified, should be established. Different options for going forward should be examined and assessed, taking into account both national and international restrictions.[309] The possible extraterritorial reach of the search (or

---

306 E.g. New Zealand New Zealand Search and Surveillance Act (Public Act 2012 No 24) 114.

307 E.g. ibid 132.

308 Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 372–373.

309 An example of a recent proposal is a report where Estonia suggested that 'it would be useful to be able to make virtual searches in data centres located in other countries without having to first identify the physical location of the server'. Council of the European Union, 'Evaluation Report on the Seventh Round of Mutual Evaluations 'The Practical Implementation and Operation of European Policies on Prevention and Combating Cybercrime' – Report on Estonia' (2016) 10953/15 38 <http://data.consilium.europa.eu/doc/document/ST-10953-2015-DCL-1/en/pdf> (last accessed 4 January 2017).

another investigative measure) should be legally justified. Circumstances, such as danger to life or 'loss of location' under which remote access to data stored in another territory may be necessary, should be determined domestically and, if possible, agreed upon internationally. Estonia should also take a stance on the issue of remote search and seizure in international discussions, such as the work in this regard undertaken by the EU and the CoE. The ideas of building upon the Schengen Treaty precedent, going forward with the CoE proposal for an Additional Protocol to CoCC or establishing a smaller circle of interested states that would allow for extraterritorial search and seizure between themselves are certainly commendable, even though these would most probably not solve the possible scenarios where the location of the data cannot be determined.[310] However, the author believes that such agreements between like-minded states will lead the way to a broader, hopefully perhaps even global, understanding on the accepted limits of extraterritorial investigative measures.

[310] Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (n 28) 373.

III CONCLUSION

This dissertation examines the legal regulation of remote search and seizure in circumstances where the targeted evidence is extraterritorially located or where it is not possible to identify the exact location of the data. In addition to discussing the legality of such investigative measures under international law, the dissertation focuses on CoE CoCC Article 19(2) and Article 32(b) in the light of the Estonian criminal procedure regime and offers a comparative view of selected European countries' domestic approaches, while keeping in mind the need to balance LE's operational capabilities with individual rights.

The author finds that generally, the options for accessing extraterritorially located data can be divided into two groups. Firstly, states still largely rely on traditional state-to-state approaches such as the universally used MLA process and the options developed by the EU for its Member States and the CoE for the CoCC Parties. While multilateral initiatives such as the EU Directive on the European Investigation Order, the EU option for Joint Investigative Teams as well as CoCC must certainly be commended for improving the conditions for accessing evidence in general, their efforts do not unfortunately address the full spectrum of challenges regarding remote search and seizure such as the 'loss of location'. Hence, as technologies such as VPNs, proxies, and Tor that allow users to anonymise their origin will continue to shape virtual crime scenes, states will be looking for alternative more operative approaches. This second group of measures can be characterised by 'sidestepping' the central role of states on whose territory the data is residing on (if it can be identified at all) such as directly contacting the SP or remotely accessing the data notwithstanding its location. Despite there being a lack of reporting on state practice and statistics regarding the frequency of the employment of the latter measures, recent case law indicates that these options are becoming more and more used by LE. In particular, different legal interpretations can be found regarding SP's role in providing evidence to foreign LE. According to the opinion of the author, such differences accentuate the fragmentation and lack of a common understanding regarding the legal limits of LE's mandate for accessing extraterritorially located data.

After analysing the different avenues for accessing extraterritorial data currently employed by states, the author concludes that unless the identified inefficiencies of the MLA process are addressed, the traditional focus on the territoriality principle will continue to shift gradually towards more operational investigative mechanisms that do not necessarily require the prior authorisation of the state where the data is located before the investigative measure such as search and seizure is carried out. This means that criminal proceedings involving extraterritorially located digital evidence would no longer be able to assume that the other state should always be the primary counterpart for carrying out investigative measures requiring access to evidence stored on that state's territory. As a consequence, conflicts and uncertainty between states may

occur as states' activities in accessing extraterritorial data may be breaching both national and international law, and may result in unsought escalation of retaliation measures. In this regard, the author suggests that states should move towards finding a consensus on the use of alternative measures for accessing extraterritorially located data which would entail reaching common ground on the interpretation of the limits of jurisdiction to enforce allowing for, under certain circumstances, direct access to the data or the SP without the prior authorisation of the other state. Foremost, more transparency is needed concerning state practice and official positions regarding the measures to be used for accessing extraterritorially located data. Another option for proceeding, which would certainly be more protective of the traditional territoriality principle, would be investing in reforming the current MLA procedures. Motivated stakeholders or regional organisations should continue to underline the relevance of these issues for the effective fight against cybercrime, and propose options for reform, hopefully setting an example of effective and transparent measures for other states and encouraging them to follow their lead.

In order to assess the legality of remote search and seizure of extraterritorial data under international law, the author then moves on to analysing in greater detail whether accessing data that is residing in a foreign jurisdiction without specific authorisation from the other the state or other legal grounds would exceed the territorial scope of jurisdiction to enforce, and thus result in breaching the other state's territorial sovereignty. After investigating different perspectives put forward in literature and case law, the author postulates that in addition to possibly being illegal within the other state's domestic framework, conducting remote search and seizure of extraterritorial data without basis under international law would entail an extraterritorial application of jurisdiction to enforce. At the same time it is evident from emerging examples of state practice that investigational needs and the increasing sophistication of cybercrime are slowly directing countries towards altering the level of acceptance for the limits of jurisdiction to enforce in order to best fit the requirements of LE and to avoid impunity for criminals. In situations where the location of the evidence is unknown, countries are struggling with the (re-)interpretation of the territoriality principle as the basis for determining the scope of jurisdiction to enforce.

It can be deduced from author's research that currently, neither individual countries nor international organisations have univocally supported remote search and seizure of extraterritorial data access without any additional legal grounds such as consent, nor is the legality of extraterritorial investigative measures widely supported by scholars. Despite examples of prominent cases where transborder access has indeed been employed, the author argues that transborder access without further legal grounds or consent can currently not be considered a rule of international customary law. Furthermore, since the author concludes that remote search and seizure of extraterritorial data can be viewed as an extraterritorial application of jurisdiction to enforce, the author is of the opinion that without the legal right deriving from an international treaty, consent or other grounds in international law, remote search and seizure of extraterritorial

data could be considered as a breach of territorial sovereignty. Yet, this statement should be viewed as a strict interpretation of *lex lata* and accompanied by a realistic side note underlining the effect that rapid technological development and the need to counter sophisticated transnational crime have on the interpretation of the concept of territorial sovereignty, ultimately rendering the traditional understanding and the nearly 90-year-old Lotus decision less relevant. The research undertaken for this dissertation points out examples of domestic law from Belgium, the Netherlands, Germany and the US where the changed nature of threats and virtual investigations together with the complicating element of 'loss of location' have led to the development of specific legal grounds or favourable interpretations for conducting remote search and seizure of data in circumstances where the location of the data cannot be determined. These conclusions are also supported by the conducted interviews suggesting that the criterion of 'location' is outdated. Considering the above, the author highlights that instead of legal ambiguity or overall *laissez-faire* approach, clear international regulation should be preferred, and this conclusion can also be seen reflected in examples of state practice and the work of international organisations such as the EU and the CoE.

Finally, the analytical compendium turns to examining the challenges related to the proposed regulation of remote search and seizure in CoCC Article 19(2) and Article 32(b). The author asserts that CoCC has been a visionary document in terms of foreseeing the need to harmonise cybercrime legislation and developing necessary procedural tools. However, the author also brings out a number of issues related to, in particular, the interpretation of Article 32(b). These include not addressing the circumstances of 'loss of location' as well as difficulties in determining the exact meaning of the terms 'lawful authority' and 'consent' in this context. Due to the challenges with interpreting and implementing Article 32(b), and the feedback from practitioners according to which in reality it would be uncommon for procedures to take into account whether the other country is a Party to CoCC or not, Article 32(b) is of limited assistance for CoCC Parties and for any other state attempting to address remote search and seizure of extraterritorial data domestically. The author concludes that unless solved by an Additional Protocol, the overall uncertainty regarding the implementation of Article 32(b) will continue and render the direct transposition of the wording of Article 32(b) impractical for Parties.

The author also observes that the current Estonian regulation regarding the remote search and seizure of computer systems is unclear and in need of an update and revision. Neither the powers prescribed in CoCC Article 19(2) nor Article 32(b) have been explicitly transposed to the domestic regulation. Given the difficulties with the legal construct provided for in CoCC Article 32(b), the dissertation does not recommend direct transposition of the provision into Estonian law. However, the issues that have been aimed to be regulated by CoCC Article 19(2) and Article 32(b) are certainly relevant for modern LE and should therefore be considered by the domestic legislator. In particular, the analytical compendium examines the following aspects related to the Estonian

regulation: principles of Estonian criminal procedure in light of collecting digital evidence and the applicability of traditional search and seizure powers to collecting digital evidence, employing surveillance powers to remotely access data and remotely accessing domestically or extraterritorially located data under search and seizure provisions (as proposed by the CoCC Article 19(2) and Article 32(b)). The author draws attention to the legal uncertainty accompanying the Estonian regulation regarding the conditions and limits for remote computer searches which currently include a potentially unreasonable amount of discretion to be wielded by LE entities and may result in the routine breaching of individuals' basic rights. In particular, the author proposes the following amendments to the current regime: 1) the scope of the current CoCP search and seizure regime should be assessed; 2) the separation of search and seizure powers and the necessary powers for the covert collection of evidence should be further analysed; 3) domestic law should introduce legal grounds for a remote search carried out either from the premises subject to the search warrant (extending the initial search as foreseen by CoCC Article 19(2)) or from LE's own devices; 4) the domestic bodies suitable for granting the authorisation for accessing extraterritorially located data should be reviewed, and 5) the difficulties in determining the location of the data that is being sought when carrying out remote search and seizure should be acknowledged and domestically addressed. While advancing domestic regulation, a balance should be achieved between legal certainty and transparency regarding the proposed investigative measures and the level of scrutiny levied by regulators over an investigation which must be careful not to hinder the flexibility of investigators to keep pace with the ever-evolving digital environment.

