UNLAWFULLY OBTAINED EVIDENCE, CROSS-BORDER LAW ENFORCEMENT OPERATIONS AND BORDERLESS NETWORKS

Juhana Riekkinen

University Lecturer in Legal Informatics, University of Lapland, Faculty of Law
Yliopistonkatu 8, PO BOX 122, 96101 Rovaniemi, FI
juhana.riekkinen@ulapland.fi; https://research.ulapland.fi/en/persons/juhana-riekkinen

Keywords: ***Criminal Investigations, Law Enforcement, International Co-operation, Evidence, Exclusionary Rules, ANOM***

Abstract: *In certain jurisdictions, national evidence law rules may prohibit the use of illegally or unlawfully gathered evidence in criminal proceedings, or at least give the court the possibility to exclude illegally gathered evidence under certain circumstances. However, when it comes to cross-border investigative measures in the global and borderless network environment, it may not always be clear what "unlawfully obtained" or "illegally obtained" actually means. This paper discusses the different possible meanings of illegality/unlawfulness in the context of such investigative operations. The discussion is based on the examples of Finnish law and case law pertaining to evidence derived from the supposedly secure ANOM messaging application, widely used by criminals, in the international law enforcement operation known as Operation Trojan Shield/Greenlight.*

1. Introduction

ANOM, a supposedly secure, encrypted messaging app running on specifically modified Android smartphones, was introduced in late 2018. In the next few years, the application became relatively popular in the criminal underworld. In reality, however, ANOM was a trojan horse promoted and distributed by the United States Federal Bureau of Investigation (FBI), and it allowed the FBI and cooperating law enforcement authorities (LEAs) around the world to monitor and collect all communications sent through this application – a total of 27 million messages were collected and processed. The sting operation was made public on 8 June 2021, when over 800 people were arrested in a coordinated raid in 16 different countries. The operation was designated Operation Trojan Shield by the FBI, Operation Greenlight by Europol, and Operation Ironside by the Australian Federal Police.[1]

In Finland, approximately 100 people were arrested and dozens have been subsequently prosecuted in connection with Operation Trojan Shield/Greenlight.[2] In several of these cases, the defendants have challenged the admissibility of evidence derived from the ANOM application. In April 2022, the Court of Appeal of

[1] See, e.g., BBC News, ANOM: Hundreds arrested in massive global crime sting using messaging app. https://www.bbc.com/news/world-57394831, 8 June 2021, Europol, 800 criminals arrested in biggest ever law enforcement operation against encrypted communication. https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication, 8 June 2021, United States Department of Justice, FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown. https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive, 8 June 2021, and Australian Federal Police, AFP-led Operation Ironside smashes organised crime. https://www.afp.gov.au/news-media/media-releases/afp-led-operation-ironside-smashes-organised-crime, 8 June 2021. See also Farlow/Edwards 2022, p. 15.

[2] See, e.g., Yle News, Trojan Shield: Finnish police arrest 100 in international bust. https://yle.fi/news/3-11970996, 8 June 2021, and Yle News, 12 charged in Finland through FBI-led sting operation. https://yle.fi/news/3-12160958, 26 October 2021.

Eastern Finland published a decision denying the defendants' requests for exclusion of ANOM messages (I-SHO 2022:2).[3] In its later judgment concerning the same criminal case (I-SHO 2022:5), the Court of Appeal again rejected the requests for exclusion and further found that the technical method of acquisition did not negatively affect the probative value of evidence acquired from the ANOM app.[4] In October 2022, the Supreme Court granted a limited leave to appeal in this case, among other issues concerning the admissibility of ANOM evidence.[5] A further Court of Appeal of Eastern Finland decision from October 2022 declared ANOM evidence admissible in a different case.[6] The Court of Appeal of Helsinki has, likewise, published a decision accepting the admissibility of ANOM evidence (HelHO 2022:4).[7] At the district court level, there have been several decisions concerning the admissibility of ANOM evidence, and in some cases requests for exclusion have been accepted.[8]

The challenges on admissibility have been mainly based on chapter 17, section 25(3) of the Code of Judicial Procedure (4/1734, CJP). This section states that [in cases other than those regulated in sub-sections 1 and 2] "the court may use also evidence that has been obtained unlawfully unless such use would endanger the conduct of fair proceedings, taking into consideration the nature of the matter, the seriousness of the violation of law in obtaining the evidence, the significance of the method of obtaining the evidence in relation to its credibility, the significance of the evidence for deciding the matter, and the other circumstances."[9]

Despite the wording that seems to set admissibility as the default option even when the evidence in question has been obtained unlawfully, the provision can be classified as a discretionary exclusionary rule (*Beweisverwertungsverbot*). Section 25, which contains separate sub-sections on exclusion of evidence that was obtained through torture[10] or in violation of the defendant's privilege against self-incrimination,[11] was added to the CJP in connection with the reform of evidence law that entered into effect on 1 January 2016 (amendment 732/2015). The new rules on exclusion of evidence are closely linked to the requirements of the right to fair trial as guaranteed by Article 6 of the European Convention on Human Rights (ECHR) and the case law of the European Court of Human Rights.

