DOI: 10.5817/MUJLT2017-1-6

THE NOTIFICATION REQUIREMENT IN TRANSBORDER REMOTE SEARCH AND SEIZURE: DOMESTIC AND INTERNATIONAL LAW PERSPECTIVES[*]

by

ANNA-MARIA OSULA[**], MARK ZOETEKOUW[***]

Modern criminal investigations increasingly rely on evidence that is not in a tangible format and can no longer be assumed to be located close to the locus delicti or the perpetrator. This article focuses on the notification requirement embedded into the legal regimes regulating one of the available investigative measures employed to access data stored in digital devices – remote search and seizure. The article will first analyse whether there is an obligation under international law to notify the other state about such a transborder investigative measure. Then we will compare the notification requirements for remote search and seizure in three countries' domestic law: in Estonia, the Netherlands and the United States. Finally, we will draw conclusions on the principal challenges related to the implementation of the notification requirement under the domestic regulation. These involve balancing, on the one hand, the difficulties in identifying the location and the identity of the possible suspect and, on the other hand, the need to provide the involved individuals' protection as guaranteed by the principles of fair trial and effective remedy.

[*] Both authors have contributed equally to this article. The views expressed herein are those of the authors and do not reflect the policy or the opinion of any other entity.

[**] Anna-Maria Osula, Ph.D., is a researcher at NATO CCD COE, Estonia and a lecturer at Tallinn Univeristy of Technology, Estonia.

[***] Mark Zoetekouw is a Ph.D. researcher at Utrecht University, the Netherlands and senior Legal Advisor Cybercrime & Digital Technology at the Dutch National Police.

KEY WORDS

Remote Search and Seizure, Notification, Fair Trial, Effective Remedy, Law Enforcement

1. INTRODUCTION

Modern criminal investigations increasingly rely on evidence that is not in a tangible format and can no longer be assumed to be located close to the locus delicti or the perpetrator. Instead, evidence may be stored in electronic devices located in foreign territories or in cloud service providers' servers. Furthermore, due to the Internet's decentralised nature and easily accessible anonymising tools, the exact location of the evidence may not be able to be determined at all.

However, these technological developments for storing and transmitting data and tools enabling the anonymisation of one's identity and footprints in the virtual world should not handicap the efforts of law enforcement (LE) in investigating crime. In the arms race between LE and criminals, LE must be equipped with effective investigative tools to counter such complex circumstances.

This article focuses on one of the available investigative measures employed to access data stored in digital devices: remote search and seizure. Traditionally, search and seizure represents a coercive power used for accessing and seizing tangible items. In the context of digital evidence and depending on the peculiarities of domestic legal regimes, search and seizure may also be used for accessing, copying and seizing data stored in domestically located devices situated on the premises specified in a search warrant. Remote search and seizure signifies searches that are either undertaken by extending the original search and seizure to devices accessible from the originally searched device (and these accessible devices may also be located outside the original premises of the search) or by remotely conducting search and seizure from other (such as the LE's own) devices.

Both – accessing data from the initially searched devices on the premises of the search or from LE's own devices – are increasingly employed in practice by LE notwithstanding whether the physical location of the data (storage) has been identified, or not.

The possible extraterritorial reach of such investigative measures has raised questions regarding their overall legality under international law.[1] Instead of revisiting this debate, the article will focus on something that has received much less attention: the obligation of notifying the involved parties about a search that has taken place.

This obligation is commonly enshrined in the domestic regulation of criminal procedure with the general aim to respect the principles of effective remedy and fair trial as set out in art. 13 and art. 6 of the European Convention of Human Rights (ECHR).[2] It is generally accepted that providing notice of a search is an obligation of investigative bodies, prosecutors' offices or courts.[3] One of the goals of notification is to explain to the participants of the proceedings the objective of the investigative measure and the rights and obligations of the involved parties, thereby granting everyone whose rights and freedoms have been violated the right of recourse to the courts.[4] Such access to the courts would be effectively non-existent if knowledge of the execution of the measure were to remain unknown to the involved parties.

In some countries, remote access to data may alternatively or additionally be regulated under surveillance activities. Similarly, in these

---

1 E.g. Goldsmith, J. (2001) *The Internet and the Legitimacy of Remote Cross-Border Searches*. University of Chicago Law School, Chicago Unbound. Available from: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgiarticle=1316&context=public_law_and_legal_theory [Accessed 8 March 2017]; Koops, B.-J. and Goodwin, M. (2014) *Cyberspace, the Cloud, and Cross-Border Criminal Investigation*. Tilburg University, Tilburg Institute for Law, Technology, and Society, WODC. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263 [Accessed 8 March 2017]; Osula, A.-M. (2015) *Transborder Access and Territorial Sovereignty.* Computer Law & Security Review, 31(6); Zoetekouw, M. (2016) *Ignorantia Terrae Non Excusat*. Available from: 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 [Acessed 8 March 2017]; see also Svantesson, D. (2016) Preliminary Report: Law Enforcement Cross-Border Acces to Data, pp. 4-5, 9. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874238 [Accessed 8 March 2017].

2 Council of Europe, *European Convention on Human Rights*, 1950.

3 See e.g. *Kriminaalmenetlusseadustik (Code of Criminal Procedure), RT I 2003, 27, 166; RT I, 31.12.2016, 46*. Estonia: Riigi Teataja. In Estonian. § 8(1). Also see art. 94 *Wetboek van Strafvordering (Dutch Criminal Procedure Code, DCPC hereafter)*, the Netherlands. In Dutch. For particularly search and seizure of goods and art. 125i jo. 125m DCPC for "*seizing*" data. The legal history on art. 126bb DCPC, while not immediately applicable to search and seizures, offers much insight into the status of notification in Dutch law in general. See footnote 8 and sub-section 3.2.2.

4 E.g. *Eesti Vabariigi põhiseadus (Constitution of the Republic of Estonia),* RT 1992, 26, 349; RT I, 15. 5. 2015, 2. Estonia: Riigi Teataja. In Estonian. § 15(1); Kergandberg, E. and Pikamäe, P. (2012) *Kriminaalmenetluse seadustik: kommenteeritud väljaanne (Code of Criminal Procedure: Commented Edition)*. Tallinn: Juura, p. 271. See e.g. 'Appeal against Activities of Investigative Body or Prosecutor's Office' Division 5 in Estonia, Kriminaalmenetlusseadustik (Code of Criminal Procedure), footnote 3.

cases the requirement of (eventual) notification is also an undisputed element of the legal regime which in addition to the already quoted basic rights touches upon the inviolability of private and family life,[5] human dignity[6] and the general right to access information held by government agencies and local authorities.[7]

But how is the requirement of notification carried out during remote search and seizure? When accessing data stored on the territory of the other state, would domestic, or international law require the notification of the other state or would such behaviour be rather regarded as a polite gesture? In particular, do the traditional means of notification that have been used to inform the suspect regarding e.g. searching his/her house suffice in the context of remote searches? How does and should domestic regulation balance on the one hand the difficulties in identifying the location and the identity of the possible suspect, and on the other hand, the need to provide the involved individuals' protection as guaranteed by the principles of fair trial and effective remedy?