REFERENCES

Literature and publications

1. **Article 29 Working Party**, 'Article 29 Working Party's Comments on the Issue of Direct Access by Third Countries' Law Enforcement Authorities to Data Stored in Other Jurisdiction, as Proposed in the Draft Elements for an Additional Protocol to the Budapest Convention on Cybercrime' (2013) <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf> (last accessed 4 January 2017)
2. **Bellia PL**, 'Chasing Bits across Borders' [2001] U. Chi. Legal F. 35
3. **Bergström M and Jonsson Cornell A**, *European Police and Criminal Law Co-Operation* (Hart Publishing 2014)
4. **Bradshaw S, Millard C and Walden I**, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services' (2011) 19 International Journal of Law and Information Technology 187
5. **Çalışkan E, Minárik T and Osula A-M**, 'Technical and Legal Overview of the Tor Anonymity Network' <https://ccdcoe.org/sites/default/files/multimedia/pdf/TOR_Anonymity_Network.pdf> (last accessed 4 January 2017)
6. **Cassese A**, *International Law* (Second Edition, Oxford University Press 2005)
7. **Chong SC S**, 'Keynote Address by the Honourable Attorney-General' (Criminal Law Conference, 17 January 2014) <https://www.agc.gov.sg/DATA/0/Docs/NewsFiles/AG%20Speech_%20Criminal%20Law%20Conference_17%20Jan%202014.pdf> (last accessed 4 January 2017)
8. **Council of Europe**, 'Assessment Report: Implementation of the Preservation Provisions of the Budapest Convention on Cybercrime' (2012) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e722e> (last accessed 4 January 2017)
9. **Council of Europe**, 'Cybercrime Legislation – Country Profile Estonia' (2010) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042f4> (last accessed 4 January 2017)
10. **Council of Europe**, '(Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data' (2013) T-CY (2013)14 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e70b6> (last accessed 4 January 2017)
11. **Council of Europe**, 'Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY' (Cybercrime Convention Committee (T-CY)) Adopted by the 12th Plenary of the T-CY (2–3 December 2014) <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf> (last accessed 4 January 2017)
12. **Council of Europe**, 'Transborder Access and Jurisdiction: What Are the Options?' (Cybercrime Convention Committee (T-CY) 2012) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8> (last accessed 4 January 2017)
13. **Council of Europe**, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (Cybercrime Convention Committee (T-CY) 2014) T-CY(2013)17rev

<http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf> (last accessed 4 January 2017)
14. **Council of Europe**, 'Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY' (2016) T-CY (2016)5 Provisional <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e> (last accessed 4 January 2017)
15. **Council of the European Union**, 'Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime" – Report on Estonia' (2016) 10953/15 <http://data.consilium.europa.eu/doc/document/ST-10953-2015-DCL-1/en/pdf> (last accessed 4 January 2017)
16. **Crawford J**, *Brownlie's Principles of Public International Law* (8th Edition, 2012)
17. **'Crossing Borders: Jurisdiction in Cyberspace'** (2016) Conference report <http://data.consilium.europa.eu/doc/document/ST-7323-2016-INIT/en/pdf> (last accessed 4 January 2017)
18. **'Crossing Borders: Jurisdiction in Cyberspace'** (*The Netherlands EU Presidency 2016*, 7 March 2016) <https://english.eu2016.nl/events/2016/03/07/crossing-borders-jurisdiction-in-cyberspace> (last accessed 4 January 2017)
19. **De Hert P**, 'Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace – Whose Sovereignty Is at Stake' in Bert-Jaap Koops and Susan W Brenner (eds), *Cybercrime and jurisdiction: a global survey* (TMC Asser; Cambridge University Press 2006) 72.
20. **'Draft Convention on Jurisdiction with Respect to Crime'** (1935) 29 The American Journal of International Law 439
21. **Dutch Minister of Security & Justice**, 'Letter to the Dutch Parliament, Cybercrime Legislation' (15 October 2012) <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2012/10/15/wetgeving-bestrijding-cybercrime/wetgeving-bestrijding-cybercrime-1.pdf> (last accessed 4 January 2017)
22. **European Committee on Crime Problems and Council of Europe**, *Computer-Related Crime: Recommendation No. R. (89) 9 on Computer-Related Crime and Final Report of the European Committee on Crime Problems* (Council of Europe, Pub and Documentation Service; Manhattan Pub Co 1990)
23. **Fisher M**, 'Here's the E-Mail Trick Petraeus and Broadwell Used to Communicate' *Washington Post* (12 November 2012) <https://www.washingtonpost.com/news/worldviews/wp/2012/11/12/heres-the-e-mail-trick-petraeus-and-broadwell-used-to-communicate/> (last accessed 4 January 2017)
24. **Gercke M**, 'Understanding Cybercrime: Phenomena, Challenge and Legal Response' (International Telecommunication Union 2012) <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf> (last accessed 4 January 2017)
25. **Giles K**, 'Russia's Public Stance on Cyberspace Issues' in C. Czosseck, R. Ottis and K. Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict* (NATO CCD COE Publications 2012) <http://www.ccdcoe.org/publications/ 2012 proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf> (last accessed 4 January 2017)
26. **Goldsmith J**, 'The Internet and the Legitimacy of Remote Cross-Border Searches' [2001] University of Chicago Law School, Chicago Unbound <http://chicagoun

bound.uchicago.edu/cgi/viewcontent.cgi?article=1316&context=public_law_and_legal_theory> (last accessed 4 January 2017)
27. **Heinegg WH von**, 'Legal Implications of Territorial Sovereignty in Cyberspace' in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict* (NATO CCD COE Publication 2012)
28. **Heinegg WH von**, 'Territorial Sovereignty and Neutrality in Cyberspace' 89 Int'l L. Stud. 123 (2013)
29. **Hildebrandt M**, 'Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace' (2013) 63 University of Toronto Law Journal 196
30. **Hirst M**, *Jurisdiction and the Ambit of the Criminal Law* (Oxford University Press 2003)
31. **Hon W K, Millard C and Walden I**, 'Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now' (2012) 16 Stanford Technology Law Review
32. **International Law Association**, 'Statement of Principles Applicable to the Formation of General Customary International Law' <http://www.ila-hq.org/download.cfm/docid/A709CDEB-92D6-4CFA-A61C4CA30217F376> (last accessed 4 January 2017)
33. **International Telecommunication Union**, 'ICT Facts and Figures 2016' (2016) <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf> (last accessed 4 January 2017)
34. **Jaan Ginter** and others, 'Analüüs isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses' (2013) <http://www.kriminaalpoliitika.ee/en/analuus-isikute-pohioiguste-tagamisest-ja-eeluurimise-kiirusest-kriminaalmenetluses> (last accessed 4 January 2017)
35. **Justiitsministeerium**, 'Kriminaalmenetlusõiguse revisjoni lähteülesanne' <http://www.just.ee/sites/www.just.ee/files/kriminaalmenetluse_revisjoni_lahteulesanne.pdf> (last accessed 4 January 2017)
36. **Justitie M van V en**, 'Van der Steur: nieuw wetboek krijgt vorm – Nieuwsbericht – Rijksoverheid.nl' (30 September 2015) <https://www.rijksoverheid.nl/actueel/nieuws/2015/09/30/van-der-steur-nieuw-wetboek-krijgt-vorm> (last accessed 4 January 2017)
37. **Kaspersen HWK**, 'Cybrcrime and Internet Jurisdiction' (Council of Europe 2009) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042b7> (last accessed 4 January 2017)
38. **Kegandberg E**, 'Eesti kriminaalmenetlus: mõned rindeteated' Juridica IV/2013
39. **Kent G**, 'Sharing Investigation Specific Data with Law Enforcement – An International Approach' [2014] Stanford Public Law Working Paper <http://ssrn.com/abstract=2472413> (last accessed 4 January 2017)
40. **Kerr OS**, 'Searches and Seizures in a Digital World' [2005] 119 Harvard Law Review 531 <http://papers.ssrn.com/abstract=697541> (last accessed 4 January 2017)
41. **Kerr OS**, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3rd Edition, Office of Legal Education Executive Office for United States Attorneys 2009) <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf> (last accessed 4 January 2017)
42. **Kerr OS**, 'Fascinating New Case on Legal Standards for Searching a Remote Computer With Unknown Location' <http://volokh.com/2013/04/26/fascinating-new-case-on-legal-standards-for-searching-a-remote-computer-with-unknown-location/> (last accessed 4 January 2017)

43. **Kerr OS**, 'Government "Hacking" and the Playpen Search Warrant' (*Washington Post*) <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/09/27/government-hacking-and-the-playpen-search-warrant/> (last accessed 4 January 2017)
44. **Koops B-J**, 'Cybercrime Legislation in the Netherlands' (2010) Vol. 14.3 Electronic Journal of Comparative Law <www.ejcl.org/143/art143-10.pdf> (last accessed 4 January 2017)
45. **Koops B-J**, 'Police Investigations in Internet Open Sources: Procedural-Law Issues' (2013) 29 Computer Law & Security Review 654
46. **Koops B-J and Goodwin M**, 'Cyberspace, the Cloud, and Cross-Border Criminal Investigation' (2014) Tilburg Law School Research Paper 5/2016 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263> (last accessed 4 January 2017)
47. **Lõhmus U**, *Põhiõigused kriminaalmenetluses* (2., täiend ja ümbertööt vlj, Juura 2014)
48. **Marquis-Boire M** and others, 'For Their Eyes Only: The Commercialization of Digital Spying' (2013) <https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf> (last accessed 4 January 2017)
49. **Miettinen S**, *Criminal Law and Policy in the European Union* (Routledge 2013)
50. **Minárik T and Osula A-M**, 'Tor Does Not Stink: Use and Abuse of the Tor Anonymity Network from the Perspective of Law' (2016) 32 Computer Law & Security Review 111
51. **Ministerie O**, 'Dutch National Crime Squad announces takedown of dangerous botnet' (*Openbaar Ministerie*, 15 October 2010) <https://www.om.nl/actueel/nieuwsberichten/@28332/dutch-national-crime/> (last accessed 4 January 2017)
52. **National Rapporteur on Trafficking in Human Beings**, 'Child Pornography – First Report of the Dutch National Rapporteur' (2011) <http://www1.umn.edu/humanrts/research/Netherlands/Netherlands_child-pornography_report_2011_en.pdf> (last accessed 4 January 2017)
53. **New Zealand and Law Commission**, *Search and Surveillance Powers* (Law Commission 2007) <http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R97.pdf> (last accessed 4 January 2017)
54. **O'Floinn M**, 'It Wasn't All White Light Before Prism: Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe' (2013) 29 Computer Law & Security Review 610
55. **Oppenheim L**, *Oppenheim's International Law* (9th Edition, Longman 1996)
56. **Osula A-M**, 'Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data' (2015) Vol 9 Masaryk University Journal of Law and Technology 43
57. **Osula A-M**, 'Transborder Access and Territorial Sovereignty' (2015) 31 Computer Law & Security Review 719
58. **Osula A-M**, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (2016) 24 (4) International Journal of Law and Information Technology 343
59. **Peers S and De Capitani E**, 'EU Law Analysis: The European Investigation Order: A New Approach to Mutual Recognition in Criminal Matters' <http://eulawanalysis.blogspot.com/2014/05/the-european-investigation-order-new.html> (last accessed 4 January 2017)