Importantly, the exclusionary rule in CJP, chapter 17, section 25(3) only applies to *unlawfully obtained evidence*. However, it remains unclear exactly what kind of requirements this wording entails when evidence has been obtained through mutual legal assistance (MLA) procedures and/or voluntary disclosure of information between authorities, and especially when evidence has been collected abroad or by foreign LEAs that are not bound by Finnish national legislation concerning measures available in intelligence activity or criminal

3 Court of Appeal of Eastern Finland, 20 April 2022, decision 185, case R 21/1261 (published as I-SHO 2022:2).

4 Court of Appeal of Eastern Finland, 8 July 2022, judgment 22/128244, case R 21/1261 (published as I-SHO 2022:5).

5 KKO VL:2022-91.

6 Court of Appeal of Eastern Finland, 24 October 2022, decision 513, case R 22/756.

7 Court of Appeal of Helsinki, 12 May 2022, decision 644, case R 21/1889 (published as HelHO 2022:4). Notably, the decision was published in November 2022, six months after it was issued.

8 A systematic review of district court decisions on the admissibility of ANOM evidence has not been performed for the purposes of this paper. The author is aware of at least two cases where the District Court of Helsinki has excluded some ANOM evidence, but more commonly district courts have rejected such requests. In a master's thesis published in March 2022, nine relevant decisions from four different district courts were identified. In three out of the nine cases the court considered the evidence unlawfully obtained, but evidence was excluded in one case only. See Rajala 2022, pp. 66–69.

9 All translations of Finnish legislative texts in this paper are from Finlex, Translations of Finnish acts and degrees. https://www.finlex.fi/en/laki/kaannokset.

10 Sub-section 1: "The court may not use evidence that has been obtained through torture."

11 Sub-section 2: "The court may not, in a criminal matter, use evidence obtained contrary to the right to remain silent provided in section 18. The prohibition against use also applies to evidence obtained from a person in a procedure other than a pre-trial investigation or in criminal proceedings, through a threat of coercive measures or otherwise against his or her will, if he or she at the time was a suspect or defendant in an offence or if a pre-trial investigation or proceedings were underway for an offence for which he or she was charged, and if the obtaining of the evidence would have been contrary to section 18. If, however, a person in other than criminal proceedings or comparable procedure has, in connection with fulfilling his or her statutory obligation, given a false statement or submitted a false or untruthful document or a false or forged object, this may be used as evidence in a criminal matter concerning his or her conduct in violation of his or her obligation."

investigations. This was the case in the FBI-led Operation Trojan Shield/Greenlight, and similar questions can be raised by other investigative actions targeting "secure" messaging apps (e.g., the earlier operations against EncroChat[12] and Sky ECC[13]).

In this paper, I discuss the alternative interpretations of the meaning of 'illegal' or 'unlawful' in the context of international law enforcement operations and evidence collection in the global network environment, and analyze the consequences that would follow from adopting these different interpretations. The discussion partially draws from the argumentation presented in the aforementioned court cases, where the lawfulness of evidence collection has been a major point of contention. To be clear, I do not aim to formulate a categorical *de lege lata* answer to the question of whether ANOM evidence should be admissible in criminal proceedings in Finland or in other countries.

2. Different meanings of unlawful or illegal

2.1. Three questions

If the (possible) exclusion of evidence in a criminal trial is dependent on whether the evidence has been obtained unlawfully, as is the case in the aforementioned exclusionary rule of CJP, chapter 17, section 25(3), it is important to pinpoint what exactly is meant by both 'unlawfully' and 'obtained'. When the evidence has been collected originally by a foreign LEA, at least three relevant distinctions can be made.

