WORK, PREY, LOVE: A CRITICAL ANALYSIS OF ESTONIAN CYBERCRIME CASE LAW 2014-2019

Kristjan Kikerpill, MA
Independent researcher

Keywords: Cybercrime, Case law, Qualitative content analysis, Convention on Cybercrime, Directive 2013/40/EU

ABSTRACT

The current study takes a closer look at the people behind the 'cybercrime' moniker in Estonia. Following a socio-legal research approach, qualitative content analysis and systematic legal interpretation were used to analyse N=42 Estonian court judgements and decisions delivered between 01.01.2014 and 10.08.2019. The results show relative uniformity in crimes involving multiple perpetrators, where the primary distinguishing factor was the level of technical sophistication of the crimes. Crimes committed by individual perpetrators exhibited more variation, ranging from low-tech account takeovers perpetrated by broken-hearted ex-partners to active use of malware and signals jamming. The systematic legal analysis showed that the current system of cybercrime provisions in the Estonian Penal Code is unnecessarily scattered, because the substantive differences between the provisions are insignificant and do not adequately reflect the inherent characteristics of cybercrime. The article thus calls into question whether the legislator has taken the easy road by mechanically adopting international instruments (Council of Europe's Convention on Cybercrime and Directive 2013/40/EU) into domestic criminal law.

INTRODUCTION

Report after report states that cybercrime is growing and diversifying, with account takeovers and various types of fraud still dominating (LexisNexis, 2019). Criminals can even hold entire townships to ransom (Newman 2018; Torbet 2019; Gallagher 2019). However, most crime never crosses the news threshold (Felson and Boba, 2010, pp. 1-4). While cyber-attacks that entail far-reaching consequences to already worried populations have become an inconvenient social reality (European Commission, 2017, p. 7), they are still in the minority compared to run-of-the-mill criminal offences such as fraud (McGuire, 2018). Conventional crime statistics can provide some insights to the general state of affairs, but are rarely entirely reliable in terms of crime-related social reality because the numbers suffer from chronic underreporting (UNODC 2013). In the past decade, criminological research into phishing (Hutchings and Hayes, 2009; Atkins and Huang, 2013; Leukfeldt, 2014), cybercrime criminal groups (Soudjin and Zegers, 2012; Leukfeldt and Jansen, 2015), identity theft (Reyns, 2013) as well as malware victimisation (Bossler and Holt, 2009; Leukfeldt and Yar, 2016) has significantly improved our knowledge about the nature of such crimes and the modus operandi of perpetrators. However, criminological research often analyses 'crime' as merely a generic social phenomenon in a way that does not inform how relevant law functions or would function in various cybercriminal situations. Additionally, only addressing crime from a doctrinal legal research perspective leaves social reality on the side-lines.

Doctrinal legal research primarily uses description and interpretation as its methods whereas little, if any, attention is given to sample formation (van Hoecke, 2011, pp. 1-18). The lack of attention to sample formation is precisely why legal opinions that only employ supportive examples in their line of argumentation run the risk of involving extreme personal (i.e. author) bias on legal matters. Another major limitation of this approach is its inclination towards creating an overly dramatic public perception of criminal events by focussing on high-profile cases (Wall, 2008; Felson and Boba, 2010). Hence, to address and counteract the inherent value-based bias of doctrinal legal research as well as to analyse cybercrime as a specific law-based phenomenon rather than generic social malice, the

current article adopts a socio-legal approach for the study of cybercrime, which is a more recent addition to the body of knowledge (Dizon, 2016; Kikerpill and Siibak, 2019).

To gain an improved understanding about the real people and the real crimes behind the 'cybercrime' moniker from the perspective of applicable criminal law, it is paramount to investigate the one place where social and legal reality always meet - the courtroom, and the resulting case law. Analysis of court and law enforcement documents is common in criminological research (Leukfeldt, 2014; Lavorgna, 2015), but is mostly only used to glean insights about the activities. Therefore, the research design of the current article offers new insights by providing a criminal-law-in-action perspective that analyses both the social and legal reality of cybercrime. Furthermore, exploring the actions of cybercriminals operating in Estonia, which has often been referred to as the most wired country in the world (Reynolds 2016, Heller 2017), would add an interesting layer to the analysis. For example, analysing the case law from Estonia enables me to investigate whether punishable offences in Estonia are committed by innovative technology savants or common people who, among other methods, use computers to commit acts and create consequences that are unpleasant and deemed socially and legally unacceptable. To achieve these goals, the current research takes a closer look at the perpetrators of cybercrimes, their actions as well as the contexts within which such actions were committed as recorded in the indictments and arguments available in Estonian cybercrime case law from 2014-2019.