60. **Pilkington E**, 'FBI Demands New Powers to Hack into Computers and Carry out Surveillance' *The Guardian* (29 October 2014) <http://www.theguardian.com/us-news/2014/oct/29/fbi-powers-hacking-computers-surveillance> (last accessed 4 January 2017)
61. **Reitman R**, 'With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government' (*Electronic Frontier Foundation*, 30 April 2016) <https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government> (last accessed 4 January 2017)
62. **'Rule 41 Coalition Letter'** <https://noglobalwarrants.org/assets/Rule41CoalitionLetter.pdf> (last accessed 4 January 2017)
63. **Ryngaert C**, *Jurisdiction in International Law* (Second Edition, Oxford University Press 2015)
64. **Schmitt MN** (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second Edition, Cambridge University Press 2017)
65. **Schmitt MN** (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013)
66. **Schneier B**, 'Anonymity and the Internet' <https://www.schneier.com/blog/archives/2010/02/anonymity_and_t_3.html> (last accessed 4 January 2017)
67. **Schwerha IV JJ**, 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"' (2010) Council of Europe Project on Cybercrime <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3dc> (last accessed 4 January 2017)
68. **Seitz N**, 'Transborder Search: A New Perspective in Law Enforcement' (2004) 7 Yale JL & Tech. 23
69. **Shaw MN**, *International Law* (Cambridge University Press 2008)
70. **Spoenle J**, 'Cloud Computing and Cybercrime Investigations: Territoriality vs. the Power of Disposal?' (CoE 2010) Discussion paper <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df> (last accessed 4 January 2017)
71. **Svantesson D**, 'Preliminary Report: Law Enforcement Cross-Border Access to Data' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2874238 <https://papers.ssrn.com/abstract=2874238> (last accessed 4 January 2017)
72. **Taylor M** and others, 'Forensic Investigation of Cloud Computing Systems' (2011) 2011 Network Security 4
73. **Tehver J**, 'Digitaalsete tõendite kasutamise võimaldamine' (2016) Kriminaalemetluse revisjoni töörühm <http://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf> (last accessed 4 January 2017)
74. **Thielman S**, 'Silk Road Operator Ross Ulbricht Sentenced to Life in Prison' *Guardian* (29 May 2015) <https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced> (last accessed 4 January 2017)
75. **Thompson II RM**, 'Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure' <https://www.fas.org/sgp/crs/misc/R44547.pdf> (last accessed 4 January 2017)
76. **Tor Project**, 'Day of Action: Stop the Changes to Rule 41' <https://blog.torproject.org/blog/day-action-stop-changes-rule-41> (last accessed 4 January 2017)
77. **Tor Project**, 'Tor Metrics – Direct Users by Country' <https://metrics.torproject.org/userstats-relay-country.html> (last accessed 4 January 2017)
78. **Tor Project**, 'Tor: Overview' <https://www.torproject.org/about/overview>

79. **Tor Project**, 'Users of Tor' <https://www.torproject.org/about/torusers.html.en>
80. **United Nations Office on Drugs and Crime**, 'Comprehensive Study on Cybercrime' (2013) <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> (last accessed 4 January 2017)
81. **United States Department of Justice**, 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage' (19 May 2014) <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor> (last accessed 4 January 2017)
82. **United States Department of Justice**, 'U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator' (2 June 2014) <https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware> (last accessed 4 January 2017)
83. **Vagias M**, *The Territorial Jurisdiction of the International Criminal Court* (Cambridge University Press 2014)
84. **Velasco C, Hörnle J and Osula A-M**, 'Global Views on Internet Jurisdiction and Trans-Border Access' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move*, vol 24 (Springer Netherlands 2016)
85. **Walden I**, *Computer Crimes and Digital Investigations* (Oxford University Press 2007)
86. **Walden I**, 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent' in Siani Pearson and George Yee (eds), *Privacy and security for cloud computing* (Springer 2013)
87. **Wikileaks**, 'SpyFiles 4' (2014) <https://wikileaks.org/spyfiles4/index.html> (last accessed 4 January 2017)
88. **Williams RD**, '(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action' (2011) 79 The George Washington Law Review <http://www.gwlr.org/wp-content/uploads/2012/08/79-4-R_Williams.pdf> (last accessed 4 January 2017)
89. **Wilske S and Schiller T**, 'International Jurisdiction in Cyberspace: Which States May Regulate the Internet' (1997) 50 Fed. Comm. LJ 117
90. **Woods AK**, 'Data Beyond Borders: Mutual Legal Assistance in the Internet Age' (2015) Global Network Initiative <https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf> (last accessed 4 January 2017)
91. **Young SM**, 'Verdugo in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases' (Social Science Research Network 2004) SSRN Scholarly Paper ID 539942 <http://papers.ssrn.com/abstract=539942> (last accessed 4 January 2017)
92. **Zoetekouw M**, 'Ignorantia Terrae Non Excusat' <https://english.eu2016.nl/documents/publications/2016/03/7/c-mzoetekouw---ignorantia-terrae-non-excusat---discussion-paper-for-the-crossing-borders---jurisdiction-in-cyberspace-conference-march-2016---final> (last accessed 4 January 2017)

Normative documents and commentary

93. Brazil, Law No. 12.965, April 23rd 2014
94. Code d'Instruction Criminelle (Belgium Code of Criminal Procedure), Livre Premier, 17 November 1808
95. Council of Europe, Convention on Cybercrime, ETS No. 185, RT II 2003, 9, 32 2001
96. Council of Europe, 'Convention on Cybercrime, List of Signatories and Ratifications.' <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG> (last accessed 4 January 2017)
97. Council of Europe, European Convention on Mutual Assistance in Criminal Matters, ETS no. 030 1959
98. Council of Europe, 'Explanatory Report to the Convention on Cybercrime (ETS No. 185)' <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b> (last accessed 4 January 2017)
99. Council of Europe, 'T-CY Guidance Note # 3: Transborder Access to Data (Article 32)' (Cybercrime Convention Committee (T-CY) 2014) T-CY (2013)7 E <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)7REV_GN3_transborder_V12adopted.pdf> (last accessed 4 January 2017)
100. Council Act of 16 October 2001 Establishing, in Accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 326, 21.11.2001)
101. 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)
102. Council Framework Decision 2003/577/JHA of 22 July 2003 on the Execution in the European Union of Orders Freezing Property or Evidence (OJ L 196, 2.8.2003)
103. Council Framework Decision 2008/978/JHA of 18 December 2008 on the European Evidence Warrant for the Purpose of Obtaining Objects, Documents and Data for use in Proceedings in Criminal Matters (OJ L 350, 30.12.2008)
104. Council of the European Union, 'Council Conclusions on Improving Criminal Justice in Cyberspace' (2016), 9 June 2016
105. Council of the European Union, 'Council Conclusions on the European Judicial Cybercrime Network' (2016), 9 June 2016
106. 'Current Rules of Practice & Procedure, Criminal Rules 4, 41, and 45, Redline of Amended Rules, Including Committee Notes' (United States Courts) <http://www.uscourts.gov/file/21315/download> (last accessed 4 January 2017)
107. 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 (OJ L 119, 4.5.2016)
108. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 Regarding the European Investigation Order in Criminal Matters (OJ L 130, 1.5.2014) 2014
109. Elektroonilise side seadus (Estonian Electronic Communication Act) (RT I 2004, 87, 593; RT I, 17.05.2016, 2)

110. Kergandberg E and Pikamäe P, Kriminaalmenetluse seadustik: kommenteeritud väljaanne (Juura 2012)
111. Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seadus, RT I, 19.03.2015, 1 2015
112. Kriminaalmenetlusseadustik (Estonian Code of Criminal Procedure) (RT I 2003, 27, 166; RT I, 20.05.2016, 1)
113. Netherlands, 'Amendments to the Criminal Code and the Code of Criminal Procedure, the Improvement and Strengthening of the Detection and Prosecution of Cybercrime (Cybercrime III) – Explanatory Memorandum' <http://www.internetconsultatie.nl/computercriminaliteit/document/727> (last accessed 4 January 2017)
114. New Zealand Search and Surveillance Act (Public Act 2012 No 24)
115. 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)
116. Rijksoverheid, 'Memorie van Toelichting Wetsvoorstel Computercriminaliteit III' (22 December 2015) <https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/memorie-van-toelichting-wetsvoorstel-computercriminaliteit-iii> (last accessed 4 January 2017)
117. Rijksoverheid, 'Opstelten Versterkt Aanpak Computercriminaliteit' (1 May 2013) <http://www.rijksoverheid.nl/ministeries/venj/nieuws/2013/05/02/opstelten-versterkt-aanpak-computercriminaliteit.html> (last accessed 4 January 2017)
118. Rijksoverheid, 'Wetsvoorstel Computercriminaliteit III' (22 December 2015) <https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/wetsvoorstel-computercriminaliteit-iii> (last accessed 4 January 2017)
119. Strafprozeßordnung (German Code of Criminal Procedure) (7 April 1987; 23 April 2014)
120. Swiss Criminal Code of 21 December 1937 (Status as of 1 October 2016)
121. The Schengen acquis – Convention Implementing the Schengen Agreement of 14 June 1985 Between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at their Common Borders (OJ L 239, 22.9.2000)
122. Wetboek van Strafvordering (the Netherlands Code of Criminal Procedure) 1921

Case law

123. Kerganberg E, 'Eriarvamus Riigikohtu kriminaalkolleegiumi 20. novembri 2015. aasta otsuse 3-1-1-93-15 juurde' <http://www.riigikohus.ee/?id=11&tekst=222579511>
124. *1-14-3029/61* (Estonian Circuit Court)
125. *3-1-1-14-14* (Estonian Supreme Court)
126. *3-1-1-57-12* (Estonian Supreme Court)
127. *3-1-1-84-09* (Estonian Supreme Court)
128. *3-1-1-93-15* (Estonian Supreme Court)
129. *Case concerning the arrest warrant of 11 April 2000 (Democratic Republic of Congo v Belgium): judgment of 14 February 2002, Dissenting Opinion of Judge van den Wyngaert* (International Court of Justice)
130. *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753, 758 (S.D. Tex. 2013)

131. *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* (Court of Justice of the European Union)
132. *The Case of the SS Lotus, Fr v Turk, 1927 PCIJ (ser A) No 10 (Decision No 9)* (Permanent Court of International Justice)
133. Government's Brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within its Custody and Control, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp*., 13 Mag. 2814 WL 1661004 (S.D.N.Y. 2014)
134. *United States v. Levin*, 15-10271-WGY, 2016 WL 2596010 (D. Mass. 2016)
135. *United States v. Arterbury*, 15-CR-182-JHP, 2016 BL 133752 (N.D. Okla. 2016)
136. *United States v Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui,* 14-118 (W.D. Pa. 2014)
137. *United States v Gorshkov*, 2001 WL 1024026 (W.D. Wash. 2001)
138. *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp*., 13 Mag. 2814 WL 1661004 (S.D.N.Y. 2014)
139. *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp*., No. 14-2985 (2d Cir. 2016)
140. Brief for appellant, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp*., 14-2985-cv (2d Cir. 2014)
141. *Yahoo! Inc* [2013] Belgium Court of Appeal of Antwerp, 12th chamber for criminal cases 2012/CO/1054
142. *Yahoo! Inc* [2015] Court of Cassation of Belgium P.13.2082.N

Interviews

143. 'Interview with Ms Eneli Laurits, Estonian Public Prosecutor' (6 April 2015)
144. 'Interview with Ms Imbi Markus, Estonian Ministry of Justice' (14 May 2015)
145. 'Interview with Mr Geert Schoorens, Federal Prosecutor's Office of Belgium' (28 May 2015)
146. 'Interview with Mr Lodewijk van Zwieten, Dutch Cyber Crime Prosecutor' (28 May 2015)
147. 'Interview with Mr Rainer Franosch, Attorney General's Office of the German Federal State of Hessen' (28 May 2015)
148. 'Interview with Mr Robert Laid, Estonian Assistant Prosecutor' (1 June 2015)
149. 'Interview with Dr Oskar Gross, Police and Border Guard Board' (9 January 2017)

ACKNOWLEDGEMENTS

Writing this dissertation has been a long and interesting journey. I would like to thank the University of Tartu and the Republic of Estonia for the support provided to PhD students. I would also like to thank the Estonian Ministry of Education and Research and Foundation Archimedes for the Kristjan Jaak scholarship that allowed me to benefit from the academic environment in Waseda University, Japan. Equally I would like to thank the European Social Fund's Doctoral Studies and Internationalisation Programme DoRa, carried out by Foundation Archimedes, for making possible my research in the London Institute of Legal Studies which was essential for gathering material for article II 'Transborder Access and Territorial Sovereignty'. In addition, my appreciation goes to the Police and Border Guard Board for their research and development scholarship provided for the compilation of this analytical compendium, and to NATO CCD COE for valuable experience and opportinities for expanding my research.