In English, 'unlawful' can mean something that is not authorized by law or based on a clear legal provision. In contrast, something that is 'illegal' may be understood to be specifically forbidden. Alternatively, the words may be understood as synonyms: 'unlawful' may also refer to something that is criminally punishable or violations of statutory law, and 'illegal' may be used to refer to something not authorized by the law or statute.[14] Similarly, the original Finnish wording of CJP, chapter 17, section 25(3) ('*lainvastaisesti hankittua*') might be perceived to leave some room for interpretation. Therefore, *the first question* to resolve is whether 'obtained unlawfully' should be understood to cover only specifically forbidden methods and means of obtaining evidence and violations of specific legal rules, or more broadly to also cover all methods of obtaining evidence that are not based on a clear authorization stated in written law.

The second question relates to the different phases of obtaining evidence. Should unlawfulness be evaluated only in relation to the original evidence collection by a (foreign) LEA, or the obtainment of such evidence by the domestic LEA through a voluntary disclosure or MLA procedure, or both of these phases?

The third question relates to the choice of laws. If the collection of evidence by a foreign LEA is relevant for whether the evidence was obtained lawfully or not, should the unlawfulness of this phase be evaluated in light of the domestic law of the country in which the evidence is used, or in light of the law(s) that apply to the LEA(s) that have performed the investigatory measure? In other words, in the context of ANOM evidence proffered in Finnish courts, does it matter whether the Operation Trojan Shield/Greenlight was lawful according to United States law (or some other foreign law), or is the relevant question whether such an operation would have been allowed under Finnish law?

Similarly, it could be asked whether it is enough for the MLA or information disclosure procedure to conform with the laws of the country receiving the evidence for the evidence to be considered lawfully obtained in

[12] See Europol, Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe, 2 July 2020.

[13] See Europol, New major interventions to block encrypted communications of criminal networks. https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks, 10 March 2021.

[14] See, e.g., Legal Information Institute, Wex. https://www.law.cornell.edu/wex, keywords 'illegal' and 'unlawful'.

this country, or whether the requirement of lawfulness entails that the authorities providing the information fully comply with their own domestic laws concerning the MLA procedure and/or cross-border disclosure of information. In the following, however, procedural issues relating to foreign legislation governing the MLA procedure or other forms of cross-border disclosure are not further addressed. Furthermore, for the sake of simplicity, I do not specifically address the question of selection between (foreign) laws that govern the execution of a cross-border operation by cooperating LEAs, and whether the authorities of one country may, in the first place, under international law conduct operations targeting data and communications stored or transmitted in foreign countries without violating the sovereignty of these countries.

2.2. Against the law or not based on law?

Section 2(3) of the Constitution of Finland (731/1999) states that "[t]he exercise of public powers shall be based on an Act. In all public activity, the law shall be strictly observed." This is particularly relevant for law enforcement activities, as they entail the use of public powers in a manner that very directly interferes with the fundamental and human rights of natural persons. It would be difficult to argue that the police would be constrained only by specific prohibitions and commandments in written law, and that in the absence of specific legal rules LEAs could freely conduct criminal investigations as they see fit and use any methods that are not specifically prohibited. This would not be compatible with the current Finnish and European understanding of *rule of law* exemplified by the aforementioned constitutional provision.

Additionally, communications are protected under section 10 of the Constitution, and limitations of the secrecy of communications may only be imposed by a parliamentary act for purposes specified in this section.[15] On the European level, Article 8 of the ECHR similarly requires any restrictions on the right to respect for private and family life (including communications) to be "in accordance with the law" and limited to specified purposes.[16] Thus, any investigative measures targeting confidential communications that lack a clear basis in a parliamentary act are unconstitutional and constitute a violation of binding international human right obligations. In general, it is clear that if the Finnish police commits an investigatory operation without any basis in the written law, this activity cannot be considered lawful.[17]

Furthermore, in the law drafting documents, it is clarified that unlawfulness in the sense of CJP, chapter 17, section 25(3) is not limited to actions that constitute criminal offences, although these can be considered a particularly serious form of unlawful conduct. The discretionary exclusionary rule also applies to methods of evidence collection that violate norms that are safeguarded by sanctions other than criminal punishment,[18] and

[15] Constitution of Finland, section 10(4) (817/2018): "Limitations of the secrecy of communications may be imposed by an Act if they are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, during deprivation of liberty, and for the purpose of obtaining information on military activities or other such activities that pose a serious threat to national security."

[16] In addition, the restrictions are required to be "necessary in a democratic society".

