EVALUATION OF EVIDENCE IN DARK WEB DRUG CASES: THE APPROACH OF THE FINNISH SUPREME COURT

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; http://bit.ly/2qvkbYk

Keywords: ***Dark Web, Tor, Narcotics, Evidence, Burden of Explanation***

Abstract: *The dark web has become a popular platform for the sale of illegal drugs. Individual cases regularly come to the attention of the criminal justice system when envelopes and parcels containing drugs are intercepted in customs inspections. In such a situation, the main evidence against the alleged buyer consists of the addressee information on the mail item. The addressee may claim to be unaware of someone ordering drugs using their name and address, and evidence relating to the activity on the dark web itself is typically lacking. The Supreme Court of Finland has recently decided two such cases with different outcomes. In this paper, the approach of the Supreme Court is analyzed in an effort to clarify the decisive factors in such cases and to consider the strengths and weaknesses of this approach.*

1. Introduction

There is more to the Internet than meets the eye. The term «deep web» denotes the part of the web that is not indexed by common search engines such as Google and therefore not as easily accessible. The term «dark web» refers to web sites and content that exist on «darknets», parts of the Internet that have been engineered to stay hidden from the public view, utilizing encryption and other techniques that make high levels of anonymity possible.[1] The Tor network[2], based on the anonymization technique known as onion routing[3] and accessible only via specific software, is the most famous example. Online anonymity is necessary for many purposes, but it also provides an infrastructure for crime and illicit activities.[4] In recent years, marketplaces operating on the Tor network and other darknets have become popular venues for the trade of illegal goods and services, including buying and selling illegal narcotics.[5]

The anonymity provided by Tor and similar networks is not absolute. Darknet services have been successfully raided and shut down, and criminals operating them have been identified and prosecuted. However, with the closing of one marketplace, illegal trade typically moves to another one. Successful operations by law

1 See, e.g., Biddle/England/Peinado/Willman, The Darknet and the Future of Content Distribution. In: Feigenbaum (Ed.), Digital Rights Management. ACM CCS-9 Workshop, DRM 2002. Washington, DC, USA, November 18, 2002. Revised Papers, Springer, Berlin/Heidelberg 2003, pp. 155–176; Wood, The Darknet: A Digital Copyright Revolution, Richmond Journal of Law and Technology, Vol. 16, Issue 4, Summer 2010, pp. 16–19; Paselli, Darknet and Payment Fraud. In: Brighi/Palmirani/Sánchez Jordán (Eds.), Informatica giuridica e informatica forense al servizio della società della conoscenza. Scritti in onore di Cesare Maioli, Aracne editrice, Canterano 2018, pp. 315–316.

2 Tor Project. https://www.torproject.org (accessed on 29 October 2019).

3 See Syverson/Goldschlag/Reed, Anonymous Connections and Onion Routing. In: Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 4–7, 1997, pp. 44–54.

4 See, generally, Minárik/Osula, Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law, Computer Law & Security Review, Vol. 32, Issue 1, February 2016, pp. 111–127.

5 Generally about crime trends on the darknet, see, e.g., Europol, Internet Organised Crime Threat Assessment (IOCTA) 2019 and previous annual IOCTA publications.

enforcement have prompted claims that «the golden age of dark web drug markets is over»[6], but the darknet crime problem has not been conclusively solved, and is unlikely to disappear anytime soon.

In addition to cases stemming from raids targeting dark web services, which result in seizure of large amounts of electronic and other evidence,[7] alleged individual buyers have been prosecuted in situations where mail items containing illegal goods have been intercepted by the Customs. In these cases, information about activities on the darknet are difficult to obtain, and there is generally no way to attribute the illegal transactions to identifiable persons through evidence such as IP addresses or other online identifiers. The main evidence consists of the seized mail item itself and its addressee information. The Finnish courts have seen their share of this type of dark web drug cases, and the Supreme Court of Finland has recently issued two judgments, focusing on evaluation of evidence.[8] In the first precedential case, KKO 2018:3, the evidence was not sufficient for a conviction, and the defendant was acquitted. The second precedential case, KKO 2019:2, in which the defendant was convicted, seems to be an attempt by the Supreme Court to further clarify what kind of evidence is required for a conviction in similar cases and to demarcate the borderline of reasonable doubt.