Many wonderful individuals have inspired, encouraged and helped me along the way, sometimes maybe not even fully acknowledging their role. I am very grateful to Prof Jaan Ginter, Prof Yukio Kawamura, Prof Marco Gercke, Prof Ian Walden, Colin Sweet, Dr Marko Kairjak, Eneli Laurits, Imbi Markus, Robert Laid, Rainer Franosch, Lodewijk van Zwieten, Geert Schoorens, Prof Dan Svantesson, Mark Zoetekouw, Dr Oskar Gross, Henry Rõigas, Tiit Kuuskmäe and the anonymous reviewers of the articles.

Lastly, my deepest gratitude belongs to my whole family, especially to my husband and our daughter, who have always been there for me and without whose support I could not have completed this work.

SUMMARY IN ESTONIAN

Piiriüleste andmete kaugläbiotsimine

Tänaseks päevaks on ligipääs Internetile rohkem kui kolmel miljardil inimesel[311] ning aastaks 2020 on Internetiga ühendatud seadmete arv ennustatavalt kuus korda suurem kui maailma elanikkond.[312] Kasvav digitaliseeritus tähendab kriminaalmenetluse jaoks seda, et üha rohkem tuleb arvestada nii Interneti, sellega seotud tehnoloogiate kui ka digitaalselt salvestatud või elektrooniliselt edastatud andmete omapäradega. Digitaalselt salvestatud andmete rolli kasvu kriminaalmenetluses tuleb vaadelda koos andmete asukoha problemaatikaga, sest aina enam tekib olukordi, kus uurimise käigus kogutavad tõendid ei asu menetlust läbiviiva riigi territooriumil. Siinkohal võib näitena tuua arvutikuritegevuses tihti kasutatavad robotvõrgud, mis võivad koosneda enam kui sajast tuhandest nakatunud arvutist üle maailma ning kus uurimise läbiviimiseks peavad jõud ühendama kümnete riikide uurimisasutused ja erasektor.[313] Tänapäeval väga populaarsed pilvetehnoloogiad on teine näide, kus andmete salvestamine ainult kasutaja koduriigi territooriumil on pigem erand kui reegel ning peegeldatud andmebaaside, erinevate serverite ning rakenduste tõttu ei suuda tihtipeale isegi teenuseosutajad (edaspidi *TO*) täielikult identifitseerida andmete tegelikku asukohta.[314] Kolmandaks näiteks, mil viisil nüüdisaegsed tehnoloogiad mõjutavad kriminaalmenetluse läbiviimist, on Tor ja teised sarnased veebirakendused, mis võimaldavad kasutaja tegeliku identiteedi ja asukoha anonümiseerida.[315] Tuginedes eelnevale keskendub käesolev väitekiri küsimusele, kuidas mõjutab uurimisasutuste kohtueelse menetluse läbiviimise õiguspäraseid võimalusi ja võimekust see, kui uurimise käigus kogutavad andmed asuvad teise riigi territooriumil või kui andmete asukohta pole võimalik kindlaks määrata. See valdkond pole oluline pelgalt arvutikuritegevuse vastu võitlemisel, sest üha enam kasutatakse digitaalseid tõendeid ka muude kuritegude menetlemisel.

Väitekiri põhineb autori poolt avaldatud viiel õigusteaduslikul artiklil:

1. Osula, Anna-Maria (2015). Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data. Masaryk University Journal of Law and Technology, Vol 9, 43–64. Artikkel analüüsib erinevaid viise, kuidas uurimisasutused saavad kohtueelse menetluse raames ligipääsu piiriülestele andmetele. Eraldi käsitletakse õigusabitaotluste protseduuride kriitikat ning infotehnoloogia arengu ja digitaalsete tõendite rolli tähtsuse kasvu tõttu populaarsust koguvaid alternatiive tavapärastele õigusabitaotlustele.

---

311 International Telecommunication Union (n 1).

312 United Nations Office on Drugs and Crime (n 2), xvii.

313 Näiteks nakatas hiljutine Zeus 'Gameover' robotvõrk 500,000-1,000,000 arvutit üle kogu maailma. United States Department of Justice, 'U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator' (n 5).

314 Taylor and others (n 7) 7.

315 Minárik and Osula (n 8).

2. Osula, Anna-Maria (2015). Transborder Access and Territorial Sovereignty. Computer Law and Security Review, 31 (6), 719–735. Artikkel keskendub kaugläbiotsimise seaduslikkusele rahvusvahelises õiguses. Autor analüüsib täidesaatva jurisdiktsiooni ning territoriaalse suveräänsuse tähendust kaugläbiotsimise korral. Erinevate riikide õiguspraktika näitel arutletakse ka selle üle, kas nn 'asukoha puudumist' (*loss of location*) võib teatud tingimustel pidada õigusvastasust välistavaks asjaoluks rahvusvahelise õiguse ja kaugläbiotsimise kontekstis.
3. Minárik, Tomas; Osula, Anna-Maria (2016). Tor Does Not Stink: Use and Abuse of the Tor Anonymity Network from the Perspective of Law. Computer Law and Security Review, 32 (1), 111–127. Artikkel lahkab Tor'i kui ühe levinuima anonüümsust võimaldava veebirakendusega seotud tehnilisi ja õiguslikke küsimusi. Eelkõige analüüsitakse Tor'i toimemehhanisme, mis võimaldavad tekitada 'asukoha puudumist' ning millest tulenevad mitmed väljakutsed nii uurijatele kui õiguskorrale üldiselt.
4. Velasco, Cristos; Hörnle, Julia; Osula, Anna-Maria (2016). Global Views on Internet Jurisdiction and Trans-Border Access. In: Gutwirth, Serge; Leenes, Ronald; De Hert, Paul (Ed.). Data Protection on the Move (465–476). Springer Netherlands. Law, Governance and Technology Series, 24. Artiklisse on koondatud läbivad õigusprobleemid, mis kerkivad üles piiriülestele andmetele ligipääsul ning erinevate jurisdiktsioonide võimalikul kohaldumisel, sealhulgas Euroopa Nõukogu (EN) arvutikuritegevusevastase konventsiooni ning TO õiguste ja kohustustega seotud küsimused.
5. Osula, Anna-Maria (2016). Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study. International Journal of Law and Information Technology, 24 (4), 343–373. Artikkel analüüsib Euroopa Nõukogu arvutikuritegevusevastase konventsiooni artikleid, mis on seotud kaugläbiotsimisega ning keskendub artikkel 32(b) tõlgendamisraskustele. Intervjuud Belgia, Madalmaade, Saksamaa ning Eesti arvutikuritegevusele spetsialiseerunud prokuröridega annavad ainest riikide kaugläbiotsimise regulatsioonide võrdlusele. Kaugläbiotsimisega seotud probleemide valguses uurib artikkel detailsemalt Eesti kehtivat regulatsiooni ning teeb ettepanekuid, mida võiks seadusandluse täiendamisel silmas pidada.

Kokkuvõtvalt on väitekirja eesmärgiks uurida, lähtudes ühe näitena EN arvutikuritegevusevastasest konventsioonist[316] (edaspidi *konventsioon*), kuidas reguleeritakse 'kaugläbiotsimist' (*remote search and seizure*) olukorras, kus kriminaalmenetluse tarbeks vajalikud digitaalsed tõendid asuvad väljaspool kriminaalasja menetleva riigi territooriumi (edaspidi *piiriülene kaugläbiotsimine*) või kui nende andmete geograafilist asukohta ei ole võimalik kindlaks määrata. Sealjuures peetakse kaugläbiotsimise all silmas läbiotsimist, mida toimetatakse (arvuti)süsteemis ning mida laiendatakse läbi selle (arvuti)süsteemi teistesse

316 Council of Europe, Council of Europe, Convention on Cybercrime (n 10).

mujal asuvatesse (arvuti)süsteemidesse (näiteks konventsiooni artikkel 19(2) alusel) või mida viiakse läbi kriminaalmenetlust toimetavate uurimisasutuste (arvuti)süsteemide kaudu. Lisaks piiriülese kaugläbiotsimise õiguslikkuse analüüsimisele rahvusvahelise õiguse kontekstis keskendub väitekiri spetsiifilisemalt konventsiooni artiklitele 19(2) ja 32(b) ning küsib, kas ja mil viisil on need artiklid üle võetud Eesti siseriiklikku kriminaalmenetlusõigusesse. Piiriülese kaugläbiotsimise regulatsiooni uurimise käigus pakub doktoritöö võrdleva vaate ka Belgia, Madalmaade ja Saksamaa lähenemistele, kus õiguslike dokumentide analüüsi täiendavad intervjuud nimetatud riikide arvutikuritegevusele spetsialiseerunud prokuröridega.[317] Analüüsiobjektiks valitud riikide regulatsioonid peegeldavad ühelt poolt nii romaani kui germaani õigusperekondade lähenemisi ning teiselt poolt näitavad, kuivõrd eriilmelised on pakutud õiguslikud lahendused neljas samaaegselt Euroopa Liitu (EL) kuuluvas ning konventsiooni ratifitseerinud riigis.

Väitekirja koostamisel on peamiselt kasutatud analüütilist, võrdlevat ja teleoloogilist meetodit.

Väitekiri keskendub kaugläbiotsimisele ega analüüsi detailsemalt muid kriminaalmenetlusõiguses reguleeritud viise piiriülestele andmetele liigpääsuks.

Uurimistöö praktilise tulemusena pakub väitekiri välja elemendid, mida tuleks Eesti kriminaalmenetlusseadustiku uuendamisel silmas pidada, võttes eesmärgiks tagada samaaegselt nii kriminaalmenetluse efektiivsus kui ka siseriiklike ja rahvusvaheliste normide järgimine. Autor loodab, et töö käigus tehtud järeldustest on kasu ka teiste riikide seadusandjatel, sest kaugläbiotsimisega seotud probleeme tõstatatakse üha enam nii eri riikide siseriikliku seadusandluse kui ka EL ja EN õigusloome kontekstis.

Eelpool nimetatud eesmärgini jõudmiseks on autor püstitanud kolm uurimisküsimust.

- Kuidas on informatsioonitehnoloogia ja digitaalsete tõendite rolli kasv mõjutanud kohtueelse menetluse läbiviimiseks sobivaimate meetmete valikut olukorras, kus kaugläbiotsimise käigus tuleb ligi pääseda andmetele, mis ei asu selle riigi territooriumil?
- Kas piiriülene kaugläbiotsimine kätkeb endas täidesaatva jurisdiktsiooni piiriülest kohaldamist ning kas seda saab seeläbi vaadelda teise riigi territoriaalse suveräänsuse rikkumisena; ning kuidas mõjutab 'asukoha puudumine' territoriaalse suveräänsuse tõlgendamist?
- Kas Eesti on siseriiklikku õigusesse üle võtnud konventsiooni artiklid 19(2) ja 32(b), kas kehtiv regulatsioon pakub lahendusi piiriülese kaugläbiotsimisega seonduvalt tõusetunud probleemidele ning arvestades väitekirjas välja toodud EL riikide seadusandluse näiteid, kas ja kuidas peaks kehtivat normatiivset lähenemist uuendama?