In order to answer these questions, the article will first look into the notification issue from the perspective of international law. The article will then turn to analysing three examples of domestic regulation in countries where the reforms of codes of criminal procedure are in different stages. Firstly, Estonia is a case study of a domestic approach where the traditional search and seizure regime is not yet taking into account the possibility of remote search and seizure and therefore illustrates well the shortcomings of the traditional notification requirements. Secondly, the Netherlands showcases a regulation which already considers the peculiarities of remote search and seizure, but is nevertheless undergoing substantial reforms. Thirdly, the United States (US) recently passed amendments to its Federal Rules of Criminal Procedure which now also address search and seizure in situations where the location of the data has been concealed. Based on the comparison of these three examples we

---

5 Eesti Vabariigi põhiseadus, footnote 4, § 26.

6 Eesti Vabariigi põhiseadus, footnote 4, § 10.

7 Eesti Vabariigi põhiseadus, footnote 4, § 44(3). See also exceptions to the general right; see also Kergandberg and Pikamäe, footnote 4, p. 328. *Grondwet (The Dutch Constitution), the* Netherlands. In Dutch. Article 110 charges the government to be transparant in the excution of its tasks. See also for specific rules, The *Wet Openbaarheid Bestuur (Governance Transparency Act),* the Netherlands. In Dutch. While the Dutch Constitution does grosso modo to provide the same basic rights as the Estonian Constitution, because of particularities of Dutch law (and the system being moderately monistic in nature) reference will more likely be made to treaties such as the ECHR to achieve the same effects.

will draw conclusions on the principal challenges related to the domestic regulation of notification of search and seizure and examine whether notification of a foreign state is, or should be considered obligatory in the case of transborder search and data seizure.

2. NOTIFICATION IN INTERNATIONAL LAW

Reservations about the possible impact of territorial sovereignty are one of the main issues holding back a wider agreement on the use of remote investigative measures such as remote search and seizure, or "*transborder access*" in terms of art. 32(b) of the Council of Europe (CoE) Convention on Cybercrime.[8] Notification of the state on whose territory the investigatory measure is affected or ends up being affected might appease some of these reservations. However, does such an obligation exist under international law? Who decides who is notified of what and at what point in time?

The drafters of the CoE Convention on Cybercrime discussed the requirement of notification as part of the established search and seizure regime. They noted that while not obligatory for the Parties of the Convention, some states may consider the notification requirement as an essential feature of the search and seizure measure with the general aim to distinguish between (generally non-surreptitious) computer search of stored data and (covert) interception of data in transmission in their domestic legislation.[9] As such a notification prior to the search may prejudice the investigation, the legislator was suggested to consider notifying the persons concerned after the search has been carried out.[10] Due to the difficulties in determining the physical location of the data to be searched (or more specifically the storage medium upon which it resides), it might be problematic to identify who ought to be notified at all. But no attention was given to that topic at the time.

---

[8] Council of Europe, Convention on Cybercrime, ETS No. 185.

[9] Council of Europe (2001) *Explanatory Report to the Convention on Cybercrime (ETS No. 185)*. Sec. 204. Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/ Display DCTMContentdocumentId=09000016800cce5b [Accessed 8 March 2017]. The requirement of notification was also discussed at the G8 in 1999 but never made it to the actual wording of art. 32(b). See Council of Europe (2012) *Transborder Access and Jurisdiction: What Are the Options?*, pp. 6-7. Available from: https://rm.coe.int/CoERM PublicCommonSearch Services/DisplayDCTMContentdocumentId=09000016802e79e8 [Accessed 8 March 2017].

[10] Council of Europe, *Explanatory Report to the Convention on Cybercrime (ETS No. 185)*, footnote 9, sec. 204.

In fact, the explanatory notes to the convention make it very clear that the issue of notification is left for domestic legislation. One of the most prominent examples of domestic regulation including the requirement to notify another state about the remote search and seizure of data stored in its territory can be found in the Belgium Code of Criminal Procedure (BCCP). BCCP art. 39bis § 3 (previously art. 88ter) allows under certain conditions the public prosecutor (previously: investigative judge) to issue a warrant 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. If the data is not situated in domestic territory, it can only be copied (and not, for instance, made inaccessible), and the public prosecutor should communicate this information to the Department of Justice, who shall inform the competent authorities of the state concerned if it can be identified.[11] However, since practice has shown that it is very difficult to determine the exact location of the data, the possibility of informing the other state has been rarely exercised, even if the provision is used often for accessing data not stored domestically.[12] Confusingly, given the text of BCCP art. 88ter (old) and art. 39bis (current), Belgium practitioners in several meetings[13] have seemed to posit an approach going beyond this. The (paraphrased) reasoning then seemed to be that if the information is accessible from the Belgium territory, its seizure is not considered extraterritorial even if the data is stored abroad as the act of seizing is executed domestically. In other words, it is the place of the LE officer acting or "*looking*" that is apparently considered the sole location of the act – disregarding the fact that the data was retrieved for viewing or copying from "*elsewhere*".

We have found no basis in international law for a specific obligation to notify the other state about a transborder investigative measure even if considerations of comity may be proposed as a reason for states to notify nevertheless. This would still not, however, imply that transborder investigative measures would be legal by default. Rather, we believe that a unilateral notification, whether before, or after the search, would not

[11] *Code d'Instruction Criminelle (Belgium Code of Criminal Procedure*), Livre Premier, Belgium. In French. Art 39bis § 3.

[12] Interview with Mr. Geert Schoorens, Federal Prosecutor's Office of Belgium, 2015. Quoted in Osula, A.-M. (2016) *Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study*. International Journal of Law and Information Technology 24(4), pp. 365-366.

[13] Amongst those: the Council of Europe Octopus 2015 meeting and the Crossing borders: Jurisdiction in Cyberspace conference of 7-8 March 2016.

impact the assessment of the legality of the transborder investigative measure. Nevertheless, while bearing no apparent legal weight under international law, the gesture of notification may be beneficial for the diplomatic relationship between countries.

3. NOTIFICATION IN DOMESTIC LAW

3. 1 ESTONIA

3.1.1 REMOTE SEARCH AND SEIZURE IN DOMESTIC LAW

In Estonia, the principal provision regulating traditional search and seizure powers is Code of Criminal Procedure (CoCP) § 91. Due to the coercive nature of the search and seizure powers, it is considered as possibly one of the most serious violations of the principle of the inviolability of the home[14] and secrecy of communication.[15]

The provision prescribes that search and seizure must be conducted for the purposes outlined in law and its objective is to locate an object to be confiscated or used as

> *"physical evidence, a document, thing or person necessary for the adjudication of a criminal matter, property to be seized for the purposes of compensation for damage caused by a criminal offence or of confiscation, or a body, or to apprehend a fugitive in a building, room, vehicle or enclosed area."*[16]

While it can generally be concluded from case law and legal commentary that evidence in digital form is accepted in courts like any "*tangible*" evidence,[17] it is not evident whether CoCP § 91 would also cover the search of the devices found on the premises subject to a search warrant.[18] Since the provision has been interpreted as to not allow

---

[14] Eesti Vabariigi põhiseadus, footnote 4, § 33; Kergandberg and Pikamäe, footnote 4, p. 268.