Next, the key facts and evidential scenarios of the two cases are presented. This is followed by an analysis of the reasoning of the Supreme Court in both cases, with the aim of recognizing the decisive factors. Finally, the strengths and weaknesses of the approach adopted by the Supreme Court are evaluated.

2. Facts of the Cases

The first case (KKO 2018:3) concerned a charge of narcotics offence (ch. 50, sec. 1 of the Criminal Code). According to the charge, the defendant had imported 10 grams of amphetamine via mail. The substance had been found in an envelope arriving from Spain inspected at the Finnish Customs at the Helsinki Airport. The addressee information on the envelope consisted of the name and address of the defendant, who denied ordering the item in question or having any knowledge of it. The District Court acquitted the defendant due to insufficient evidence. The prosecutor appealed against the decision, and the Court of Appeal found the defendant guilty, stating that there was no reasonable doubt as to their guilt. The Supreme Court granted the defendant leave to appeal and held an oral hearing in the matter. In its judgment, issued on 16 January 2018, the Supreme Court acquitted the defendant, as their guilt had not been proven beyond reasonable doubt.

The second case (KKO 2019:2) also concerned a charge of narcotics offence. As in the previous case, the charge related to an envelope sent to the defendant, originating from Spain. In this envelope, the Customs had discovered 250 blotter paper tabs containing 25C-NBOMe, an illegal psychedelic drug. The defendant denied ordering the envelope or having any knowledge of it. In contrast to the previous case, the defendant was additionally charged with unlawful use of narcotics (ch. 50, sec. 2(a) of the Criminal Code). This second charge, which the defendant admitted, did not directly relate to the intercepted envelope and concerned different narcotic substances that had been found in the defendant's possession at a later time. (It did, however, play a role in the prosecution's argumentation relating to the first charge, as did the defendant's previous convictions for narcotics-related crime.) The District Court found the defendant guilty on both charges. The defendant appealed against the conviction on the first charge, but the Court of Appeal dismissed the appeal. The Supreme

6 Brandom, The golden age of dark web drug markets is over. In: The Verge. https://www.theverge.com/2019/2/17/18226718/alphabay-takedown-drug-marketplace-federal-arrest (accessed on 23 October 2019), 2019.

7 E.g., the server of the Finnish darknet marketplace Silkkitie was seized in early 2019 in cooperation with foreign authorities. Thanks to the data recovered from the server database, including messages and detailed transaction information, authorities claim to have identified up to 7500 users. See Yle News, Police launch thousands of investigations into suspected crimes on the Finnish Silk Road. https://yle.fi/uutiset/osasto/news/police_launch_thousands_of_investigations_into_suspected_crimes_on_finnish_silk_road/11107617 (accessed on 16 December 2019), 2019.

8 The Supreme Court may alter the decisions of the lower instances both in matters of law and in matters of fact. In recent years, it has granted leave to appeal in numerous cases where the disagreement mainly or solely concerned issues of fact, providing guidance on evaluation of evidence in different types of cases (e.g., various drug-related offences, sexual offences, assault, and homicide).

Court, again, granted leave to appeal and held an oral hearing. In its judgment, issued almost exactly a year after KKO 2018:3 on 15 January 2019, the Supreme Court upheld the verdict of the lower courts.

In both cases, the main evidence supporting the charges consisted of the addressee information on the intercepted envelope. Both envelopes were addressed to the defendants with their respective names and home addresses. The most significant evidence in favor of the defendant was in both cases their own testimony denying any knowledge of the drugs. While it was obvious that the drugs had most likely been ordered via a dark web marketplace to be sent by mail to the buyer, in neither case was there any sort of evidence directly relating to the online transaction, such as messages, server logs, IP addresses or direct payment trails from the buyer to the seller.[9] As a result, the argumentation in these cases largely revolved around typical aspects of dark web narcotics trade, the personal circumstances of the defendants, and the credibility of their testimonies.