[317] Tuleb märkida, et intervjuud ei peegelda selle riigi ametlikku lähenemist piiriülesele kaugläbiotsimisele kriminaalmenetluses vaid pigem osutavad praktikas üleskerkinud probleemidele.

Alljärgnevalt esitab autor kokkuvõtte töös esitatud väidetest ja nende põhjendustest.

I Meetmed piiriülestele andmetele ligipääsu tagamiseks kriminaalmenetluse raames

Kaitsmisele kuuluv väide

Meetmed kriminaalmenetluse läbiviimisel piiriülestele andmetele ligipääsuks saab üldjoontes jagada kahte gruppi: 1) riikidevahelised meetmed ning 2) meetmed, mis ei lähtu tingimata andmete asukohariigist ja selle nõusolekust andmetele ligi pääseda. Kui riigid ei panusta vastastikuse õigusabitaotluste süsteemi parendamisse või teistesse riikidevaheliste lahenduste arendamisse, väheneb territoriaalse suveräänsuse roll, mille alusel eeldatakse traditsiooniliselt, et kriminaalmenetluse raames andmete piiriülese kogumise teiseks (ning menetlustoimingut autoriseerivaks) osapooleks peaks olema riik, mille territooriumil need andmed asuvad. Selle asemel nihkub praeguse praktika järgi uurimisasutuste eelistus operatiivsematele meetmetele, mis teise riigi eelnevat heakskiitu menetlustoiminguile nagu kaugläbiotsimine tingimata ei vaja. Kuivõrd piiriülestele andmetele ligipääsul võidakse rikkuda nii siseriiklikku kui rahvusvahelist õigust ning olukord võib päädida soovimatu eskalatsiooni ja vastumeetmetega, võivad sageneda riikidevahelised konfliktid ja levida üldine ebakindlus.

Probleemi kirjeldus ja põhjendused

Väitekirja analüüsi tulemusena võib hetkel kasutatavad meetmed digitaalsete tõendite piiriüleseks kogumiseks jagada üldjoontes kaheks. Esiteks meetmed, mis lähtuvad eelkõige riigist, kelle territooriumil andmed asuvad ning võtavad kas formaalseid või vähemformaalseid kanaleid kasutades ühendust selle riigi esindajatega. Siia alla kuuluvad näiteks rahvusvaheliste lepingute alusel esitatavad rahvusvahelised õigusabi taotlused, mis Ühinenud Rahvaste Organisatsiooni (ÜRO) hiljutise uuringu kohaselt moodustavad digitaalsetele andmetele ligipääsuks kasutavatest meetmetest hinnanguliselt 70%.[318] Kuid seoses digitaalsete tõendite volatiilsusega ehk ohuga, et need võivad kiiresti hävida, on vastastikuse õigusabi mehhanism saanud mitmesugust kriitikat. Nimelt võib vastastikusele õigusabi taotlusele vastust oodata mitmeid kuid. Hiljutised uuringud on välja toonud ka muid õigusabitaotlustega seotud probleeme – näiteks standardse lähenemise puudumine ja seega mehhanismide erisused riigiti, erinevad pädevad uurimisasutused olenevalt andmete iseloomust, protsessi üldine keerukus ja ressursimahukus, õigusabi kohaldamatus osades riikides või juhtumite puhul, kus tekitatud kahju jääb alla teatud piirmäära, õigusabi taotlemiseks vajalike lepingute puudumine, üldised kommunikatsiooniprobleemid ja õigus-

[318] See järeldus on tehtud 69 riigi tagasiside põhjal. United Nations Office on Drugs and Crime (n 2) 201.

süsteemide erisused.[319] EN uurimisrühm on kokkuvõtvalt nentinud, et õigusabitaotluste süsteem on üldiselt ebaefektiivne ning digitaalsete tõendite saamiseks lausa sobimatu, takistades riigi võitlust kuritegevusega, mille menetlemiseks on vajalikud piiriülesed digitaalsed tõendid.[320]

EL ja EN on kaks näidet rahvusvahelistest organisatsioonidest, kes on efektiivsema rahvusvahelise koostöö tarbeks välja arendanud spetsiaalsed instrumendid. Neist hiljutisema näitena võib tuua Euroopa Parlamendi ja Nõukogu Direktiivi 2014/41/EL, mis käsitleb Euroopa uurimismäärust kriminaalasjades. Selles sisalduva vastastikuse tunnustamise põhimõtte[321] eesmärgiks on paremini toimiv liikmesriikidevaheline koostöö, kuid kahjuks ei paku direktiiv siiski täielikku lahendust digitaalsete tõendite ajakriitilise hankimise vajadusele, sest näeb taotluste puhul ette kuni 90-päevase vastamisaja.[322] Piiriülese kaugläbiotsimise seaduslikkuse osas seisukoha võtmise jaoks on kindlasti oluline ka Euroopa Komisjoni poolt 2017. aastal esitatav raport, mis käsitleb õigusabi süsteemi parendamist, TO-ga tõhusama koostöö loomist ning täidesaatva jurisdiktsiooni kohaldamist.[323] Samuti on Euroopa Liidu Nõukogu rõhutanud arvutikuritegevusealase koostöö tõhustamise vajalikkust Eurojusti raamistikus.[324] EN puhul tuleb eraldi ära märkida arvutikuritegevusevastases konventsioonis sisalduvad vastastikkust õigusabi reguleerivad artiklid, sest tegu on ainsa rahvusvahelise arvutikuritegevusevastasele võitlusele suunatud kokkuleppega. Kuid seoses vastastikuse õigusabi süsteemi keerukusega puudub kahjuks ülevaade, mil määral konventsioonis sisalduvaid sätteid praktikas kasutatakse. EN kutsub üles nimetatud sätteid rohkem rakendama ning on välja andnud soovitused nii konventsiooniga ühinenud riikidele kui teistele seotud toimijatele, kuidas piiriülestele andmetele ligipääsu nende sätete abil veelgi hõlbustada.[325] Lisaks nimetatud instrumentidele võivad riigid kasutada ka muid riikidevahelisi koostööraamistikke nagu Eurojust ja Interpol, (mitte)ametlikku suhtlust uurimisasutuste vahel, 24/7 võrkusid või ühiseid uurimisrühmasid. Riikidevaheliste koostöövormide kasutamine on aga raskendatud või kohaldamatu olukordades, kus näiteks tänu Tor'i kasutamisele ei ole andmete tegelikku asukohta võimalik

---

319 E.g. New Zealand and Law Commission (n 20) 226; Kent (n 46) 6–9; Koops, B-J and Goodwin, M (n 6) 26–27; Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (n 11) 123.

320 Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (n 11) 123.

321 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters (OJ L 130, 1.5.2014) (n 23) Article 1(2).

322 ibid Article 12 (4).

323 Council of the European Union, 'Council Conclusions on Improving Criminal Justice in Cyberspace' (n 60).

324 Council of the European Union, 'Council Conclusions on the European Judicial Cybercrime Network' (n 61) 2.

325 Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (n 11) 125–127.

kindlaks määrata (eelpool mainitud 'asukoha puudumine') ning seetõttu ei saa uurimise läbiviimisel esmajärjekorras arvestada andmete tegeliku asukohaga seotud riigi õigusabiga.

Seega saab järeldada, et informatsioonitehnoloogia areng, geograafilise asukoha varjamist võimaldavate tööriistade populaarsus ning arvutikuritegevuse keerukus ja leviku kasv on kriminaalmenetluse läbiviimist mõjutanud viisil, kus arvutikuritegevuse vastu võitlemiseks ei pöörduta enam tingimata teise riigi poole, vaid kasutatakse alternatiivseid meetodeid. Need meetodid, näiteks otse TO poole pöördumine või andmetele otsene ligipääs (sealhulgas riikliku õiguse alusel läbiviidav piiriülene kaugläbiotsimine, mida täpsemalt analüüsitakse kokkuvõtte kolmandas osas) ei vaja andmete asukohariigi poolt heakskiitu ning seega puudub riigil kontroll, kes ja millistel põhjustel tema territooriumil salvestatud andmetele ligi saavad. Selline piiriülene andmetele ligipääs on aga hetkel ühtselt reguleerimata ning õiguslikud tõlgendused, näiteks TO kohustusest välismaistele uurimisasutustele andmete jagamise osas, erinevad riigiti tugevalt. Traditsioonilise lähenemise kõrval, mille alusel pöördutakse teise riigi territooriumil asuva TO käest andmete saamiseks teise riigi pädevate ametiasutuste poole, hakkab riikide praktikale toetudes üha enam levima TO-ga otse suhtlemine. Õiguslikus debatis tõusetuvad peamiselt kaks küsimust. Esiteks, kas kriminaalmenetluse raames võib otse pöörduda TO poole (näiteks kelle peakorter asub välisriigis, kuid harukontor kriminaalmenetlust läbiviivas riigis) ning kas sellisel juhul on TO-l kohustus koostööd teha.[326] Teiseks, kas kriminaalmenetluse käigus võib otse pöörduda oma riigi territooriumil asuva TO poole ka siis, kui andmed ise on salvestatud teise riigi territooriumil.[327] Erisused nendes küsimustes viitavad autori hinnangul taaskord kriminaalmenetluse raames läbiviidavate piiriülese haardega toimingute regulatsiooni killustatusele ning andmete tegeliku asukoha tähtsuse suhtelisusele.

Kokkuvõtvalt tuleb nentida, et praegune olukord, kus ühtsed reeglid piiriülestele andmetele ligipääsuks puuduvad, võib lisaks teise riigi suveräänsuse rikkumisele tuua kaasa ka üksikisiku põhiõiguste ebaproportsionaalseid riiveid. Üheks võimalikuks arengusuunaks oleks eelpool välja toodud nn alternatiivsete meetodite kasutamise täiendav formaliseerimine, mida on arvutikuritegevusevastases konventsioonis, eeskätt artiklis 32(b) ning sellega seotud uurimistöö pinnalt tehtud ettepanekutes osaliselt üritanud teha EN. Kindlasti nõuab selles valdkonnas edasiliikumine laiapinnalisi arutelusid, mis peaksid muuhulgas hõlmama ka täidesaatva jurisdiktsiooni tõlgenduse uut läbimõtlemist, mida analüüsib täpsemalt järgmine alapeatükk. Esmajärjekorras peaksid riigid olema läbipaistvamad oma senise praktika osas, sest praeguse kriitika kohaselt ei lähe riikide ametlikud positsioonid tihtipeale kokku tegelike kriminaalmenetluses

326 Vt nt *Yahoo! Inc.* (n 78), *Yahoo! Inc* (n 76).

327 Vt nt *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp*. (n 82).

kasutatavate toimingutega.[328] Teiseks võimalikuks, ja miks mitte paralleelseks, sihiks võiks olla riikidevaheliste õigusabi taotluste süsteemi või muude koostöömehhanismide tõhustamine. Multilateraalsetel mehhanismidel (näiteks nimetatud EL ja EN arengud) või väiksema grupi huvitatud riikide tihedamal koostööl võivad ilmneda piiriülese kuritegevuse kontekstis teatud geograafilised piirangud, kuid need võiksid sellegipoolest olla ülejäänud riikidele heaks näiteks toimivatest ja läbipaistvatest lahendustest, mis ei vähenda riikide keskset rolli kriminaalmenetluses.