[15] Eesti Vabariigi põhiseadus, footnote 4, § 43; Lõhmus, U. (2014) *Põhiõigused kriminaalmenetluses (Fundamental Rights in Criminal Procedure*). 2nd ed. Tallinn: Juura, p. 312.

[16] Kriminaalmenetlusseadustik (Code of Criminal Procedure), footnote 3, § 91(1), § 64(3).

[17] Estonian CoCP does not specifically include the concept of digital evidence but *lex lata* has been interpreted to also cover evidence in digital form. CoCP's lack of clarity regarding digital evidence has been subject to critique in recent research. See e.g. Ginter, J. et al (2013) *Analüüs isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses (Analysis of Ensuring Fundamental Rights and the Speed of Preliminary Investigation in Criminal Procedure)*, pp. 148-151. Available from: http://www.kriminaalpoliitika.ee/en/analuus-isikute-pohioiguste-tagamisest-ja-eeluurimise-kiirusest-kriminaalmenetluses [Accessed 8 March 2017]. See also Osula, Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study, footnote 12, pp. 356-359.

[18] Lõhmus, footnote 15, pp. 312-313.

the digital environment or a computer system as an objective of a search,[19] it is doubtful whether the current CoCP § 91 alone can, in addition to seizing the device where the data is stored, also be applied for searching the data located on the device.

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.[20] For example, in circumstances where an immediate examination of the evidence found on the search premises is not reasonable due to the amount of data and the time needed for listing all the documents in the search protocol, LE can decide that the evidence should be seized for later inspection.[21] Inspection can be used for collecting

> "*information necessary for the adjudication of a criminal matter, detect the evidentiary traces of the criminal offence and confiscate objects which can be used as physical evidence*",

and objects for inspection can include a

> "*document, other evidence or any other object or physical evidence.*"[22]

Nevertheless, it is unclear whether CoCP § 91 alone or in conjunction with CoCP § 83, § 86(2) would offer legal bases for remotely accessing and seizing data, or whether the CoCP surveillance activities[23] should be employed instead. Hopefully the ongoing CoCP reform[24] will clarify the current ambiguity of domestic regulation and thereby offer better protection against possible breach of basic rights.[25]

3.1.2 NOTIFICATION REQUIREMENT FOR REMOTE SEARCH AND SEIZURE IN DOMESTIC LAW

As explained, the Estonian law does not clearly regulate remote search and seizure. Therefore it is not evident what the notification requirement

---

[19] Kergandberg and Pikamäe, footnote 4, p. 269; Lõhmus, footnote 15, p. 313.

[20] Kergandberg and Pikamäe, footnote 4, p. 269.

[21] Kergandberg and Pikamäe, footnote 4, p. 253.

[22] Kriminaalmenetlusseadustik (Code of Criminal Procedure), footnote 3, § 83(1)-(2).

[23] Kriminaalmenetlusseadustik (Code of Criminal Procedure), footnote 3, chap. 31.

[24] Estonia, *Justiitsministeerium, Kriminaalmenetlusõiguse revisjoni lähteülesanne (Initial Task of the Revision of the Law of Criminal Procedure)*, 2015. Available from: http://www.just.ee/sites/www.just.ee/files/kriminaalmenetluse_revisjoni_lahteulesanne.pdf [Accessed 8 March 2017].

[25] Lõhmus, footnote 15, pp. 310, 313.

for remote search and seizure would entail. However, if we take the traditional search and seizure as an example, we would turn to CoCP § 91(7). It prescribes that a search warrant has to be presented for examination to the person

> "*whose premises are to be searched or to his or her adult family member or a representative of the legal person or the state or local government agency whose premises are to be searched.*"

The search warrant identifies what is being searched for, what the objectives of the search are, the reasons for the search as well as the place where the search is conducted [CoCP § 91(4)]. The warrant will have to be signed by the individual to whom the warrant is presented [CoCP § 91(7)]. In the current wording, it appears to be difficult to directly apply the notification requirement in remote search and seizure circumstances, especially with regards to the requirement of signing the warrant, as LE officials carrying out remote searches do generally not come into direct contact with the involved individual.

Remarkably, the regulation does not prescribe an option to delay the notification for search and seizure, such as is possible under the surveillance activities regime. With regard to the latter, a general legal obligation exists to notify

> "*the person with respect to whom the surveillance activities were conducted and the person whose private or family life was significantly violated by the surveillance activities and who was identified in the course of the proceedings*".[26]

This notification explicitly includes explaining the procedure for appeal.[27] However, CoCP § 126^{13}(2) allows a surveillance agency, with the permission of a prosecutor, not to give notification of conduct of surveillance activities if this may

> "*significantly damage the criminal proceedings; significantly damage the rights and freedoms of another person which are guaranteed by law or endanger another person, or endanger the confidentiality of the methods and tactics of a surveillance agency, the equipment or police agent used*

[26] Kriminaalmenetlusseadustik (Code of Criminal Procedure), footnote 3, § 126^{13}(1).
[27] Kriminaalmenetlusseadustik (Code of Criminal Procedure), footnote 3, § 126^{13}(7).

in conducting surveillance activities, of an undercover agent or person who has been recruited for secret cooperation."

The rest of CoCP § 126[13] regulates the conditions for extending the period of non-notification.

3.1.3 NOTIFICATION REQUIREMENT IN THE CASE OF "LOSS OF LOCATION"

Given the traditional focus on tangible items and the overall critique towards the need to update the current search and seizure regime, the circumstances where it is not possible to identify the location of the data to be remotely searched, are not addressed in current regulation. According to practitioners, no specific internal guidelines exist which would help to clarify the details of undertaking remote search and seizure in case of "*loss of location*".[28] It has been suggested that such guidelines should be established and different options for going forward should be examined and assessed domestically, taking into account both national and international restrictions. Any possible extraterritorial reach of the search (or another investigative measure) should be legally justified, though no specific proposals have been made. 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.[29]

3.2 NETHERLANDS

3.2.1 REMOTE SEARCH AND SEIZURE IN DUTCH DOMESTIC LAW

In the Netherlands, search and seizure for LE purposes is regulated in the Dutch Criminal Procedure Code[30] (DCPC) art. 94-99 and art. 110. Depending on the infringement on the right to privacy inherent to that type of location,[31] the competent authority to lead or authorise the search ranges from any law enforcement officer via public prosecutor to investigation judge.