3. Reasoning of the Supreme Court

3.1. Addressee Information

In KKO 2018:3, the parties disagreed about the evidentiary value of the addressee information on the envelope. The prosecution considered the addressee information to be sufficient proof of the defendant's guilt unless there was a specific reason to suspect that they had not personally ordered the narcotics. The defendant argued that the addressee information alone could not be considered proof of them having imported the drugs via mail.[10] The Court stated that it can be considered very probable that the addressee of the mail item is in fact the person responsible for making the order. Therefore, the addressee information in itself is strong evidence supporting the guilt of the defendant. However, in the Court's view, this kind of evidence, based on prior probabilities, is not by itself enough to prove that the addressee has imported illegal substances or goods. The prosecution needs to be able to show further circumstances supporting the guilt of the defendant in order to satisfy the standard of proof.[11] This was restated in KKO 2019:2 with a reference to the previous judgment.[12]

The significance of the defendant's living circumstances and mail delivery practices were considered in both cases. The defendant in KKO 2018:3 lived by themselves in an apartment building. Mail was delivered directly inside the apartment through a mail slot in the door. The defendant had been living in the same apartment for 10 years, and only one other person (the defendant's brother) possessed a key. The Court found the addressee information and the information concerning these conditions to be strong evidence that give a reason to require the defendant to «substantiate the grounds for their denial [of the charge]» and to «tell [the court] about the circumstances relating to the mail item».[13] In other words, the Court established that in these circumstances the addressee information is sufficiently strong evidence that calls for an explanation by the defendant, despite their right to remain silent—even if the burden of proof cannot be shifted from the prosecution to the defense.[14]

---

9 In KKO 2019:2, a bank account inquiry did provide information about the use of virtual currencies. See section 3.3.

10 KKO 2018:3, paras 8–9.

11 KKO 2018:3, para 14. The standard of proof in criminal cases is defined in the Code of Judicial Procedure, ch. 17, sec. 3, subsec. 2: «A judgment of guilty may be made only on the condition that there is no reasonable doubt regarding the guilt of the defendant.» This essentially corresponds to the Anglo-American «beyond reasonable doubt» standard.

12 KKO 2019:2, para 9.

13 KKO 2018:3, para 16.

14 This kind of call for an explanation, or «burden of explanation», has been accepted, under specific circumstances, in ECtHR case law. See, e.g., Murray v. United Kingdom (8 February 1996), Condron v. United Kingdom (2 May 2000), Averill v. United Kingdom (6 June 2000), Beckles v. United Kingdom (8 October 2002) and more recently, the decision in Zschüschen v. Belgium (2 May 2017). Cf. Telfner v. Austria (20 March 2001) and Krumpholz v. Austria (18 March 2010), in which the circumstances did not call for an explanation by the defendant, as the prosecution had not been able to establish a convincing prima facie case (the cases concerned traffic offences, and the defendants denied having been the driver of the vehicle at the time). In Finland, the attitude towards any kind of requirement of explanation has traditionally been very reserved or outright negative.

In KKO 2019:2, the defendant also lived in an apartment where mail was delivered through a mail slot in the door, but they had moved into this apartment in the beginning of September 2015, only a short time before the envelope had been sent and subsequently intercepted on 14 September 2015. Furthermore, disclosure of the defendant's personal information from the population registration system, including his home municipality and address, had been restricted for security reasons. The defendant had, however, waived this restriction on 4 September 2015. The Court, again, found the addressee information and the information concerning the defendant's living conditions to be strong evidence that necessitate the defendant to substantiate the grounds for the denial, i.e., call for some sort of an explanation. In the Court's view, the recent move to a new apartment and the restriction on disclosure of personal information, although the latter had been cancelled shortly before the envelope had been sent, further diminished the probability of someone else having had knowledge of the defendant's new address and having been able to use it when ordering drugs in early September 2015.[15]