II Täidesaatev jurisdiktsioon, territoriaalne suveräänsus ja 'asukoha puudumine'

Kaitsmisele kuuluv väide

Lisaks sellele, et piiriülese kaugläbiotsimise läbiviimine võib osutuda ebaseaduslikuks teise riigi siseriikliku õiguse järgi, võib selline uurimistoiming sisaldada ka täidesaatva jurisdiktsiooni piiriülest kohaldamist ning seeläbi riikidevahelise konventsiooni, teise riigi nõusoleku või muu õigusliku aluseta kätkeda endas teise riigi territoriaalse suveräänsuse rikkumist. Ent kehtiva õiguse sellist ranget tõlgendust tuleb siiski käsitleda koos areneva praktikaga, kust nähtub, et infotehnoloogiline evolutsioon ja vajadus võidelda keeruka piiriülese kuritegevusega mõjutab territoriaalse suveräänsuse kontseptsiooni tõlgendamist, selle traditsioonilise tähenduse olulisust vähendades. Samuti lubab riikide praktika järeldada, et olukorda, kus andmete asukohta pole võimalik kindlaks määrata, võib pidada kaugläbiotsimise õigusvastasust välistavaks asjaoluks rahvusvahelise õiguse kontekstis.

Probleemi kirjeldus ja põhjendused

Niinimetatud Lotuse printsiibi kohaselt ei ole riigil õigus oma täidesaatvat võimu teise riigi territooriumil teostada, välja arvatud juhul, kui see tuleneb rahvusvahelisest tavaõigusest või konventsioonist.[329] Väitekiri analüüsib, kas piiriülese kaugläbiotsimise toimetamisel toimub täidesaatva jurisdiktsiooni kohaldamine teise riigi territooriumil. Õigusalase kirjanduse ning eri riikide kohtuinstantside arvamuste alusel eristab väitekiri kolme tõlgendust. Esiteks võib väita, et teise riigi territooriumil asuvate andmete kaugläbiotsimine viiakse läbi enda territooriumil juhul, kui uurimist läbiviivad isikud riigist ei lahku. Teiseks võib väita, et kaugläbiotsimine toimub nii enda kui ka teise riigi territooriumil. Kolmandaks ning levinuimaks arvamuseks on, et piiriülest kaugläbiotsimist tuleb pidada täidesaatva võimu teostamiseks teise riigi territooriumil, sest seal on andmete tegelik asukoht. Autor ei leidnud piisavalt tõendeid ei kirjandusest, kohtu- ega riikide praktikast, mis viitaksid vastupidisele tõlgendusele. Järg-

[328] 'Interview with Mr Rainer Franosch, Attorney General's Office of the German Federal State of Hessen' (n 192).

[329] *The Case of the S.S. Lotus, Fr. v. Turk., 1927 P.C.I.J. (ser. A) No. 10 (Decision No. 9)* (n 34).

misena tuleb seega küsida, kas piiriülest kaugläbiotsimist võib pidada teise riigi territoriaalset suveräänsust rikkuvaks. Kahjuks ei leia ka sellele küsimusele ühest vastust. Ühelt poolt väidetakse, et suveräänsuse rikkumiseks ei pea toiminguga tingimata kaasnema materiaalne kahju. Teisalt argumenteeritakse, et suveräänsuse rikkumine toimub ainult siis, kui materiaalne kahju on tuvastatav või kui toimingut teostatakse näiteks diplomaatiliste esinduste õigusi riivates. Autor leiab, et vaatamata näidetele kaasustest, kus teadaolevalt on piiriüleseid uurimistoiminguid kasutatud, ei saa sellist menetlustoimingut siiski veel tavaõiguseks pidada. Kuivõrd antud väitekirja kontekstis esmased õigusallikad territoriaalse suveräänsuse tõlgendamise kohta puuduvad, osutab väitekiri mitmetele kaudsetele viidetele, mis võiksid hõlbustada territoriaalse suveräänsuse mõiste sisustamist. Esiteks toob autor välja rahvusvaheliste organisatsioonide nagu EL ja EN aktiivse töö eesmärgiga leida piiriülesele kaugläbiotsimisele õiguslik alus. Arvutikuritegevusevastase konventsiooni artikkel 32(b) on konkreetne näide rahvusvahelisest lepingust, mis lubab 'erandina territoriaalsusele'[330] konventsiooniosaliste territooriumil paiknevatele andmetele piiriülest ligipääsu ilma igakordse asukohariigi autoriseerimiseta. Vaatamata artikkel 32(b) tõlgendamisprobleemidele töötab EN jätkuvalt selles suunas, et tagada huvitatud riikidele piiriüleseks ligipääsuks õiguslik alus[331] ning seeläbi vältida võimalikku rahvusvahelise õiguse rikkumist. Teiseks toob autor näiteid valitud riikide seadusandlusest ja praktikast, kus on erinevate lähenemiste kaudu selgelt püütud leida õiguslikke põhjendusi teatud olukordades piiriülese kaugläbiotsimine läbiviimiseks. Belgia kriminaalmenetlusseaduse (*Code d'Instruction Criminelle*) artikkel 88ter § 1 alusel võib uurimiskohtunik teatud tingimustel piiriülesele kaugläbiotsimisele loa anda ning kui andmete asukoht on võimalik tuvastada, tuleb peale uurimistoimingu läbiviimist teist riiki sellest teavitada. Madalmaades tuleb andmete asukoha teadmisel reeglina kasutada õigusabitaotluste protseduuri, kuid parasjagu on käsil kriminaalmenetlusseadustiku (*Wetboek van Strafrecht*) uuendamine, mille alusel oleks teatud tingimustel lubatud ka piiriülene kaugläbiotsimine ning on näiteid, kus uurimise käigus on kasutatud '*ubiquity'* printsiipi jurisdiktsiooni tõlgendamisel, mis on andnud aluse piiriülesteks menetlustoiminguteks, kui andmete asukohta pole olnud võimalik kindlaks määrata. Saksamaa kriminaalmenetlusõigus (*Strafprozeßordnung ehk StPO*) ei luba piiriülest kaugläbiotsimist juhul, kui andmete asukoht on teada (siis tuleb kasutada vastastikust õigusabi), kuid kehtiv tõlgendus lubab 'asukoha puudumisel' eeldada, et StPO 110(3) alusel toimetatavate toimingute puhul asuvad andmed kohalike TO poolt peegeldatuna samaaegselt ka Saksamaa pinnal. Peale käesoleva väitekirja jaoks kirjutatud artiklite avaldamist võeti Ameerika Ühendriikides vastu kriminaalmenetlust reguleeriva seaduse (*Federal Rules of Criminal Procedure*) muudatus, mille reegel 41 lubab nüüdsest kaugläbiotsimist

[330] Council of Europe, 'T-CY Guidance Note #3: Transborder Access to Data (Article 32)' (n 28) 3.

[331] Nt Council of Europe, '(Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data' (n 253).

toimetada olukorras, kus andmete asukohta on tehnoloogiliselt üritatud varjata. Autori hinnangul on selge, et kui kaugläbiotsimine on lubatud 'asukoha puudumise' korral, ei saa enam eeldada, et kaugläbiotsimisele kehtiksid ranged ainult oma riigi territooriumiga piirduvad reeglid. Eelpool toodud näidetele osundades on autori hinnangul võimalik järeldada, et praeguse riikide praktika kohaselt võidakse piiriülest kaugläbiotsimist pidada teise riigi suveräänsuse rikkumiseks ning seetõttu näeb siseriiklik regulatsioon olukorras, kus andmete asukoht on identifitseeritud, esmajärjekorras ette vastastikuste õigusabi taotluste või muude riikidevaheliste mehhanismide kasutamise. Küll aga võib mainitud riikide lähenemistes näha territoriaalse suveräänsuse rikkumise osas erandi tekkimist situatsioonis, kus andmete asukohta ei ole võimalik tuvastada. Autor leiab, et rahvusvahelise arvutikuritegevusevastase võitluse tugevdamiseks peavad riigid välja töötama meetmed, mida kasutada olukorras, kus riigil ei ole võimalik andmete asukohta tuvastada. Samaväärselt tuleks panustada riikidevahelise arusaama kujundamisse, mis võimaldaks üheselt ja läbipaistvalt tõlgendada täidesaatva jurisdiktsiooni kohaldumist kaugläbiotsimise korral.

III Kaugläbiotsimise regulatsioon EN arvutikuritegevusevastases konventsioonis ja Eesti õiguses: uurimisasutuste piiriülese pädevuse ebaselgus

Kaitsmisele kuuluv väide

Vaatamata sellele, et EN arvutikuritegevusevastase konventsiooni visiooniks on olnud arvutikuritegevusealase seadusandluse harmoniseerimine ja vajalike protseduuriliste reeglite väljatöötamine, on artikkel 32(b)-st tõlgendamis- ja kohaldamisraskuste tõttu piiriülese kaugläbiotsimise siseriikliku regulatsiooni arendamisel piiratud kasu. Eestis on piiriülese kaugläbiotsimise regulatsioon ebaselge ning vajab täpsustamist. Konventsiooni artiklid 19(2) ega 32(b) pole selgesõnaliselt siseriiklikku seadusandlusesse üle võetud. Arvestades artikkel 32(b)-ga seotud tõlgendus- ja kohaldamisprobleeme, ei soovita väitekiri seda ka otsesõnu Eesti õigusesse üle võtta. Samal ajal on artiklite 19(2) ja 32(b) kohaldamisalas olevad menetlustoimingud kahtlemata olulised tänapäevase kriminaalmenetluse jaoks ning peaksid seega pälvima seadusandja tähelepanu. Vastasel juhul võib kaugläbiotsimise regulatsiooni puudumisest tuleneva õigusselgusetuse tagajärjeks olla üksikisiku põhiõiguste rutiinne rikkumine, mis võib tuleneda uurimisasutustele jäetud ebamõistlikult laiast pädevusest kaugläbiotsimise toimetamisel. Seetõttu tuleks kehtiv läbiotsimise regulatsioon üle vaadata; läbiotsimist ja pealtkuulamist võimaldavate menetlustoimingute kasutamine tuleks selgemalt eristada ja nende kohaldamist täiendavalt analüüsida; siseriiklik õigus peaks sätestama konventsiooni artikkel 19(2) eeskujul kaugläbiotsimise (kas laiendatud läbiotsimise või uurimisasutuste endi süsteemidest läbiviidava kaugläbiotsimise); täiendavalt tuleks analüüsida piiriüleseks kaugläbiotsimiseks loa andvate instantside pädevusi ning ka 'asukoha puudumise' ilmnemisega seotud raskusi tuleks siseriiklikult adresseerida.