---

[28] Interview with Ms. Eneli Laurits, Estonian Public Prosecutor, 2015; Interview with Mr. Robert Laid, Estonian Assistant Prosecutor, 2015; Interview with Mr. Oskar Gross, Police and Border Guard Board, 2017. Quoted in Osula, A.-M. (2017) *Remote Search and Seizure of Extraterritorial Data*. University of Tartu Press, p. 60.

[29] Osula, Remote Search and Seizure of Extraterritorial Data, footnote 28, pp. 58-62.

[30] DCPC, footnote 3.

However, data in the Netherlands are regarded as non-objects which, bar a few exceptional circumstances based on jurisprudence,[32] for that reason cannot be stolen or fenced or seized by LE in the traditional sense of the law. Instead, they are considered a class of their own.[33] As (regular) seizure is a concept limited to physical objects, "*data seizure*" has received its own definition that allows for it to be taken into the possession or copied for law enforcement purposes.[34] For the purposes of this article we will call this "*data seizure*".[35]

Currently search and data seizure in the Netherlands is limited to situations where physical premises are searched with the express purpose of data seizure.[36] Computers or data storage devices, whether local or remote, are not considered "*premises*" and as such cannot be the target locations of a regular search and seizure.[37] If relevant to the investigation,

---

[31] Under Dutch law a general stratification is made with regards to the inherent privacy of certain locations. In general, homes are more private than a private building that in turn is more private than a vehicle and ultimately a public area. The minimum level of authority that should give the permission is tied to that general stratification.

[32] As a result of jurisprudence there is a category of data under Dutch law that is still considered to be objects. In order for this to happen data has to have similar characteristics to real objects. The most important one of these is the fact that in the case of transfer of an object from one person to another the former must necessarily lose possession of it. This is an uncommon characteristic for data as it can usually be shared and multiplied with losing control of the original data or reducing its quality. See *Runescape* (2012), Hoge Raad, ECLI:NL:HR:2012:BQ9251 and *Habbo Hotel* (2009), Rechtbank Amsterdam, ECLI:NL:RBAMS:2009:BH9789.

[33] Article 80quinquies *(Wetboek van Strafrecht, Dutch Criminal Code – DCC hereafter)*, the Netherlands. In Dutch, defines data "*as any representation of facts, concepts or instructions organised in an standardized format suitable for transfer, interpretation or processing by persons of automated works*" (read: computers, see also footnote 39). This may also include written and printed texts. This definition carries over into the DCPC, footnote 3, though this is not made explicit in the law.

[34] DCPC, footnote 3, art. 125i regulates the existence of this special data seizure as well as the conditions under which it may take place.

[35] A more correct translation – given the discussion in Dutch law about the difference in nature between goods and data – would probably "*securing of data*". For this article we will however use "*data seizure*".

[36] Although if a premise is searched under this power and potentially relevant computers or data storage found they may, under circumstances, still be physically seized for investigation. The Dutch legislator has however indicated that search and data seizure should be used unless taking the objects is absolutely necessary as a matter of subsidiarity. Differently put, as long as there is a reasonable option to take just the data, use of seizure of the data carrier is not allowed. There are of course also other ways for law enforcement to obtain relevant data, such as wiretaps (both voice and data) [DCPC, footnote 3, art. 126m / t / zg] and production orders for all manner of data [DCPC, footnote 3, art. 126n to 126ni] to almost any party in possession of such data.

[37] The law references back to the articles for physical seizure for conditions and competent authorities. DCPC, footnote 3, art. 126n to 126ni jo. DCPC, footnote 3, art. 96b, 97.

data may be seized subject to the same conditions and under the same competent authorities as regular objects.[38]

If devices are found during the execution of the search and data seizure which have access to data stored on remote "*automated works*",[39] those remote systems may be searched as well and any data required to "*uncover the truth*"[40] seized. A simple example of this might be a Network Attached Storage or "*standalone*" hard disks where daily backups of laptops are stored. One important limitation is that such remote data seizure may only take place to the extent that the persons working or residing in the physical place being searched have lawful access to (parts of) those remote systems. Differently put, if such persons have unlawful access to (parts of) such a remote machine, that machine may not be searched in the course of the search and data seizure execution. Currently the law does not specifically provide for remote access outside of the search location.[41]

3.2.2 NOTIFICATION REQUIREMENT FOR REMOTE SEARCH AND SEIZURE IN DOMESTIC LAW

Under Dutch law, notification is considered an essential part of civil rights and liberties and the obligation to notify involved parties after the use of investigatory measures in integrated throughout the DCPC. The Dutch legislator considers the duty to notify corollary to the right to effective remedy as guaranteed by art. 13 ECHR.

In principle, search and data seizure is done "*in the open*" like regular search and seizure. This means that in standard circumstances no attempt is made to (temporarily) hide the fact a search and data seizure took place. Contrary to most other investigatory powers, for which notification is regulated in art. 126bb DCPC, notification for search and data seizure is regulated separately, in art. 125m DCPC. If any data seizure has taken place, the article stipulates all "*involved parties*" should be notified in writing

[38] In practice this requirement is not followed too strictly; however, some sensible (possible) connection to the investigation should exist.

[39] This is the direct translation of the Dutch term defined in DCC, footnote 33, art. 80sexies. The definition also includes automation such as routers, smart watches etc. Under the new Computercriminaliteit III (Computercrime III) law proposal, the definition will be changed to be even more comprehensive. The term however, is clunky even in Dutch, so we will use more regular terms for the remainder of the article.

[40] Dutch police in an criminal investigation are tasked to uncover the truth whatever it may be.

[41] We may, however, soon see a testcase where the search is not formally closed and then "*continued*" from a remote location, the police station. It then becomes a remote remote search. It is unclear whether the judiciary would agree to this.

of the fact that search and data seizure took place as well as the general nature of the data seized data as long as this is reasonable possible.[42]

In principle all relevant parties[43] must, within reason, be notified of an investigatory measure. Information about the kind and general extent of data seized should be included in the notification as to allow involved parties to determine if and how much their rights may have been infringed. This does not create an obligation to provide a detailed list or description of all data seized.

The involved parties that should be notified are the suspect, the party responsible for the data and the rightful owner or user or inhabitant of the physical premises searched. However, notification of the suspect may be omitted if he will be made aware of the fact though the official documents in his case (which he will receive at the latest at the moment of his indictment).[44]

In deviation of the law regulating regular search and seizure the public prosecutor in charge of the data search and seizure, or the investigate judge if he was the authority executing the search, is explicitly given the legal possibility to postpone notification of all involved parties as long as the due course of the investigation would be negatively impacted due to notification as per art. 125m, lid 2 DCPC.

3.2.3 NOTIFICATION REQUIREMENT IN THE CASE OF "LOSS OF LOCATION"

Currently no particular legislation exists in the Netherlands to deal with the problem of "*loss of (knowledge of) location*".[45] As discussed above, the law does not expect "*unreasonable*" effort to notify. Not knowing who to address or where could clearly fall under this limitation. However from the legislative documents it is clear that cyberspace and a habitual situation of "*loss of location*" was not particularly on the legislators mind. The legislator seems to have assumed that any inadvertent cross-border

[42] The legislators intent here is not to overburden law enforcement with (neigh) impossible tasks such as for instance finding a suspect who has left for another country, current location unknown.