[17] This was not always the case; earlier, police authorities were understood to have a general mandate to investigate crime. In the area of police work, the newer conception of rule of law has led to many legislative changes. In the last three decades, several new provisions defining new coercive measures and the conditions of their use have been added to the Finnish law in order to comply with this constitutional requirement. Currently, investigatory powers in the context of criminal investigations are defined in the Coercive Measures Act (806/2011), with related provisions also in the Criminal Investigation Act (805/2011) and the Police Act (872/2011), which all entered into effect on 1 January 2014.

[18] Arguably, this might include data protection principles and rules that are subject to administrative fines under Regulation (EU) 2016/679 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). The GDPR and the threat of administrative fines do not apply to the processing of personal data by competent LEAs in the context of criminal investigations. Still, personal data that may be relevant as evidence may also be processed by private parties, and CJP, chapter 17, section 25(3) is *not* limited to evidence obtained unlawfully *by* LEAs, as is further discussed in the following sub-chapter.

even prohibitions and commandments for which the law proscribes no sanctions at all.[19] For public officials, unlawfulness can also mean exceeding their legal mandate. In addition to violations of norms in parliamentary acts, violations of norms stated in international instruments, national decrees and other lower-level statutes, and even case law are included.[20]

In the domestic setting, the answer to the first question is thus relatively clear, at least *prima facie*: unlawfulness is to be understood in a wide sense, and the expression "unlawfully obtained" covers both violations of specific legal rules (with the backing of criminal sanctions or otherwise, and without regard to the nature of legislative instrument in which they are contained) and the lack of appropriate legal basis in a parliamentary act for law enforcement operations. However, the answer becomes blurrier in an international context and when we consider it in connection with the other two questions specified earlier, as we will see next.

2.3. Which phases of evidence collection are relevant?

The wording "evidence that has been obtained unlawfully" does not specify at which point the evidence should be considered "obtained", and who may "obtain" evidence. In the domestic context, it is clear that CJP, chapter 17, section 25(3) does not only concern evidence that has been obtained by the police through unlawful action of law enforcement officers, but also evidence that has been obtained unlawfully by other actors, including private parties (e.g., suspects, victims, witnesses and other third parties). If a private individual obtains a document or an item that is relevant as evidence by committing a criminal offence, and consequently presents this evidence to the court, it should be considered unlawfully obtained. The same holds true when the individual, instead of presenting the evidence directly in court themselves, first willingly hands it over to the police, and subsequently the evidence is presented by the prosecutor in the court.[21]

Following this reasoning, it could be argued that it should not be significant whether the party responsible for the unlawful step in obtaining the evidence is domestic or foreign, or whether the unlawful action has taken place inside or outside the borders of the jurisdiction where the evidence is proffered to the court, or specifically when the evidence was transferred across the border by one LEA to another. Therefore, even if the domestic LEA committed no unlawful action in obtaining the evidence, we should also consider the earlier steps of evidence collection by other actors abroad.

On the other hand, it could be argued that actions outside the national jurisdictional sphere should be treated differently. First, domestic authorities have no jurisdiction to investigate activities that have been carried out abroad by foreign LEAs, and therefore it may be difficult to ascertain the circumstances under which the evidence has been originally collected by a foreign LEA. This may make it difficult to identify illegal activities, and if it was simply presumed that foreign LEAs habitually collect evidence unlawfully, this would present obstacles to efficient cross-border law enforcement cooperation.[22] Second, even if the factual circumstances related to the original collection of evidence are clear, domestic authorities or courts may not be in a good

[19] While even minor procedural violations are not excepted from the scope of the provision and any evidence obtained without full compliance with the law should be considered "unlawfully obtained", the type and seriousness of the unlawful conduct are important factors in the final consideration of whether this unlawfully obtained evidence should be excluded or admitted despite the unlawfulness. In particular, evidence obtained through intentional, serious criminal offences committed by law enforcement officers is likely to be excluded.

[20] Government Proposal HE 46/2014 vp, p. 92–93.

[21] See Government Proposal HE 46/2014 vp, p. 94. According to the proposal, if the unlawful action has been committed by a private individual without the initiative or cooperation of authorities, this can be considered a factor that "to some extent" supports the admissibility of evidence (despite the unlawfulness). The parliamentary Legal Affairs Committee, instead, stated that evidence that has been obtained through a criminal offence committed by a private third party should only be excluded in extremely exceptional cases (Legal Affairs Committee Report LaVM 19/2014 vp, p. 21).