The article at hand begins by providing a brief overview of the history of cybercrime provisions in Estonian criminal law as well as the methods used in collecting and analysing relevant case law are described in more detail. The third section presents the findings and qualitative analysis, focussing on offences resulting from romantic/personal relationships, including employment-related matters, and predatory crimes. Based on the findings and qualitative analysis, the final section provides a systematic legal interpretation of the chosen provisions with the aim of suggesting future considerations for decluttering the black letter law *vis-à-vis* cybercrime.

1. DATA, METHODS AND THE LAW

Literature on cybercrime related criminal law in Estonia is sparse (Sootak 1997, Hirsnik 2014). Computer-related offences were first established in Estonian criminal law in 1997, when the adoption of the Databases Act introduced special offence descriptions to the Criminal Code based on European Union recommendation R(89)9 of 13 September 1989 (Sootak, 1997). Since the coming into force of the Penal Code (PC) on 1 September 2002 (Penal Code, 2001), offence descriptions for computer-related offences have seen important changes multiple times, namely in redactions that came into force on 24.03.2008 and 01.01.2015. These changes came about with the ratification of the Council of Europe's Convention on Cybercrime (Convention, 2004) and the EU Directive on attacks against information systems (Directive, 2013). In the course of 15 years, the number of registered cybercrimes has remained remarkably low. From 2003 to 2018 (Ministry of Justice, 2019, p. 66), only 181 registered cases of interference with computer data (PC §206: the attacks against data provision; Directive Art 5, Convention Art 4), 78 cases of illegal interference with computer systems (PC §207: the disruption provision; Directive Art 4, Convention Art 5), 91 cases of preparation of a computer-related offence (PC §216[1]: the preparation provision; Directive Art 7, Convention Art 6) and 513 cases where access to a computer system was obtained illegally (PC §217: the illegal access provision; Directive Art 3, Convention Art 2). Nevertheless, recent years (2015-2018) have seen a noticeable uptick in registered cases (Ministry of Justice, 2019, p. 66). While an increased number of registered offences does not guarantee an increase in relevant case law, it provides a reason to take a closer look at currently available decided cases.

The case law data for the present study was collected from the Estonian National Gazette (Riigi Teataja) law database, which also includes a search option for court judgements and decisions. The performed search was limited to judgements and decisions made on or after 01.01.2014 and used the term "KarS §2**", i.e. the official abbreviation of the PC in Estonian, in the "text of the case" ("lahendi tekst") search field as the provision-based search option for the database is non-functioning. This required manually reviewing each potential case for suitability. The

search was repeated four times, one for each provision pertaining to computer-related offences (PC §206, §207, §216[1] or §217). Collected judgements and decisions were further filtered to account for one judgement or decision describing multiple offences. The final sample comprised 42 judgements and decisions, where seven cases mentioned more than one of the four provisions. Detailed analysis of the substantive proximity of the provisions is presented in Section 3.

For each case in the final sample (N=42), the case number, date of the judgement or decision, the description of the act where available, and notes on whether PC §213 was included in the judgement or decision were extracted (See Table 1).

TABLE 1: CASES MARKED WITH 'X?' INCLUDED A DISCUSSION OF THE MARKED PROVISION. (X) marks the corresponding provision of the Penal Code in force after 01.01.2015.

Case no.	Date of judgement or decision	§206	§207	§2161	§217	Did the indictment also include §213 (computer-related fraud)?
1-13-7311	09.06.14			X		X
1-14-1081	05.02.14			X		
1-14-3029	31.03.15				X?	
1-14-3276	22.04.14			X		
1-14-3919	28.05.14			X		
1-14-4596	10.06.14			X		X
1-14-5312	04.07.14		X			
1-14-6295	24.09.14			X		X
1-14-6731	14.08.14			X		X
1-14-7403	19.09.14			X		
1-14-9398	19.11.14			X		
1-15-157	29.01.15				X	
1-15-2520	31.03.15			X		
1-15-2640	20.06.17			X		X
1-15-4923	02.09.15			X		
1-15-509	15.04.16		X			
1-15-7057	01.09.15				X	
1-15-8676	09.11.15	X			X	
1-15-8782	02.12.15				X	

TABLE 1: CONTINUED

1-16-11609	14.02.17	X				
1-16-3392	18.05.16	X			X	
1-16-4479	28.02.17	X				
1-16-4515	14.06.16				X	
1-16-636	07.03.16	X			(X)	
1-17-10795	30.11.17		X			
1-17-5454	13.07.17			X		
1-17-6114	21.07.17		X		X	
1-17-8208	25.09.17		X	X	X	
1-18-1220	21.03.18			X		
1-18-3022	08.11.18	X				
1-18-3767	08.10.18			X		X
1-18-6408	30.11.18			X		
1-18-7073	26.09.18			X		X
1-18-827	08.02.18	X				
1-18-830	19.02.18	X				X
1-18-9335	19.12.18			X		
1-19-1662	03.04.19				X	X
1-19-1669	13.03.19			X		
1-19-2202	11.04.19	X			X	
1-19-3674	20.05.19			X		X
3-1-1-93-15	20.11.15				X?	
3-1-1-94-14	22.06.15	(X)	(X)		(X)	