[43] Explicit reference is made in the legislatory documents to Recommendation R(95) 13 of the Council of Europe defining "*involved parties*" with regards to investigatory measures with regards to data, extending the parties to be notified from previous legislation.

[44] More detailed rules apply in particular circumstances, but are beyond the scope of this article.

[45] See Koops and Goodwin, footnote 1, pp. 8-9 for a distinction between the two. In practice both meanings are relevant.

search and data seizure would be an exception and employing the MLA procedures the traditional means to be employed.[46]

Habitual loss of location potentially adds a new relevant "*involved*" party to the mix, i.e. the state in which the remote data was (as determined eventually) seized. However, the legislator's intent to create a limited list of parties to be notified is clear in the legislative documents,[47] and foreign states are not on the list.

However, new law currently being developed is (likely) going to change relevant legislation with regards to search and data seizure.

The first of these law proposals is the Dutch Computer Crime III law proposal which was passed by the House of Commons in December 2016 and is currently awaiting continuation of the legislative process.[48] If this law passes, remote search and data seizure will no longer be tied to the search of physical locations. Instead systems or "*devices*" may be remotely targeted. After considerable debate, the power for remote search and seizure on systems or devices has been limited to crimes which carry a maximum penalty of eight years imprisonment minimum or crimes that will be specifically listed in lower regulation.[49] This is a significant increase from earlier plans[50] and together with other results from parliamentary

---

[46] See Tweede Kamer (2004/2005), *Kamerstukken II 2004/2005*, 26 671, nr. 10, p. 23. Available from: https://zoek.officielebekendmakingen.nl/kst-26671-10.pdf [Accessed 8 March 2017].

[47] Tweede Kamer, (1998/1999), *Kamerstukken II 1998/1999*, 26671, 3, p. 52. Available from: https://zoek.officielebekendmakingen.nl/kst-26671-3.pdf [Accessed 8 March 2017].

[48] All official documents pertaining to this law proposal can be found under parliamentary file number 34372. An overview of the current state of the law proposal as well as all official documents can be found at the site of 1e Kamer, where the proposal is currently awaiting being put on the agenda to be discussed. Eerste Kamer, *afdeling Inhoudelijke Ondersteuning en de unit Communicatie & Protocol*. Available from: https://www.eerstekamer.nl/wetsvoorstel/34372_computercriminaliteit_iii [Accessed 8 March 2017].

[49] Eerste Kamer (2015/2016), *Kamerstukken I 2015/2016, 34372*, A p. 5, art. 126nba (1), second section and under d. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-A.pdf [Accessed 8 March 2017]; Tweede Kamer (2004/2005), *Kamerstukken II 2015/2016* Kamerstukken II 2015/2016, 34372, 4, p. 5. Available from: https://zoek.officiele bekendmakingen.nl/kst-34372-4.pdf [Accessed 8 March 2017]; Tweede Kamer (2004/2005), *Kamerstukken II 2015/2016* Kamerstukken II 2015/2016, 34372, 34, item 17. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-17.pdf [Accessed 8 March 2017]; Tweede Kamer (2015/2016), *Kamerstukken II 2015/2016*, 34372, 34, item 25. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-25.pdf [Accessed 8 March 2017]; Tweede Kamer (2004/2005), *Kamerstukken II 2015/2016*, Handelingen II, 2015/2016, 34372, 34, item 26, p. 17, 29, 42-44, 52. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-26.pdf [Accessed 8 March 2017].

[50] See the Internet consultation on this law proposal: Kennis- en exploitatiecentrum Officiële Overheidspublicaties, *Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (Computercriminaliteit III).* Available from: https://www.internet consultatie.nl/computercriminaliteit/document/727 [Accessed 8 March 2017]. The proposed article was at that time known as 125ja Sv (DCPC).

proceedings dramatically reduces the number of situations in which such a remote search and seizure may be executed.

This new remote search and data seizure is classified as a "*special investigatory measure*". Notification for this new investigatory measure will therefore be regulated by art. 126bb DCPC, the general notification article for the Dutch special powers of investigation. The differences with the notification for art. 125m DCPC are limited, which is not surprising as the legislator explicitly took art. 126bb DCPC as the model for art. 125m DCPC.[51] The article will still not count "*foreign states*" under the "*parties involved*" that need to be notified, although extensive coverage in the legislative proceedings make it clear the government is aware of the issue.

The government has stated during the legislative process that the Netherlands, when engaging in (potentially) cross-border investigative activity, will in principle stop the activity and notify the state involved when the physical nexus of the activity becomes apparent and is outside Dutch territory. From the wording, however, it is clear that this is seen as a matter of comity and not of legal obligation.[52] According to the government, the possibility of "*loss of location*" and difficulties with the requirement of notification should not be an absolute barrier to (potentially) cross-border investigations.[53]

At the very least this seems to be a new direction that introduces a divide in the DCPC. For instance, current legislation for placing a wiretap on a phone when it is known to be active in the territory of another state or when this becomes apparent during the wiretap, would in principle require notification and consent of that state.[54]

A second relevant law proposal is a significant redraft of the complete DCPC. It is too early to talk about specific content and consequences of this proposal, since it is unlikely to enter into force before 2022 and its drafting is currently very much in initial stages. Nevertheless, the intent

---

[51] Tweede Kamer (2003/2004), *Kamerstukken II 2003/2004,* 29441, 3, p. 19. Available from: https://zoek.officielebekendmakingen.nl/kst-29441-3.pdf [Accessed 8 March 2017].

[52] Tweede Kamer (2015/2016), *Handelingen II 2015/2016, 34372, 34, item 26*, pp. 42, 43, 45. Available from: https://zoek.officielebekendmakingen.nl/h-tk-20162017-34-26.pdf [Accessed 8 March 2017].

[53] Tweede Kamer (2015/2016), *Handelingen II 2015/2016, 34372, 34, item 26*, p. 45. Available from: https://zoek.officielebekendmakingen.nl/h-tk-20162017-34-26.pdf [Accessed 8 March 2017].

[54] DCPC, footnote 3, art. 126ma.

of the legislator, as apparent from the first draft put up for Internet consultation,[55] does not seem to indicate significant changes to the general ideas behind notification, nor do the plans seem to include notification of a foreign state when an investigation turns cross-border beyond any such requirements already existent in current law.

3.3. UNITED STATES

Rule 41 of the Federal Rules of Criminal Procedure (FRCP) regulates the procedures for obtaining a search warrant in federal court. The US has recently amended FRCP Rule 41 so that it now also allows for remote search warrants as well as physical search warrants. Under the amended FRCP Rule 41, a judge can now 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"*

and a search of multiple computers in numerous districts would be allowed.[56] From the reading of the new text of the law, which allows to target data when the location of the data is unknown, it follows that possible extraterritoriality cannot be always avoided.