[22] However, if evidence from abroad is admitted with limited information about its origins, the lack of knowledge concerning the technical details of evidence collection may complicate the evaluation of this evidence. This could also be seen as an argument in favor of categorical or strongly presumed inadmissibility of evidence collected by foreign actors. Alternatively, if the prosecution is unable to

position to interpret whether the collection has in fact conformed to the standards and formalities of applicable foreign law. Third, exclusion of evidence that has been obtained through unlawful actions by foreign LEAs would not serve the function of steering the behavior of (domestic) LEAs, and it would be inefficient in deterring similar illegal law enforcement activity in the future.

None of the arguments above, however, decisively mean that CJP, chapter 17, section 25(3) could not be interpreted in accordance with its wording which specifies no explicit limitations on where and by whom the unlawful step in obtaining of evidence has been performed. In any case, domestic courts regularly have to engage in fact-finding concerning events that have taken place abroad and other events that may be difficult to clarify. Whenever certainty cannot be reached, legal rules on the burden and standard of proof come into play. Likewise, the content of foreign law is a question of evidence in the Finnish courts, and the parties can be required to provide information concerning the relevant law.[23] As for the third argument, deterring illegal (police) activity is by no means the only function served by the exclusionary rule, which at least in principle – as has been already mentioned – also applies to evidence obtained through unlawful actions by private parties.[24]

In terms of current law, therefore, there seems to be no compelling reason not to consider all phases of evidence collection regardless of where and by whom they have been carried out. However, the fact that evidence about the content of foreign law can be presented does not resolve the third question. In order to lawfully obtain evidence in the context of cross-border operations, should the activities of foreign LEAs conform to their own national legislation, the legislation of the country where the evidence is to be used, or both?

2.4. Which law is relevant?

In the ANOM case, the sting operation was primarily orchestrated by the FBI without prior initiative or involvement of Finnish authorities, and the server where the intercepted communications were stored was not located in Finland; the data was apparently initially collected to a server in an unknown European state, and then forwarded to the FBI server in the United States on the basis of a request for legal assistance.[25] However, ANOM devices had been distributed to users in different countries, including Finland, and the intercepted messages included communications sent and/or received by people residing in Finland. The data had been analyzed by the FBI, and messages with links to Finland had then been voluntarily handed over to the Finnish authorities at the initiative of the FBI. Later, the Finnish authorities had separately requested permission to use some of this data as evidence under the MLA procedure. The initial disclosure and the subsequent permission requests were based on a bilateral treaty between Finland and the USA, and the legality of these procedures has not been specifically challenged.

In the aforementioned case that is currently pending in the Supreme Court, the prosecution argued that the sting operation had been conducted by the FBI in accordance with United States law. Although the legal complexities of the case are far from clear from the perspective of US law,[26] the dissenting Court of Appeal judge in I-SHO 2022:2 stated that no reason had arisen to doubt that the actions by the FBI had not been in accordance with the legislation applicable to this US agency. However, the majority opinion did not consider

clarify uncertainties about the technical aspects of evidence collection that may influence the reliability of said evidence, this can be factored in when determining the weight and probative value of the evidence according to the free theory of evidence.

23 CJP, chapter 17, section 4(2): "If the law of a foreign state is to be applied to the matter and the court does not know its contents, the court shall exhort the party to present clarification thereon. Separate provisions are laid down on the obligation of the court to obtain clarification on the contents of the law of a foreign state ex officio."

24 Notably, the Legal Affairs Committee specifically rejected the idea that the exclusionary rule would be intended to function as a disciplinary measure to errors and irregularities in public activity. Legal Affairs Committee Report LaVM 19/2014 vp, p. 6.

25 See Cox 2022.

26 See, e.g., Baker/Klehm 2021.

this question,[27] and instead focused on whether the operation, including (and particularly in regard to) the original collection of the evidence by the FBI, had been lawful from a Finnish law perspective.

According to the majority, the ANOM communications in question had taken place in Finland and the messages were without doubt intended as confidential communications protected by section 10 of the Constitution. Therefore, interference with this communication could only be legally performed based on authorization in a parliamentary act. The majority further found that US law could not trump the constitutional protection so that it would allow the messages to be used by Finnish prosecutors in a similar manner as evidence obtained in accordance with Finnish legislation concerning coercive measures. The location of the server where the messages were collected was not considered relevant. Because no provision in a parliamentary act allowed for the FBI to interfere with the confidentiality of communications in Finland, and because it was not even claimed that the Finnish legislation concerning secret methods of gathering intelligence or covert coercive measures in the context of criminal investigations had been followed, the majority considered ANOM evidence originally obtained unlawfully by the FBI. Even though the same evidence had been subsequently obtained without further unlawfulness by the Finnish authorities, CJP, chapter 17, section 25(3) was applicable.