3.2. Credibility of the Defendants' Testimonies

The defendant in KKO 2018:3 told the Court that they had not ordered any mail item from Spain, and they had not given their personal information to anyone in order to receive a delivery on someone else's behalf. The defendant claimed to have no knowledge at all of the mail item. They further testified about disagreements with a certain person who owed money to the defendant. The defendant also admitted to having browsed the Tor network out of curiosity at a friend's place, and—from early on and out of their own initiative—to having used narcotics (cannabis products) in the past.[16] The Supreme Court noted that the defendant's testimony had undergone minor changes during the course of the proceedings, and the defendant's testimony in the Supreme Court had not been particularly elaborate or detailed. On the other hand, the changes in the story had concerned minor details and they did not hint at the testimony being generally untruthful. Further, the defendant had mentioned things that were both helpful and harmful to themselves, which the Court saw as boosting the credibility of their story. No circumstances *undermining* the credibility of the testimony had emerged.[17]

Similarly, the defendant in KKO 2019:2 denied ordering the mail item containing 25C-NBOMe or having ever had anything to do with this particular type of drugs. This time, however, the Supreme Court saw the defendant's testimony in a different light. As in the previous case, the Court noted that the defendant had given mostly short answers to questions presented to them, and the testimony had not been detailed. The defendant had not been specific about certain key aspect of their story, and they had also added some elements to the story during the course of the proceedings. In direct contrast to what the Court concluded in KKO 2018:3, in KKO 2019:2 the Court stated that the defendant's story and the way in which they told it had not brought up any circumstances that would *support* the credibility of the story, and the story received no support from other evidence.[18]

[15] KKO 2019:2, paras 11–12. The prosecution further argued that the defendant had purposefully waived the restriction in order to have the possibility of attributing the illegal activity to an external person in case the delivery was intercepted. The Supreme Court rejected this argument and accepted the defendant's explanation for the reason behind this action: to be able to receive the payday loan with which they had acquired virtual currency (paras 16, 29). The same virtual currency was, ultimately, found to have been used for paying for the drugs. See section 3.3.

[16] KKO 2018:3, para 17.

[17] KKO 2018:3, paras 18–19.

[18] KKO 2019:2, paras 15, 17–18.

3.3. Virtual Currencies

In the first case, while investigative measures including a search of the defendant's home and an inquiry relating to the defendant's bank account had been performed, virtually no supporting or circumstantial evidence had been found.[19] In the second case, a bank account inquiry had revealed several transactions between the defendant and a company involved in the trade of virtual currencies. One transaction from the defendant to the company had taken place three days prior to the date when the envelope containing 25C-NBOMe tabs had been sent from Spain (10 September 2019). This transaction was of 160 €, just enough to pay for the particular quantity of drugs that had been ordered using the defendant's name and address.[20]

The defendant's explanation for purchasing the virtual currency tied in with their story that they owed some people money from previous drug deals, which the defendant suggested was the motivation behind someone using their name and address to order the narcotics. The defendant claimed to have purchased the virtual currency in order to put money out of their debtors' reach.[21] Later, the defendant presented an additional reason: having virtual currency was more profitable than keeping the money in the bank. This «investment» argument was undermined by the type and amount of bank account transactions between the defendant and the virtual currency agent. The defendant could not present any detailed information about transactions in virtual currency, as this had been allegedly lost when they had switched their old mobile phone to a new one.[22]

The Supreme Court stated it to be general knowledge that virtual currencies are used to procure narcotics via the Internet, also noting that virtual currencies are used for other purposes and that the use of virtual currencies in itself cannot be taken as proof of the person in question having committed any crimes. In this case, the Court found that the use of a virtual currency did function as evidence supporting the charge due to the temporal connection and the linkage between the amount of the transaction and the value of the drugs in the envelope.[23]

3.4. Involvement with Illegal Drugs

In both cases, the defendant had been previously involved with narcotics. The defendant in KKO 2018:3 had volunteered information about their past drug use, but they did not have convictions that would have been considered in the judgment. The defendant in KKO 2019:2 not only had prior convictions, but several types of illegal drugs were found in their possession three months after the 25C-NBOMe envelope was intercepted (the second charge). Debts relating to prior involvement with drugs were a major part of the alternative hypothesis put forward by the defense, and an alleged reason for the purchase of the virtual currency.