Probleemi kirjeldus ja põhjendused

Piiriülese andmetele ligipääsu regulatsioon on tänaseks olnud EN-s arutusel pea kakskümmend aastat. 2001. aastal vastu võetud EN arvutikuritegevusevastase konventsiooni artikkel 19(2) sätestab esialgse läbiotsimise laiendamise teistesse seotud (arvuti)süsteemidesse, kuid piiritleb menetlustoimingu läbiotsimist toimetava riigi territooriumiga.[332] Sisuliselt sarnase kuid piiriülese iseloomuga menetlustoimingu sätestab vastastikust uurimisabi reguleerivas jaotuses konventsiooni artikkel 32(b), mille alusel võib konventsiooniosaline teise konventsiooniosalise igakordse loata 'saada oma territooriumil paikneva arvutisüsteemi kaudu teises konventsiooniosalises riigis asuvaid salvestatud arvutiandmeid, kui ta saab selleks seadusliku ja vabatahtliku nõusoleku isikult, kellel on seaduslik volitus avalikustada andmeid nimetatud arvutisüsteemi kaudu.'[333] Kuigi teoreetiliselt võiks nimetatud artikkel kiirendada kriminaalmenetluse käiku ning olla mõistlik alternatiiv traditsioonilistele vastastikuse õigusabi taotlustele, on kokkulepitud sõnastus tekitanud mitmeid küsimusi sellise volituse sisu ja piiride osas. Näiteks on problemaatiline artikli geograafiline piiratus, mis ei luba seda kasutada 'asukoha puudumisel' või olukorras, kus andmed asuvad konventsiooniga mitteliitunud riigi territooriumil. Praktikud on ka nentinud, et kriminaalmenetluse läbiviimisel ja olukorras, kus tuleb piiriülestele andmetele ligi pääseda, ei ole tavapärane kontrollida, kas teine riik üldse on konventsiooniosaline. Samuti ei olda ühel meelel, mida tähendab antud artikli kontekstis 'seaduslik volitus' (*lawful authority*) ning 'nõusolek' (*consent*). Kuigi EN on üritanud artikli sisu täpsustada ning identifitseeritud probleeme veel vastu võtmata täiendava protokolliga lahendada, pole siiani konkreetseid edusamme tehtud.

Väitekiri nõustub, et Eesti kriminaalmenetlusseadustiku (KrMS) §-s 91 sätestatu alusel pole (arvuti)süsteemide ja digitaalselt salvestatud andmete läbiotsimise regulatsioon üheselt mõistetav. Samuti ei ole selge, milliseid põhimõtteid tuleks digitaalsete tõendite kogumisel ning kohtulikul kasutamisel järgida. Autor leiab, et võib kaaluda digitaalsete tõendite kogumiseks ja kohtulikuks kasutamiseks erikorra sätestamist, kuid väitekirjas uuritud riikide seadusandluse näited annavad tunnistust ka praktikast, mille alusel kasutatakse digitaalsete tõendite kogumiseks edukalt (vastavalt täiendatud) traditsioonilisi läbiotsimise sätteid. Lisaks võiksid autori hinnangul olla seaduses täpsemalt eristatud tingimused, millal kohaldatakse andmetele ligipääsuks läbiotsimist ja millal pealtkuulamist reguleerivaid sätteid.

Käesoleva väitekirja kontekstis on eelkõige oluline järeldus, et Eesti kehtiv õiguskord kaugläbiotsimist ega ka piiriülest kaugläbiotsimist otseselt ei reguleeri, kuigi praktiline vajadus selle jaoks on olemas. Samuti puudusid väitekirja tarbeks intervjuude läbiviimise hetkel selliste olukordade käsitlemiseks ka amet-

---

[332] Samuti näeb konventsiooni artikkel 14(1) ette, et "Konventsiooniosaline võtab seadusandlikke ja muid meetmeid, et kehtestada selles jaos käsitletud eeluurimise ja menetluse kord ning et anda asja eeluurimiseks või menetlemiseks vajalikud volitused."

[333] Euroopa Nõukogu, Council of Europe, Convention on Cybercrime (n 10).

likud ametkonnasisesed juhised, kuigi praktika viitas sellele, et välisriigis asuvatele tõenditele ligipääsemisel tõlgendati menetlustoiminguid siiski Eesti jurisdiktsioonis läbiviidavaiks, sest neile andmetele oli ligipääs ning andmete analüüs toimus Eestis. Seoses väitekirjas analüüsitud konventsiooni artikkel 32(b)-ga seotud tõlgendus- ja rakendusprobleemidega pole väitekirja autori hinnangul otstarbekas nimetatud artikli otsesõnu siseriiklikusse õigusesse ülevõtmine, kuid kahtlemata on kaugläbiotsimine ning selle võimalik piiriülesus tänapäeva kriminaalmenetluse jaoks olulised toimingud.

Märkimisväärne on ka hiljutisest Riigikohtu otsusest tulenev täpsustus, mille alusel võib salvestatud andmetele ligipääsu kvalifitseerida, kui jälitustoimingute kasutamine on õigustatud, KrMS § 126[5] alusel. Seega on vajalik 'asja', mis antud kaasuse puhul oli Google server, läbivaatamiseks prokuröri luba.[334] Autori arvates tuleks täiendavalt selgitada, kas prokuröri loast piisab, kui läbivaadatavad andmed asuvad teise riigi territorriumil.

Autor on seisukohal, et selleks, et vältida liialt suurt tõlgendusruumi ning uurimisasutuste ülemäära avarat tegutsemisvabadust, peaks kaugläbiotsimist ning selle võimalikku piiriülesust sätestama läbipaistvam regulatsioon. Piiriülestele andmetele ligipääsuks kasutatavate toimingute valik peaks olema põhjendatud, üksikisikule peaksid olema selged ja kättesaadavad õiguskaitsevahendid ning täiendavalt peaks analüüsima meetmeid, mille abil kriminaalmenetluse käigus tagada ligipääs andmetele, kui vajalikke paroole ei ole käepärast või andmetele ligipääs on muul viisil raskendatud. Samuti peaks seadusandlus kaugläbiotsimise kontekstis sätestama uurimisasutuste tegevuse üle konkreetsemad kontrollmehhanismid, mis võimaldaksid kogutud tõendite tõendusväärtuslikkust hinnata. Võttes arvesse teise riigi õiguse ja rahvusvahelise õiguse võimalikku rikkumist, peaks hoolikalt kaaluma, millistel tingimustel ning millised ametiasutused võivad piiriüleseid toiminguid autoriseerida; näiteks ei peaks autori hinnangul piiriüleste toimingute läbiviimiseks piisama prokuröri heakskiidust. Kaugläbiotsimise korral tuleks täiendavalt analüüsida, kas toimingu osaks on andmetele ligipääs ja nende kopeerimine või võib nende sätete alusel ka andmeid 'kindlustada' (*secure*), eemaldada või ligipääsematuks muuta ning milliseid tehnilisi lahendusi võib selleks kasutada. Samuti tuleks analüüsida kaugläbiotsimisse kaasatavate ekspertide õigusi ja kohustusi ning kaugläbiotsimisest teavitamise erisusi.

334 Riigikohus *3-1-1-93-15* (n 286) 89.

PUBLICATIONS

CURRICULUM VITAE

Name: Anna-Maria Osula
Date of birth: October 2, 1984
E-mail: annamaria.osula@gmail.com

Career

2013–…	Lecturer, Tallinn University of Technology, Faculty of Information Technology, Department of Computer Science
2013–...	Senior Researcher, NATO Cooperative Cyber Defence Centre of Excellence
2008–2011	Junior Researcher, NATO Cooperative Cyber Defence Centre of Excellence

Education

2010–...	PhD studies in law, University of Tartu, Estonia
2011–2012	PhD research, Waseda university, Japan
2007–2008	Master Degree in IT Law, Stockholm university, Sweden
2006–2006	Exchange semester in Paris VIII Saint Denis-Vincenne university, France
2005–2005	Exchange semester in Voronezh university, Russia
2003–2007	Bachelor degree in law, University of Tartu, Estonia

Publications

Minárik, Tomas; Osula, Anna-Maria (2016). Tor Does Not Stink: Use and Abuse of the Tor Anonymity Network from the Perspective of Law. Computer Law and Security Review, 32 (1), 111–127.

Osula, Anna-Maria (2016). Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study. International Journal of Law and Information Technology, 24 (4), 343–373.

Velasco, Cristos; Hörnle, Julia; Osula, Anna-Maria (2016). Global Views on Internet Jurisdiction and Trans-Border Access. In: Gutwirth, Serge; Leenes, Ronald; De Hert, Paul (Ed.). Data Protection on the Move (465–476). Springer Netherlands. Law, Governance and Technology Series, 24.

Osula, Anna-Maria; Rõigas, Henry (2016). Introduction. In: Osula, Anna-Maria; Rõigas, Henry (Ed.). International Cyber Norms: Legal, Policy & Industry Perspectives (11–22). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Osula, Anna-Maria; Rõigas, Henry (2016). International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Osula, Anna-Maria (2015). Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data. Masaryk University Journal of Law and Technology, Vol 9, 43–64.

Osula, Anna-Maria (2015). Transborder Access and Territorial Sovereignty. Computer Law and Security Review, 31 (6), 719–735.
Osula, Anna-Maria (2015). Accessing Extraterritorially Located Data: Options for States. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 1–27.
Osula, Anna-Maria (2015). National Cyber Security Organisation: Estonia. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 1–15.
Osula, Anna-Maria (2015). National Cyber Security Organisation: United Kingdom. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 1–24.
Çalışkan, Emin; Minárik, Tomáš; Osula, Anna-Maria (2015). Technical and Legal Overview of the Tor Anonymity Network. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 1–32.
Kont, Markus; Pihelgas, Mauno; Wojtkowiak, Jesse; Trinberg, Lorena; Osula, Anna-Maria (2015). Insider Threat Detection Study. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 1–59.
Maybaum, Markus; Osula, Anna-Maria; Lindström, Lauri (2015). Cyber Conflict: Architectures in Cyberspace (CyCon), 2015 7th International Conference. Tallinn, Estonia: IEEE.
Kaska, Kadri; Osula, Anna-Maria; Stinissen, Jan (2013). The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 1–45.

ELULOOKIRJELDUS

Nimi: Anna-Maria Osula
Sünniaeg: 2. oktoober 1984
E-mail: annamaria.osula@gmail.com

Töökogemus

2013–…	Lektor, Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Arvutiteaduse instituut
2013–...	Vanemteadur, NATO Kooperatiivse Küberkaitse Kompetentsikeskus
2008–2011	Nooremteadur, NATO Kooperatiivse Küberkaitse Kompetentsikeskus

Hariduskäik

2010–...	Doktorantuur, õigusteadus, Tartu ülikool, Eesti
2011–2012	Teadustöö doktorantuuri raames, Waseda ülikool, Jaapan
2007–2008	Magistrikraad IT-õiguses, Stockholmi ülikool, Rootsi
2006–2006	Vahetussemester Pariisi VIII Saint Denis-Vincenne ülikoolis, Prantsusmaa
2005–2005	Vahetussemester Voronezhi ülikoolis, Venemaa
2003–2007	Bakalaureusekraad õigusteaduses, Tartu Ülikool, Eesti

Publikatsioonid

Minárik, Tomas; Osula, Anna-Maria (2016). Tor Does Not Stink: Use and Abuse of the Tor Anonymity Network from the Perspective of Law. Computer Law and Security Review, 32 (1), 111–127.

Osula, Anna-Maria (2016). Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study. International Journal of Law and Information Technology, 24 (4), 343–373.