Instead, the dissenting judge noted that Finnish authorities had not requested or cooperated with FBI in collecting the evidence, and that the collection of ANOM messages had been performed abroad, by a foreign LEA, and from a server located outside Finland. Consequently, the dissenting judge found that Finnish law was not applicable despite the fact that some communications of Finnish individuals that had taken place in Finland had been captured along with other messages. In this argumentation, the dissenting judge also noted that ANOM devices had not been generally available in Finland, and that the Finnish users had acquired their devices from abroad.

In short, therefore, the majority in I-SHO 2022:2 considered Finnish law relevant for the original collection, whereas the dissenting judge considered US law relevant for this phase. For the subsequent obtainment of evidence by the Finnish authorities, lawfulness was not considered in much detail, and only in light of the bilateral treaty between Finland and United States; no specific observations regarding national implementations and legislation supporting this treaty in either country were made.

It is worth noting that neither the majority nor the dissenting judge explicitly considered the possible interpretation that the sting operation would have needed to conform simultaneously to *both* Finnish *and* US law for the evidence to be considered lawfully obtained. In this particular case, it was relatively clear that Operation Trojan Shield/Greenlight had not and could not have been legally performed under Finnish law, so it was not necessary for the majority to further investigate the lawfulness of this operation under US law. However, it could be argued that for a cross-border law enforcement operation to be completely lawful, it would need to conform to the legislation of both (or all) countries in which it is performed or in which targeted people reside.

Of course, this interpretation would present obvious practical difficulties in many investigative scenarios typical in the network environment, where it may be difficult or impossible to determine the location of the targeted devices or people in advance. In some cases, simultaneous compliance might even be impossible due to conflicting requirements in different national laws. In general, in a setting where a limited number of target countries can be identified in advance, it might be possibly to satisfy national requirements relating to decision making (such as *ex ante* authorization by a court or other competent authority) and to make sure that there is appropriate legal basis for the operation in each of the national laws of these countries.[28]

---

[27] As is stated in the later published judgment I-SHO 2022:5, the court in I-SHO 2022:2 had been under the impression that the operation had been carried out in accordance with US law. In I-SHO 2022:5, the court admitted that in light of new information concerning the involvement of a third country, this had been an erroneous assessment.

[28] Further alternative interpretations (and/or *de lege ferenda* policy suggestions) can be imagined. For example, as a compromise solution, it could be argued that the operation could/should be considered lawful as long as there is an appropriate legal basis in the laws of the jurisdiction of the (leading) LEA, the procedural requirements of this jurisdiction are followed, and the operation does not

In regard to this issue, the argumentation in HelHO 2022:4 offers an interesting variation from the I-SHO 2022:2 majority opinion. In this unanimous decision, the Court of Appeal of Helsinki stressed the principles of territoriality and respect for national sovereignty. Because all ANOM messages in this case had involved a party located in Finland (although the other, unidentified party may have resided abroad), the court found that the legality of the interception was to be evaluated *solely* in the light of Finnish law–explicitly stating that it was irrelevant whether the FBI had adhered to US law. As neither Finnish parliamentary acts nor binding international treaty obligations[29] provided a basis for the operation, the Helsinki court found that ANOM evidence had been unlawfully obtained by the FBI.

A recent unpublished decision of the Court of Appeal of Eastern Finland of 24 October 2022 further highlights the complexities relating to selection of laws in cross-border situations. In the same way as the dissenting judge in I-SHO 2022:2, the court unanimously found that Finnish law was not applicable to Operation Trojan Shield/Greenlight. However, in this case the court noted the involvement of a third country in assisting the FBI in the interception of ANOM messages,[30] and the fact that this arrangement had apparently been made to circumvent the applicability of US law, as the law of this third country was more permissible. As a consequence, the court found that there was reason to suspect that the operation had not been performed in accordance with US law, and the messages were considered unlawfully obtained because of this. Notably, it was not evaluated whether the operation actually conformed to the laws of the unknown third country.

3. Conclusions

As can be seen, unlawfulness in obtaining evidence is a blurry concept especially in the context of cross-border operations and global networks which form an environment that is in many ways borderless. Based on the discussion above, the reader may wonder whether unlawfulness is a reasonable standard for excluding evidence in criminal proceedings. In my view, the answer to this question is simple: *it is not*. Exclusion of evidence as a sanction for minor infractions, which often have little to do with the fundamental rights of the accused, would regularly lead to disproportional consequences to the interests of the criminal justice system and the rights of crime victims. This would not be well suited for a legal system where evidence law is strongly based on the free theory of evidence and the free discretion of the judge(s) in assessing the probative value of evidence, such as Finland.