The Supreme Court considered the value of the defendant's prior convictions in a cautious and lengthy manner (a total of 8 paragraphs). The starting point, established in the case law of the Supreme Court, is that the defendant's prior convictions generally play no role in considering whether the defendant is guilty of the current charge. However, when criminal acts of which the defendant has already been convicted share a modus operandi or other common traits with the current charge, these prior convictions can have an effect on the evaluation of evidence.[24] A clear connection between the crimes, based on rules of experience, is needed, and this connection may either support or contradict the current charge.[25]

---

19 KKO 2018:3, para 22.

20 KKO 2019:2, para 13.

21 Allegedly, the debtors had gained possession of the defendant's bank credentials—a claim which was not supported by the transactions on the defendant's account.

22 KKO 2019:2, paras 16, 18.

23 KKO 2019:2, para 14.

24 KKO 2019:2, para 22, citing precedents KKO 2017:12, para 12 and KKO 2017:93, para 11, which also concern drug-related crimes.

25 KKO 2019:2, para 23.

The Court noted that the exact evidential effect of prior convictions depends on several factors. In mail order drug cases, if the prior convictions show that the defendant has previously used the same substance as has been ordered, this may render the current charge more likely in comparison to a situation where the defendant has no previous involvement with narcotic substances. However, prolonged use of drugs may also indicate that the defendant has connections to people who may have an interest to order narcotic substances using someone else's personal information. This would render also the alternative hypothesis more probable. Consequently, the Court called for special care and cautiousness in evaluating the effect of previous convictions. In the present case, the charge concerned a psychedelic drug known as 25C-NBOMe. The defendant's previous convictions, from 2014, concerned ecstasy and amphetamine, and they had no prior involvement with neither this particular drug nor LSD (a similar psychedelic drug). On the other hand, the size of the intercepted batch (250 tabs) made it likely that the drugs were intended for redistribution, not only personal use, and a prior conviction concerned distribution. Further, several types of drugs in different forms were found in the defendant's possession three months after the envelope had been intercepted, which indicated that the criminal act relating to the second charge was probably not a one-time occurrence, as the defendant asserted.[26]

In summary, the Court noted that the circumstances relating to the defendant's prior and later involvement with drugs did not have evidentiary value in the present matter when each was considered in isolation. Considering the relations between the different criminal acts in both temporal and factual terms, taken together with each other, these circumstances could be seen as supporting the charge, but only to a small extent.[27]

3.5. Alternative Hypotheses and Conclusions of the Supreme Court

In both cases, the Supreme Court considered whether someone else might have ordered the narcotics using the defendants' names and home addresses. In KKO 2018:3, the Court stated that the most noteworthy alternative course of events was that someone else had ordered the drugs using the defendant's name and address with the intention of gaining possession of the mail item. This hypothesis was rendered more likely because, as noted by the prosecution, a guide had been published in the Tor network, advising people interested in ordering illegal narcotics to use other people's addresses to avoid being caught. The Court further noted that it could not rule out the possibility of someone having used the defendant's name and address in an attempt to cause them nuisance or to seek revenge against them, but the low probability of the mail item being intercepted needed to be considered when evaluating the likelihood of this hypothesis.[28] In this case, the defendant's mail was delivered directly inside the apartment, which would have rendered it difficult for an external person to gain possession of the drugs (the external person would have needed to either gain possession before the envelope was delivered—by confronting the mailman—or have a key or be otherwise able access the inside of the apartment). In relation to the second alternative hypothesis, the defendant was unable to single out any specific events that would have hinted at someone having the motive to harm the defendant. These facts diminished the likelihood of alternative hypotheses and thus, according to the Court, supported the charge.[29]

In KKO 2019:2, the defendant mentioned having drug-related debts and stated a suspicion that someone might have ordered the drugs in an attempt to cause the defendant nuisance or to seek revenge against them. No debtor or any other person had been in contact with the defendant in regard to the drugs in the envelope. The Court did not see the defendant's testimony as supporting the alternative hypothesis of an external person

[26] KKO 2019:2, paras 21, 24–26.

[27] KKO 2019:2, para 27.

[28] Cf. KKO 2019:2, para 28. In this case, the prosecutor had presented a similar line of argument, further arguing that blotter paper tabs were very unlikely to be discovered in customs inspections, which rendered the possibility of a harm/revenge motive even more unlikely. The Supreme Court rejected this argument, however, because there was no evidence on how the type of drug actually affected the likelihood of it being discovered and intercepted.