Velasco, Cristos; Hörnle, Julia; Osula, Anna-Maria (2016). Global Views on Internet Jurisdiction and Trans-Border Access. In: Gutwirth, Serge; Leenes, Ronald; De Hert, Paul (Ed.). Data Protection on the Move (465–476). Springer Netherlands. Law, Governance and Technology Series, 24.

Osula, Anna-Maria; Rõigas, Henry (2016). Introduction. In: Osula, Anna-Maria; Rõigas, Henry (Ed.). International Cyber Norms: Legal, Policy & Industry Perspectives (11–22). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Osula, Anna-Maria; Rõigas, Henry (2016). International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Osula, Anna-Maria (2015). Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data. Masaryk University Journal of Law and Technology, Vol 9, 43–64.
Osula, Anna-Maria (2015). Transborder Access and Territorial Sovereignty. Computer Law and Security Review, 31 (6), 719–735.
Osula, Anna-Maria (2015). Accessing Extraterritorially Located Data: Options for States. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 1–27.
Osula, Anna-Maria (2015). National Cyber Security Organisation: Estonia. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 1–15.
Osula, Anna-Maria (2015). National Cyber Security Organisation: United Kingdom. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 1–24.
Çalışkan, Emin; Minárik, Tomáš; Osula, Anna-Maria (2015). Technical and Legal Overview of the Tor Anonymity Network. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 1–32.
Kont, Markus; Pihelgas, Mauno; Wojtkowiak, Jesse; Trinberg, Lorena; Osula, Anna-Maria (2015). Insider Threat Detection Study. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 1–59.
Maybaum, Markus; Osula, Anna-Maria; Lindström, Lauri (2015). Cyber Conflict: Architectures in Cyberspace (CyCon), 2015 7th International Conference. Tallinn, Estonia: IEEE.
Kaska, Kadri; Osula, Anna-Maria; Stinissen, Jan (2013). The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 1–45.

DISSERTATIONES IURIDICAE UNIVERSITATIS TARTUENSIS

1. **Херберт Линдмяэ**. Управление проведением судебных экспертиз и его эффективность в уголовном судопроизводстве. Тарту, 1991.
2. **Peep Pruks**. Strafprozesse: Wissenschaftliche "Lügendetektion". (Instrumentaldiagnostik der emotionalen Spannung und ihre Anwendungsmöglichkeiten in Strafprozess). Tartu, 1991.
3 **Marju Luts**. Juhuslik ja isamaaline: F. G. v. Bunge provintsiaalõigusteadus. Tartu, 2000.
4. **Gaabriel Tavits**. Tööõiguse rakendusala määratlemine töötaja, tööandja ja töölepingu mõistete abil. Tartu, 2001.
5. **Merle Muda**. Töötajate õiguste kaitse tööandja tegevuse ümberkorraldamisel. Tartu, 2001.
6. **Margus Kingisepp**. Kahjuhüvitis postmodernses deliktiõiguses. Tartu, 2002.
7. **Vallo Olle**. Kohaliku omavalitsuse teostamine vahetu demokraatia vormis: kohalik rahvaalgatus ja rahvahääletus. Tartu, 2002.
8. **Irene Kull**. Hea usu põhimõte kaasaegses lepinguõiguses. Tartu, 2002.
9. **Jüri Saar**. Õigusvastane käitumine alaealisena ja kriminaalsed karjäärid (Eesti 1985–1999 longituuduurimuse andmetel). Tartu, 2003.
10. **Julia Laffranque**. Kohtuniku eriarvamus. Selle võimalikkus ja vajalikkus Eesti Vabariigi Riigikohtus ja Euroopa Kohtus. Tartu, 2003.
11. **Hannes Veinla**. Ettevaatusprintsiip keskkonnaõiguses. Tartu, 2004.
12. **Kalev Saare**. Eraõigusliku juriidilise isiku õigussubjektsuse piiritlemine. Tartu, 2004.
13. **Meris Sillaots**. Kokkuleppemenetlus kriminaalmenetluses. Tartu, 2004.
14. **Mario Rosentau**. Õiguse olemus: sotsiaalse käitumise funktsionaalne programm. Tartu, 2004.
15. **Ants Nõmper**. Open consent – a new form of informed consent for population genetic databases. Tartu, 2005.
16. **Janno Lahe**. Süü deliktiõiguses. Tartu, 2005.
17. **Priit Pikamäe**. Tahtluse struktuur. Tahtlus kui koosseisupäraste asjaolude teadmine. Tartu, 2006.
18. **Ivo Pilving**. Haldusakti siduvus. Uurimus kehtiva haldusakti õiguslikust tähendusest rõhuasetusega avalik-õiguslikel lubadel. Tartu, 2006.
19. **Karin Sein**. Ettenähtavus ja rikutud kohustuse eesmärk kui lepingulise kahjuhüvitise piiramise alused. Tartu, 2007.
20. **Mart Susi**. Õigus tõhusale menetlusele enda kaitseks – Euroopa Inimõiguste ja Põhivabaduste Kaitse Konventsiooni artikkel 13 Euroopa Inimõiguste Kohtu dünaamilises käsitluses. Tartu, 2008.
21. **Carri Ginter**. Application of principles of European Law in the supreme court of Estonia. Tartu, 2008.
22. **Villu Kõve**. Varaliste tehingute süsteem Eestis. Tartu, 2009.

23. **Katri Paas**. Implications of Smallness of an Economy on Merger Control. Tartu, 2009.
24. **Anneli Alekand**. Proportsionaalsuse printsiip põhiõiguste riive mõõdupuuna täitemenetluses. Tartu, 2009.
25. **Aleksei Kelli**. Developments of the Estonian Intellectual Property System to Meet the Challenges of the Knowledge-based Economy. Tartu, 2009.
26. **Merike Ristikivi**. Latin terms in the Estonian legal language: form, meaning and influences. Tartu, 2009.
27. **Mari Ann Simovart**. Lepinguvabaduse piirid riigihankes: Euroopa Liidu hankeõiguse mõju Eesti eraõigusele. Tartu, 2010.
28. **Priidu Pärna**. Korteriomanike ühisus: piiritlemine, õigusvõime, vastutus. Tartu, 2010.
29. **René Värk**. Riikide enesekaitse ja kollektiivse julgeolekusüsteemi võimalikkusest mitteriiklike terroristlike rühmituste kontekstis. Tartu, 2011.
30. **Paavo Randma**. Organisatsiooniline teovalitsemine – *täideviija täideviija taga* kontseptsioon teoorias ja selle rakendamine praktikas. Tartu, 2011.
31. **Urmas Volens**. Usaldusvastutus kui iseseisev vastutussüsteem ja selle avaldumisvormid. Tartu, 2011.
32. **Margit Vutt**. Aktsionäri derivatiivnõue kui õiguskaitsevahend ja ühingujuhtimise abinõu. Tartu, 2011.
33. **Hesi Siimets-Gross**. Das „Liv-, Est- und Curlaendische Privatrecht" (1864/65) und das römische Recht im Baltikum. Tartu, 2011.
34. **Andres Vutt**. Legal capital rules as a measure for creditor and shareholder protection. Tartu, 2011.
35. **Eneken Tikk**. Comprehensive legal approach to cyber security. Tartu, 2011.
36. **Silvia Kaugia**. Õigusteadvuse olemus ja arengudeterminandid. Tartu, 2011.
37. **Kadri Siibak**. Pangandussüsteemi usaldusväärsuse tagamine ja teabekohustuste määratlemine finantsteenuste lepingutes. Tartu, 2011.
38. **Signe Viimsalu**. The meaning and functioning of secondary insolvency proceedings. Tartu, 2011.
39. **Ingrid Ulst**. Balancing the rights of consumers and service providers in electronic retail lending in Estonia. Tartu, 2011.
40. **Priit Manavald**. Maksejõuetusõigusliku regulatsiooni valikuvõimaluste majanduslik põhjendamine. Tartu, 2011, 193 lk.
41. **Anneli Soo**. Remedies against ineffectiveness of defense counsel. Judicial supervision over the performance of defense counsel in Estonian criminal proceedings. Tartu, 2011, 282 p.
42. **Arnold Sinisalu**. Mõjutustegevuse piirid rahvusvahelises õiguses. Tartu, 2012, 277 lk.
43. **Kaspar Lind**. Käibemaksupettused ja nende tõkestamine. Tartu, 2012, 155 lk.
44. **Berit Aaviksoo**. Riigi otsustusruumi ahenemine: kodakondsus nüüdisaegses Euroopas. Tartu, 2013, 368 lk.
45. **Kai Kullerkupp**. Vallasomandi üleandmine. Õigusdogmaatiline raamistik ja kujundusvõimalused. Tartu, 2013, 398 lk.

46. **Iko Nõmm**. Käibekohustuse rikkumisel põhinev deliktiõiguslik vastutus. Tartu, 2013, 212 lk.
47. **Piia Kalamees**. Hinna alandamine õiguskaitsevahendite süsteemis. Tartu, 2013, 232 lk.
48. **Irina Nossova**. Russia's international legal claims in its adjacent seas: the realm of sea as extension of Sovereignty. Tartu, 2013, 205 p.
49. **Age Värv**. Kulutuste kondiktsioon: teise isiku esemele tehtud kulutuste hüvitamine alusetu rikastumise õiguses. Tartu, 2013, 273 lk.
50. **Elise Vasamäe**. Autoriõiguste ja autoriõigusega kaasnevate õiguste jätkusuutlik kollektiivne teostamine. Tartu, 2014, 308 lk.
51. **Marko Kairjak**. Keerukuse redutseerimine Eesti õiguses karistusseadustiku § 217^2 objektiivse koosseisu relatiivsete õigusmõistete sisustamise näitel. Tartu, 2015, 179 lk.
52. **Kadi Pärnits**. Kollektiivlepingu roll ja regulatsioon nüüdisaegsetes töösuhetes. Tartu, 2015, 179 lk.
53. **Leonid Tolstov**. Tort liability of the director to company's creditors. Tartu, 2015, 169 p.
54. **Janar Jäätma**. Ohutõrjeõigus politsei- ja korrakaitseõiguses: kooskõla põhiseadusega. Tartu, 2015, 242 lk.
55. **Katre Luhamaa**. Universal Human Rights in National Contexts: Application of International Rights of the Child in Estonia, Finland and Russia. Tartu, 2015, 217 p.
56. **Mait Laaring**. Eesti korrakaitseõigus ohuennetusõigusena. Tartu, 2015, 267 lk.
57. **Priit Kama**. Valduse ja kohtuliku registri kande publitsiteet Eesti eraõiguses. Tartu, 2016, 194 lk.
58. **Kristel Degener**. Abikaasade vara juurdekasvu tasaarvestuse varasuhe. Tartu, 2016, 242 lk.
59. **Olavi-Jüri Luik**. The application of principles of European insurance contract law to policyholders of the Baltic states: A measure for the protection of policyholders. Tartu, 2016, 228 p.
60. **Kaido Künnapas**. Maksukohustuse täitmise preventiivne tagamine enne maksukohustuse tuvastamist: ettevaatuspõhimõte maksumenetluses.Tartu, 2016, 388 lk.
61. **Eve Fink**. Õiguspärase ootuse kaitse põhimõtte eeldused ja piirid Euroopa liidu õiguses. Tartu, 2016, 245 lk.
62. **Arsi Pavelts**. Kahju hüvitamise nõue täitmise asemel ostja õiguste näitel. Tartu, 2017, 414 lk.