However, it is worth reiterating that in Finland, unlawfulness in obtaining evidence is not, as such, grounds for excluding the evidence; it is merely a condition for the applicability of CJP, chapter 17, section 25(3), which leaves the ultimate decision on admissibility to the discretion of the court. The main criterium for exclusion is whether the use of the (unlawfully obtained) evidence would *endanger the conduct of fair proceedings* which, although perhaps somewhat open to interpretation, is a substantive standard linked with fundamental and human rights and a significant body of case law. In I-SHO 2022:2, after considering the open-ended list of factors specifically mentioned in the provision, the majority ultimately found that exclusion was not required to maintain the fairness of the proceedings, and rejected the requests for exclusion. In I-SHO 2022:5, the court again rejected the requests for exclusion despite the new information concerning the involvement of a third country in Operation Trojan Shield/Greenlight. The same conclusion was reached in HelHO 2022:4 and the aforementioned unpublished decision of 24 October 2022. Moreover, the dissenting judge in I-SHO 2022:2, who found the sting operation lawful under US law, considered the possible exclusion of *lawfully* obtained evidence based on a so-called independent exclusionary rule (*selbstständiges Beweisverwertungsverbot*), the

constitute a criminal offence and/or violate substantive standards of protection for fundamental rights provided under the laws of other targeted countries.

29 In addition to Finnish MLA laws, the court considered the bilateral Finland–USA agreement on enhancing cooperation in preventing and combating crime and the Convention on Cybercrime (CETS 185), specifically Article 32.

30 This information had been derived from I-SHO 2022:5, which was issued a few months earlier (in July).

existence of which has not been generally recognized in Finnish law, but suggested in legal literature.[31] Using similar factors as are provided CJP, chapter 17, section 25(3), the dissenting judge did not find grounds for exclusion of ANOM messages, and therefore reached the same final result as the majority.

If evidence that has been obtained unlawfully is not automatically excluded, but instead subjected to additional scrutiny which may or may not lead to exclusion based on further criteria that are intrinsically tied with the fundamental right to fair trial, as is the case of CJP, chapter 17, section 25(3), there is no obvious disadvantage to adopting a wide concept of unlawfulness; it is reasonable to include all forms of unlawfulness (section 2.2) and all phases of evidence collection (section 2.3). The most problematic question, however, is which law is the relevant standard against which the lawfulness of evidence collection should be evaluated (section 2.4).

I do not presume to have a definite *de lege lata* answer for whether the lawfulness of Operation Trojan Shield/Greenlight should be evaluated in light of Finnish law, US law, or both. Yet, there is a further argument to be presented in favor of the interpretations of the majority in I-SHO 2022:2 and the court in HelHO 2022:4: disregarding the laws of the jurisdiction where the targeted individuals or their communications devices are located would provide a strong incentive for *jurisdiction shopping* in cross-border online operations.[32] This would mean that law enforcement operations with global effects could be performed under the least restrictive laws which give no effective protection to the rights of users of global communication networks. As long as the domestic authorities remained passive and only received information without asking the foreign LEA to perform specific investigative measures, any evidence collected by the foreign authority would be considered lawfully obtained, and therefore, by default, admissible without further scrutiny.

As the minority opinion in I-SHO 2022:2 demonstrates, there is an alternative way around this problem: the construct of independent exclusionary rules, which could be used to exclude evidence that has been obtained "lawfully" under foreign law, even in the absence of a specific exclusionary rule provision. In terms of foreseeability, however, considering lawfulness under the domestic law seems more advantageous, and this option also more naturally fits to the national constitutional doctrine on limitations to fundamental rights. Even so, I posit that independent exclusionary rules can function as a safety valve, also in purely domestic situations where the interference with fundamental rights has not been accurately foreseen by the legislator.

From a *de lege ferenda* perspective, the requirement of full compliance with all the national laws in global cross-border investigations, including adherence to the respective procedural requirements of each jurisdiction, is arguably too burdensome. National laws governing law enforcement activities and powers are currently largely disharmonized. If evidence derived from cross-border operations was unusable in most countries due to difficulties in complying with a set of differing national laws, this would likely hinder effective operations in the online environment. To mitigate this risk, attempts can be made to harmonize legislation relating to criminal investigations and to strengthen cooperation through international treaties, but this is no simple task.