[29] KKO 2018:3, paras 20–21.

having ordered the drugs. The defendant had not presented other alternative hypotheses, and no grounds for further hypotheses could be found from the evidence presented in the case.[30]

In both cases, the Supreme Court almost completely rejected the alternative hypotheses. However, this did not prove fatal to the case of the defendant in KKO 2018:3, as the Court did not find enough evidence supporting the charge, despite the significant evidentiary value of the addressee information. The Court referred, in particular, to the lack of evidence produced by investigatory measures that had been performed, the lack of any evidence concerning the use of virtual currencies, and the credibility of the defendant's testimony. In conclusion, the Court noted that the evidence supporting the charge was not sufficient to rule out reasonable doubt concerning the defendant's guilt.[31] In KKO 2019:2, the Supreme Court began its summary by citing the significant evidentiary value of the addressee information, which was increased by the timing of the move and the waiving of the restriction on disclosure of personal information. In addition to this, the charge was supported by the evidence concerning the defendant's use of virtual currencies and, to a small extent, the connections between the charge and the defendant's other crimes. Considering that the relevant alternative hypothesis was not supported by the defendant's testimony or other evidence, the evidence against the defendant was strong and credible as a whole, and no reasonable doubt as to their guilt remained.[32]

4. Evaluation and Conclusions

KKO 2018:3 may seem to set the bar for conviction rather high. Even though alternative hypotheses were found unlikely, the defendant was not convicted. However, this is logical, given that the alternative hypotheses need only be considered in the event that the prosecution is able to provide strong enough evidence in the first place, and addressee information alone can and should not be considered such. Even rejection of alternative hypotheses does not—and should not—increase the evidentiary value of the prosecution's evidence that is not sufficiently strong in itself. The Supreme Court has already earlier made it clear that the consideration of alternative hypotheses is an additional test that is performed if the prosecution is able to provide sufficient evidence.[33] In KKO 2018:3, it was therefore not strictly necessary for the Supreme Court to even consider alternative hypotheses. The reason why this was done may have related to the fact that the Court of Appeal seemed to place a high value on the unlikelihood of anyone ordering valuable narcotics using someone else's name and address without their knowledge, and seemed to view this as a strong presumption that the defendant needed to disprove. Additionally, the Supreme Court may have seen the case as an opportunity to provide guidance on how to evaluate typical alternative explanations, even though they were not crucial for the end result in this particular case.

The latter case can be seen as an attempt to curb excessive interpretations of the first judgment. In KKO 2019:2, the Supreme Court found a case in which the prosecution did have some evidence relating to virtual currencies, the lack of which was noted in KKO 2018:3. The Supreme Court still required something more than just the addressee information from the prosecution, but it did not require anything impossible. In a case where the intercepted batch is large enough for distribution, standard investigative measures such as bank account inquiries may well yield supporting evidence that raises the likelihood of a conviction. In cases concerning small batches of non-dangerous drugs, especially if bank account inquiries prove unfruitful, the investigators should evaluate the effort it would take to gather enough supporting evidence, and consider prioritizing other cases instead of devoting resources to prosecute a minor offence with uncertain results.

30 KKO 2019:2, paras 15, 17, 19.
31 KKO 2018:3, paras 22–23.
32 KKO 2019:2, para 30.
33 See KKO 2013:96, para 6.

In practical terms, the two Supreme Court judgments seem to strike a successful balance. In legal and theoretical terms, the most problematic aspect of the Supreme Court's approach is the notion that the mere presence of the defendant's name and address on the envelope calls for some explanation by the defendant, at least when mail is delivered directly inside the apartment of the addressee. The problem arises from the nature of the offence in question. A hypothetical innocent defendant with no history of crime who knows nothing about the mail item—or even the dark web—cannot tell anything useful to the court. The only thing they could be expected to testify about are the reasons and circumstances relating to their own conduct that might be seen as indicating guilt. In this scenario, there is no such conduct to be explained—there is simply an intercepted mail item that the defendant has never even seen. An innocent defendant cannot be expected to know who might have actually placed the order and for what reason. The addressee does possess knowledge about mail delivery practices, but this information can easily be obtained from other sources besides the defendant, which renders any limitation of the defendant's right to silence needless for this purpose. Any other testimony demanded from an innocent defendant would practically require guesswork about potential enemies and grudge-holders.