---

[55] See Ministerie van Veiligheid en Justitie, *Memorie van Toelichting: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek*. Available from: https://www.rijksoverheid.nl/documenten/kamerstukken/2017/02/07/memorie-van-toelichting-vaststellingswet-boek-2-van-het-nieuwe-wetboek-van-strafvordering-het-opsporingsonderzoek [Accessed 8 March 2017] – preliminary numbering (these numbers will change in a later stage of the legislative procedure) section 7.3.1/art. 2.7.3.1.1, pp. 184-188. Confusingly, as these legislative processes are running parallel, this proposal is not taking into account the changes due to be made through the Wet Computercriminaliteit III yet.

[56] The previous wording of Rule 41 entailed a territorial limitation to the locations within the district. See United States Courts (2016) *Current Rules of Practice & Procedure, Criminal Rules 4, 41, and 45, Redline of Amended Rules, Including Committee Notes* pp. 10-14. Available from: http://www.uscourts.gov/file/21315/download [Accessed 8 March 2017]. See also US Government's comments on extraterritoriality at United States Department of Justice (2013) *Mythili Raman Letter to Advisory Committee on the Criminal Rules.* Available from: http://justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf [Accessed 8 March 2017].

The amendments were target to a substantial criticism,[57] cautioning that such transborder access would 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.[58]

In terms of notification, FRCP Rule 41 (f)(1)(c) prescribes that, in case of remote search and seizure,

> "*the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied"*.

The means of accomplishing the notification may among others include electronic means, reasonably calculated to reach that person. Such wording has received critique as it does not set an absolute obligation to provide the notice but instead requires the officer to make "*reasonable efforts"*, thereby casting doubt to the "*constitutional adequacy"* of the warrant.[59] Professor Orin Kerr has warned that since a remote search is essentially a secret search, there is nothing about the search itself to provide notice, and therefore this may signify a shift from a standard of notice searches to a standard of delayed notice (aka "*sneak and peek"*) searches.[60]

---

[57] E.g. Rule 41 Coalition Letter (2016). Available from: https://noglobalwarrants.org/assets/Rule41CoalitionLetter.pdf [Accessed 8 March 2017]; Reitman, R. (2016) *With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Governmen*t, Electronic Frontier Foundation. Available from: https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government [Accessed 8 March 2017]; Tor Project Blog (2016) *Day of Action: Stop the Ch*anges to Rule 41. Available from: https://blog.torproject.org/blog/day-action-stop-changes-rule-41 [Accessed 8 March 2017] inviting the US Congress to support the "*Stop Mass Hacking Act*".

[58] Pilkington, E. (2014) *FBI Demands New Powers to Hack into Computers and Carry out Surveillance.* [Online] The Guardian. Available from: http://www.theguardian.com/us-news/2014/oct/29/fbi-powers-hacking-computers-surveillance [Accessed 8 March 2017]. Read more at e.g. Thompson II, R. (2016) *Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure*. Congressional Research Service. Available from: https://www.fas.org/sgp/crs/misc/R44547.pdf [Accessed 8 March 2017]; Osula, Transborder Access and Territorial Sovereignty, footnote 1, p. 731.

[59] American Civil Liberties Union, *ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media* (2014) p. 15. Available from: https://www.aclu.org/sites/default/files/assets/aclu_comments_on_rule_41.pdf [Accessed 8 March 2017] quoting *United States v. Freitas*, 800 F.2d 1451,1456 (9th Cir. 1986) [citing *Berger v. New York*, 388 U.S. 41, 60 (1967)].

[60] United States Courts (2014). Advisory Committee on Rules of Criminal Procedure - April 2014., p. 252. Available from: http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2014 [Accessed 8 March 2017].

Another concern was that the new wording gives LE the option to leave the notice at the third-party service providers as the (legal) person whose property was searched. However, this would not guarantee the actual target of the search to get the notice, thereby leaving him/her without the possibility to challenge the search warrant.[61]

The government's response to the above-mentioned critique explained that the wording of the provision was chosen to provide a parallel system to notices in physical searches where similarly, in case of not being able to deliver a notice to the person from whom, or from whose premises, the property was taken, the copy of the warrant and receipt may be left at the place where the officer took the property.[62] Upon government's request, the notice may be delayed "*only if authorised by a statute"* [Rule 41 (f) (3)].[63]

There have also been proposals from academics suggesting that in case it would inadvertently turn out that the subject of the search is located outside the territory of the US, the foreign government should be immediately notified and general information about such searches and their circumstances reported and made public to the extent possible, unless there are grounds to believe that that such notification would significantly jeopardize the investigation.[64] Currently, such an option is not foreseen in the law.

4. DISCUSSION

This article compared three countries' domestic regulation of the notification requirement under the remote search and seizure regime. The regulation of notification in none of these countries has been free from critique and as can be seen below may differ significantly.

	Netherlands	United States	Estonia
Regulation of search and seizure of digital evidence	DCPC art. 94, 94a, 95-97, 110, 125i, 125j, Awbi art. 2-6, 10	FRCP Rule 41	Somewhat unclear but generally CoCP § 91 and CoCP § 83, § 86(2)

[61] ACLU suggests that notice should be given to both. American Civil Liberties Union, footnote 59, p. 16.

[62] United States Courts (2015). Advisory Committee on Rules of Criminal Procedure - May 2015, p. 93. Available from: http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-may-2015 [Accessed 8 March 2017].

[63] See generally, Thompson II, footnote 58, p. 10.

[64] Daskal, J. (2016) *Rule 41 Has Been Updated: What's Needed Next* [Online] Just Security. Available from: https://www.justsecurity.org/35136/rule-41-updated-needed/ [Accessed 8 March 2017].

Regulation of remote search and seizure	DCPC 125i, 125m, 125j	FRCP Rule 41	Not explicitly regulated
Notification requirement	DCPC 94 (3) (providing a description of assets seized), 125m, Awbi art. 11	FRCP Rule 41 (f)(1)(c) "*must take reasonable efforts*"	CoCP § 91(7) but does not take into account the characteristics of remote search and seizure
Possibility to delay the notification of search and seizure	DCPC 125m (only for search and data seizure 125i DCPC cases), Awbi art 11 (2)	FRCP Rule 41 (f)(3)	Not regulated under the search and seizure regime but mentioned under surveillance activities

Tab. 1: Comparison of the domestic regulation of the Netherlands, United Nations and Estonia

Firstly, we observe that the increasingly occurring circumstances of "*loss of location*" are making it difficult for the legislator to directly employ the traditional notification regime designed for searching and seizing tangible items. Examples were presented in this article where the notification of the involved parties would require signing the warrant which may be challenging in situations where LE does not have direct contact with the individuals in question. Particularly, we would like to point out the difficulties in defining "*reasonable effort*" which needs to be made by the LE in identifying the individual to be notified. On the one hand, a relatively low threshold of the "*effort*" would probably speed up the investigation, but at the same time would not aim to grant the widest possible protection for the actual targets of the search. On the other hand, too high of a threshold would saddle LE with an unmanageable task as well as (depending on domestic regulation) increase the risk of procedural errors. The more detailed meaning of "*reasonable effort*" will probably develop with emerging case law.