A workable compromise between international law enforcement interests and protecting the rights of internet users could relate to the adequate level of substantive standards of protection for fundamental rights. On the national level, it could be decided that evidence derived from online operations by foreign LEAs could be considered lawfully obtained (and admissible) as long as these LEAs comply with their own national legislation and this legislation provides adequate substantive protection and remedies for the rights of the targeted individuals. To fulfill the constitutional requirements, in Finland this kind of a provision would certainly need

[31] The possibility of excluding lawfully obtained evidence in certain situations where the use of this evidence would in itself constitute a particularly serious infringement of a fundamental right, such as privacy rights, has been (among others) suggested by the author of this paper in his doctoral dissertation, which the dissenting judge cited.

[32] Indeed, a certain form of jurisdiction shopping was attempted in Operation Trojan Shield/Greenlight with the help of a third, unknown country. For the purpose of the aforementioned Court of Appeal of Eastern Finland decision of 24 October 2022, this was not entirely successful, as the court regarded the attempt to circumvent US law as a possible violation of US law.

to be placed in a parliamentary act. Even so, it is dubious if it would survive closer constitutional scrutiny relating to the general conditions for limiting fundamental rights, and whether any sort of effective checks and balances or remedies against foreign LEAs could be arranged in practice. Further, without widespread acceptance of this kind of a policy (perhaps through an international convention), the admissibility rules of a single country would do little to facilitate international cross-border operations. In any case, there is certainly a clear need to clarify what can and should be considered lawful and acceptable in the context of law enforcement in the online world.

4. References

Australian Federal Police, AFP-led Operation Ironside smashes organised crime. https://www.afp.gov.au/news-media/media-releases/afp-led-operation-ironside-smashes-organised-crime (accessed 12 November 2022), 8 June 2021.

Baker, Steward/Klehm, Bryce, Legal Tetris and the FBI's ANOM Program. In: Lawfare. https://www.lawfareblog.com/legal-tetris-and-fbis-anom-program (accessed 12 November 2022), 22 July 2021.

BBC News, ANOM: Hundreds arrested in massive global crime sting using messaging app. https://www.bbc.com/news/world-57394831 (accessed 12 November 2022), 8 June 2021.

Cox, Joseph, A European Country Helped the FBI Intercept Anom Messages, But It Wants to Remain Hidden. In: Motherboard. https://www.vice.com/en/article/qjbggq/anom-third-country-europe-european-union-fbi (accessed 12 November 2022), 3 June 2022.

Europol, Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe (accessed 12 November 2022), 2 July 2020.

Europol, New major interventions to block encrypted communications of criminal networks. https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks (accessed 12 November 2022), 10 March 2021.

Europol, 800 criminals arrested in biggest ever law enforcement operation against encrypted communication. https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication (accessed 12 November 2022), 8 June 2021.

Farlow, Harriet/Edwards, Belinda M., Shining a light on 'going dark': A framework to guide the co-design and communication of decryption laws based on the passage of the Telecommunications and Other Legislation (Assistance and Access) Bill 2018, Computer Law & Security Review, Vol. 46, September 2022, 105726.

Finlex, Translations of Finnish acts and degrees. https://www.finlex.fi/en/laki/kaannokset (accessed 12 November 2022).

Government Proposal HE 46/2014 vp [Hallituksen esitys 46/2014 vp eduskunnalle oikeudenkäymiskaaren 17 luvun ja siihen liittyvän todistelua yleisissä tuomioistuimissa koskevan lainsäädännön uudistamiseksi].

Legal Affairs Committee Report LaVM 19/2014 [Lakivaliokunnan mietintö 19/2014 vp].

Legal Information Institute, Wex. https://www.law.cornell.edu/wex (accessed 12 November 2022).

Rajala, Petri, Hyödyntämiskieltopunninta oikeudenmukaisen oikeudenkäynnin valossa [Applying the exclusionary rule in light of fair trial], Master's thesis, University of Helsinki 2022.

United States Department of Justice, FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown. https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive (accessed on 12 November 2022), 8 June 2021.

Yle News, Trojan Shield: Finnish police arrest 100 in international bust. https://yle.fi/news/3-11970996 (accessed 12 November 2022), 8 June 2021.

Yle News, 12 charged in Finland through FBI-led sting operation. https://yle.fi/news/3-12160958 (12 November 2022), 26 October 2021.