The Supreme Court was no doubt aware of the problem: instead of actually using the expression «call for an explanation», they opted for the cryptical «substantiation of the grounds for their denial», the exact meaning of which is unfortunately left somewhat unclear. In the absence of electronic evidence relating to activities in the online environment, both judgments highlight the importance of evaluating the defendant's testimony. Obliging the defendant to speak up—about anything—makes it more likely that there is a testimony to evaluate. The approach reflects reluctance to let silence guarantee acquittal in cases where the prior probability of the defendant's guilt is high but direct evidence is hard to obtain. Yet, it is dubious whether the situation really clearly calls for an explanation by the defendant in the sense accepted by the ECtHR as not breaching the defendant's right to silence.[34] In the author's view, it is undesirable to expand the «burden of explanation» to crimes and cases where the true perpetrator could be virtually anyone and there is no direct evidence linking the defendant to any sort of suspicious activity or conduct.[35]

5. References

Biddle, Peter/England, Paul/Peinado, Marcus/Willman, Bryan, The Darknet and the Future of Content Distribution. In: Feigenbaum, Joan (Ed.), Digital Rights Management. ACM CCS-9 Workshop, DRM 2002, Washington, DC, USA, November 18, 2002. Revised Papers, Springer, Berlin/Heidelberg 2003, pp. 155–176.

Brandom, Russell, The golden age of dark web drug markets is over. In: The Verge. https://www.theverge.com/2019/2/17/18226718/alphabay-takedown-drug-marketplace-federal-arrest (accessed on 23 October 2019), 2019.

Europol, Internet Organised Crime Threat Assessment (IOCTA) 2019. https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf (accessed on 29 October 2019).

Minárik, Tomáš/Osula, Anna-Maria, Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law, Computer Law & Security Review, Vol. 32, Issue 1, February 2016, pp. 111–127.

Paselli, Andrea, Darknet and Payment Fraud. In: Brighi, Raffaella/Palmirani, Monica/Sánchez Jordán, María Elena (Eds.), Informatica giuridica e informatica forense al servizio della società della conoscenza. Scritti in onore di Cesare Maioli, Aracne editrice, Canterano 2018, pp. 315–334.

[34] The prima facie case against the defendant does not seem any more convincing than in the aforementioned ECtHR cases of Telfner and Krumpholz. The «intercepted envelope» scenario shares considerable similarities with traffic offence cases where the suspect is identified merely based on the registration number of the car involved, although the pool of potential perpetrators is typically much narrower in traffic cases.

[35] The «intercepted envelope» scenario also shares traits with cybercrime cases where a suspect is identified through an IP address and subscriber information received from the ISP, but there are also notable differences between these situations. Compared to the addressee, the subscriber of an internet connection service has more information of and control over who may access the internet using the associated IP address, and is in a better position to testify about facts affecting the likelihood of alternative hypotheses. Still, if no additional evidence excluding the possibility of an external perpetrator is presented, the prima facie case is unlikely to be convincing enough to call for an explanation.

Syverson, Paul F./Goldschlag, David M./Reed, Michael G., Anonymous Connections and Onion Routing. In: Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 4–7, 1997, pp. 44–54. https://www.onion-router.net/Publications/SSP-1997.pdf (accessed on 29 October 2019).

Tor Project. https://www.torproject.org/ (accessed on 29 October 2019).

Wood, Jessica, The Darknet: A Digital Copyright Revolution, Richmond Journal of Law and Technology, Vol. 16, Issue 4, Summer 2010. http://jolt.richmond.edu/v16i4/article14.pdf (accessed on 29 October 2019).

Yle News, Police launch thousands of investigations into suspected crimes on the Finnish Silk Road. https://yle.fi/uutiset/osasto/news/police_launch_thousands_of_investigations_into_suspected_crimes_on_finnish_silk_road/11107617 (accessed on 16 December 2019), 2019.