Secondly, we can see that countries are having trouble in identifying the "*involved parties*" whose rights may have been infringed upon and who should therefore be notified about the employment of the investigative measure. In the cases of the Netherlands and the US, the issue has been under discussion, whereas in Estonia the legal debate has not yet reached these questions as part of the on-going CoCP reform. We believe that the standard approach should be the requirement to notify person in overall control of the computer system which was remotely searched or data to be

targeted by the remote search and seizure. If the actual target of the search cannot be reasonably identified, a third party service provider may be notified instead. Notification of all parties of whom relevant data was found during the search could be considered as an option but should not be a legal obligation as this may place to great a burden on the investigation.

Thirdly, we suggest including an explicit possibility of a delayed notice for the notification requirement of the remote search and seizure regime, such as foreseen by the Dutch and US legislation. This option may be connected with specific exigent circumstances and should be accompanied with further regulation on the conditions for postponing the notification as not to allow for avoiding the notification requirement altogether.

Fourthly, we conclude that despite all countries being aware of the fact that remote search and seizure may add foreign states to the list of parties whose rights have been infringed upon, only Belgium law currently requires the foreign state, within reason, to be notified. Failure to do so however is not considered a critical breach of law as apparent from case law.[65] It has also been suggested that prior notification to the other state is not desirable due to uncertainty and potential delay.[66]

It follows then that none of the researched states seem to think of notification of a foreign state as a matter of obligation under international law. Instead it is seen, at most, as a matter of comity, regardless of domestic regulation or lack thereof. The authors have not found any indications that the researched countries are deviant from the norm in this respect.

Looking from an international law perspective, and avoiding going into the details of the debate of legality of extraterritorial remote search and seizure, the authors have found no indication of an obligation to notify the other state about a transborder remote search and seizure targeting data stored on the territory of that state. In fact, the CoE Convention on Cybercrime has left the matter explicitly to domestic law.

Finally, we underline that the notification regime, despite the challenges set out above must remain as an integral part of the remote search and seizure regime due to the need to protect the principles of fair trial and effective remedy. Countries should consider options for making

[65] Hof van Beroep Brussel 26-06-2008, vol. 6, Tijdschrift voor Strafrecht: jurisprudentie, nieuwe wetgeving en doctrine voor de praktijk, 2008, 26th june, p. 467.

[66] New Zealand and Law Commission (2007) *Search and Surveillance Powers.* Wellington. p. 228. Available from: http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R97.pdf [Accessed 8 March 2017].

the notification of other states more feasible under the circumstances of "*loss of location*". One option would be to develop a shared platform, or use an existing one, between cooperative states where information regarding transborder investigative measures could be shared, if needed, in retrospect.

5. CONCLUSION

Despite the requirement for notification being widely accepted as part of traditional search and seizure, following this obligation in the context of remote search and seizure is not an easy task for LE. On the international level, the notification of foreign states about remote search and seizure of data located on their territory, if they can even be identified, is at the time being a matter of comity and not a legal obligation. Domestically, traditional search and seizure regimes may not be equipped with flexible options for notifying individuals who are not present at the premises of the search or who cannot be easily identified. "*Loss of location*" that may occur, for example, due to the employment of anonymising tools, is challenging the notification requirement even further by possibly making the identification of the individual targeted by the search unfeasible at all. However, given that notification serves as an important tool for the targeted individual by way of protecting his/her right for a fair trial and effective remedy, the legislator should not abandon the requirement as part of remote search and seizure but instead use the reasonable effort approach.

LIST OF REFERENCES

[1] Advisory Committee on Rules of Criminal Procedure - April 2014, United States Courts. Available from: http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2014 [Accessed 8 March 2017].

[2] Advisory Committee on Rules of Criminal Procedure - May 2015, United States Courts. Available from: http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-may-2015 [Accessed 8 March 2017].

[3] American Civil Liberties Union, *ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media* (2014), p. 15. Available from: https://www.aclu.org/sites/default/files/assets/aclu_comments_on_rule_41.pdf [Accessed 8 March 2017].

[4] Hof van Beroep Brussel 26-06-2008, vol. 6, Tijdschrift voor Strafrecht: jurisprudentie, nieuwe wetgeving en doctrine voor de praktijk, 2008, 26th june, p. 467.

[5] *Code d'Instruction Criminelle (Belgium Code of Criminal Procedure)*, Livre Premier, Belgium. In France.

[6] Council of Europe (2001) *Explanatory Report to the Convention on Cybercrime (ETS No. 185)*. Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContentdocumentId=09000016800cce5b [Accessed 8 March 2017].

[7] Council of Europe (2012) *Transborder Access and Jurisdiction: What Are the Options?* Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContentdocumentId=09000016802e79e8 [Accessed 8 March 2017].

[8] Council of Europe, Convention on Cybercrime, ETS No. 185.

[9] Council of Europe, European Convention on Human Rights, 1950.

[10] Council of Europe, Recommendation R(95) 13.

[11] Daskal, J. (2016) *Rule 41 Has Been Updated: What's Needed Next* [Online] Just Security. Available from: https://www.justsecurity.org/35136/rule-41-updated-needed/ [Accessed 8 March 2017].

[12] Eerste Kamer (2015/2016), *Kamerstukken I 2015/2016*, 34372, A p. 5. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-A.pdf [Accessed 8 March 2017].

[13] Eerste Kamer, *afdeling Inhoudelijke Ondersteuning en de unit Communicatie & Protocol*. Available from: https://www.eerstekamer.nl/wetsvoorstel/34372_computercriminaliteit_iii [Accessed 8 March 2017].

[14] *Eesti Vabariigi põhiseadus (Constitution of the Republic of Estonia)*, RT 1992, 26, 349; RT I, 15. 5. 2015, 2. Estonia: Riigi Teataja. In Estonian.

[15] Estonia, Justiitsministeerium, *Kriminaalmenetlusõiguse revisjoni lähteülesanne (Initial Task of the Revision of the Law of Criminal Procedure)*, 2015. Available from: http://www.just.ee/sites/www.just.ee/files/kriminaalmenetluse_revisjoni_lahteulesanne.pdf [Accessed 8 March 2017].

[16] Ginter, J. et al. (2013) *Analüüs isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses (Analysis of Ensuring Fundamental Rights and the Speed of Preliminary Investigation in Criminal Procedure)*. Available from: http://www.kriminaalpoliitika.ee/en/analuus-isikute-pohioiguste-tagamisest-jaeeluurimise-kiirusest-kriminaalmenetluses [Accessed 8 March 2017].

[17] Goldsmith, J. (2001) *The Internet and the Legitimacy of Remote Cross-Border Searches*. University of Chicago Law School, Chicago Unbound. Available from:

http://chicagounbound.uchicago.edu/cgi/viewcontent.cgiarticle=1316&contextpublic_law_and_legal_theory [Accessed 8 March 2017].

[18] *Grondwet (The Dutch Constitution)*, the Netherlands. In Dutch.

[19] Habbo Hotel (2009), Rechtbank Amsterdam, ECLI:NL:RBAMS:2009:BH9789.

[20] Interview with Mr. Geert Schoorens, Federal Prosecutor's Office of Belgium, 2015.

[21] Interview with Mr. Oskar Gross, Police and Border Guard Board, 2017.

[22] Interview with Mr. Robert Laid, Estonian Assistant Prosecutor, 2015.

[23] Interview with Ms. Eneli Laurits, Estonian Public Prosecutor, 2015.

[24] Kennis- en exploitatiecentrum Officiële Overheidspublicaties, *Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (Computercriminaliteit III)*. Available from: https://www.internetconsultatie.nl/computercriminaliteit/document/727 [Accessed 8 March 2017].

[25] Kergandberg, E. and Pikamäe, P. (2012) *Kriminaalmenetluse seadustik: kommenteeritud väljaanne (Code of Criminal Procedure: Commented Edition)*. Tallinn: Juura.

[26] Koops, B.-J. and Goodwin, M. (2014) *Cyberspace, the Cloud, and Cross-Border Criminal Investigation*. Tilburg University, Tilburg Institute for Law, Technology, and Society, WODC. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263 [Accessed 8 March 2017].

[27] *Kriminaalmenetlusseadustik (Code of Criminal Procedure)*, RT I 2003, 27, 166; RT I, 31. 12. 2016, 46. Estonia: Riigi Teataja. In Estonian.

[28] Lõhmus, U. (2014) *Põhiõigused kriminaalmenetluses (Fundamental Rights in Criminal Procedure)*. 2nd ed. Tallinn: Juura.

[29] Ministerie van Veiligheid en Justitie, *Memorie van Toelichting: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek*. (2017) Available from: https://www.rijksoverheid.nl/documenten/kamerstukken/2017/02/07/memorie-van-toelichting-vaststellingswet-boek-2-van-het-nieuwe-wetboek-van-strafvordering-het-opsporingsonderzoek[Accessed 8 March 2017].

[30] New Zealand and Law Commission (2007) *Search and Surveillance Powers.* Wellington. Available from: http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R97.pdf [Accessed 8 March 2017].

[31] Osula, A.-M. (2015) *Transborder Access and Territorial Sovereignty*. Computer Law & Security Review, 31(6).

[32] Osula, A.-M. (2016) *Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Stud*y. International Journal of Law and Information Technology 24(4).

[33] Osula, A.-M. (2017) *Remote Search and Seizure of Extraterritorial Data*. University of Tartu Press.

[34] Pilkington, E. (2014) *FBI Demands New Powers to Hack into Computers and Carry out Surveillance*. [Online] The Guardian Available from: http://www.theguardian.com/us-news/2014/oct/29/fbi-powers-hacking-computers-surveillance [Accessed 8 March 2017].

[35] Reitman, R. (2016) *With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government*, Electronic Frontier Foundation. Available from: https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government [Accessed 8 March 2017].

[36] Rule 41 Coalition Letter (2016). Available from: https://noglobalwarrants.org/assets/Rule41CoalitionLetter.pdf [Accessed 8 March 2017].

[37] Runescape (2012), Hoge Raad, ECLI:NL:HR:2012:BQ9251.

[38] Svantesson, D. (2016) *Preliminary Report: Law Enforcement Cross-Border Acces to Data*, pp. 4-5, 9. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874238 [Accessed 8 March 2017].

[39] *The Wet Openbaarheid Bestuur (Governance Transparency Act)*, the Netherlands. In Dutch.

[40] Thompson II, R. (2016) *Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure*. Congressional Research Service. Available from: https://www.fas.org/sgp/crs/misc/R44547.pdf [Accessed 8 March 2017].

[41] Tor Project Blog (2016) *Day of Action: Stop the Changes to Rule 41*. Available from: https://blog.torproject.org/blog/day-action-stop-changes-rule-41 [Accessed 8 March 2017].

[42] Tweede Kamer (2004/2005), *Kamerstukken II 2004/2005, 26 671, nr. 10*. Available from: https://zoek.officielebekendmakingen.nl/kst-26671-10.pdf [Accessed 8 March 2017].

[43] Tweede Kamer (2004/2005), *Kamerstukken II 2015/2016 Kamerstukken II 2015/2016, 34372*, 4. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-4.pdf [Accessed 8 March 2017]

[44] Tweede Kamer (2004/2005), *Kamerstukken II 2015/2016 Kamerstukken II 2015/2016, 34372*, 34. Available from: https://zoek.officielebekendmakingen.nl/kst-34372-17.pdf [Accessed 8 March 2017].

[45] Tweede Kamer (2004/2005), *Kamerstukken II 2015/2016, Handelingen II, 2015/2016, 34372, 34.* Available from: https://zoek.officielebekendmakingen.nl/kst-34372-26.pdf [Accessed 8 March 2017].

[46] Tweede Kamer (2015/2016), *Handelingen II 2015/2016, 34372, 3*4. Available from: https://zoek.officielebekendmakingen.nl/h-tk-20162017-34-26.pdf [Accessed 8 March 2017].

[47] Tweede Kamer (2015/2016), *Kamerstukken II 2015/2016, 34372, 34.* Available from: https://zoek.officielebekendmakingen.nl/kst-34372-25.pdf [Accessed 8 March 2017].

[48] Tweede Kamer (1998/1999), *Kamerstukken II 1998/1999, 26671, 3*. Available from: https://zoek.officielebekendmakingen.nl/kst-26671-3.pdf [Accessed 8 March 2017].

[49] Tweede Kamer (2003/2004), *Kamerstukken II 2003/2004, 29441, 3*. Available from: https://zoek.officielebekendmakingen.nl/kst-29441-3.pdf [Accessed 8 March 2017].

[50] United States Courts. (2016) *Current Rules of Practice & Procedure, Criminal Rules 4, 41, and 45, Redline of Amended Rules, Including Committee Notes*. Available from: http://www.uscourts.gov/file/21315/ download [Accessed 8 March 2017].

[51] *United States v. Freitas*, 800 F.2d 1451,1456 (9th Cir. 1986).

[52] US Government's comments on extraterritoriality at United States Department of Justice (2013) Mythili Raman Letter to Advisory Committee on the Criminal Rules. Available from: http://justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf [Accessed 8 March 2017].

[53] *Wetboek van Strafrecht (Dutch Criminal Code)*, the Netherlands. In Dutch.

[54] *Wetboek van Strafvordering (Dutch Criminal Procedure Code)*, the Netherlands. In Dutch.

[55] *Wetboek van Strafvordering*, the Netherlands. In Dutch.

[56] Zoetekouw, M. (2016) *Ignorantia Terrae Non Excusat*. Available from: 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 [Acessed 8 March 2017].