Qualitative content analysis (Kuckartz, 2019) was performed on the extracted action descriptions. Firstly, it was noted whether the case involved only one perpetrator or multiple ones, establishing categories "individual perpetrator" and "multiple perpetrators". The second round of coding noted the specific acts the perpetrators had committed, e.g. "*inserted another person's password"* or "*changed the content of the website*". From this, two categories emerged, namely "technically advanced" and "technically simple" acts. Further, the indictments and lines of argumentation were analysed to establish the context within which the perpetrator(s) committed their acts. Two main context categories that emerged were "personal" and "property-related". Under the

"personal" category, two sub-categories could be distinguished, namely "romantic relationship" and "work-related" sub-categories. Regarding the "property-related" category, it must be clarified that pursuant to the PC, all computer-related offences are legally categorised as offences against property. However, there is a contextual difference between cases where another person's password is entered to gain access to their email account with the purpose of reading their messages or when a password is entered to gain access to someone's online bank account. This distinction prompted another categorisation of the acts according to the purpose with which these were committed. The resulting categories of purpose were "to obtain illicit gains" and "to disrupt or destroy". The results of the qualitative content analysis based on the aforementioned categories, including any relevant overlapping and co-occurrence, is presented in the following section.

2. FINDINGS

The presentation of the results follows from the first round of coding, i.e. separating committed offences based on whether one or multiple perpetrators were involved. The analysis begins with offences involving multiple perpetrators due to the relative uniformity present in these cases. Case law pertaining to offences that only involved one perpetrator had more variation in terms of acts, intent and context. For the purposes of analytical clarity, the individual perpetrator sub-section presents findings based on the context within which the crimes were committed, i.e. "work-related", "romantic relationships" and "other predatory offences".

2.1 MULTIPLE PERPETRATORS

The main distinguishing factor between cases involving multiple perpetrators was whether the committed crimes were technically advanced or not. The largest single stream of similar cases involved the placement and use of "skimmers". Skimmers are devices affixed to ATM machines with the purpose of secretly obtaining debit and credit card information from the card's magnetic strip when people use the ATM. More recently, the use of a specific type of skimmer called a "shimmer" has been witnessed. Shimmers are referred to as such, because it acts as a shim that sits between the chip on the card and the chip reader in the ATM (Krebs, 2015). This difference is significant due to the type of payment cards used in various parts of the world. Europe has been using payment cards with integrated chips a lot longer than in the United States. Although the chip itself cannot be copied, the information from the magnetic stripe remains available for the perpetrators (MacDonald, 2017). Hence, that information can still be used to create payment cards for illegal use where the cards are only 'swiped' for verification. In the sample cases, the typical offence involving the placement and use of skimmers had two perpetrators working in tandem, placing the skimmers onto ATMs along with cameras to record legitimate users entering their PIN-codes. Analysis of the cases revealed that perpetrators were detained at various stages of committing the offence. While some were detained prior to completing the placement of the skimmer itself (Case 1-14-1081), others had already placed the skimmer, copied the data and used payment cards

created with the stolen information to also withdraw cash (Case 1-14-6731). Nine cases that centred on the use of skimmers were decided in Estonian courts in between 2014-2015 and only one in 2018. This could be indicative of how certain modus operandi are used in waves or trends, i.e. during certain periods of time, one cybercrime or another is trending compared to others. Additionally, the indictments lacked information on whether the perpetrators had created and fashioned the skimmers themselves or obtained them from third parties. The use of skimmers, and hence almost a quarter of the total cases, can be categorised as technically simple. Clients of the bank also reported suspicions about there being something wrong with the ATMs (Case 1-14-3276) and increased police surveillance was enough to catch perpetrators in the act.

My analysis indicates that only a few offences exhibited more sophistication either in terms of technical knowledge or organising the operations of the group. In fact, two significant types of cases were revealed through my analysis. On the one hand there was the Ghost Click case (Hacquebord 2011), i.e. case 3-1-1-94-14, and on the other hand, there were cases where crime groups were laundering money or obtaining large quantities of credit card information and perpetrating computer fraud by purchasing goods or services in online stores (Cases 1-15-2640, 1-15-4923, 1-18-6408, 1-18-9935), i.e. cases with a strong connection to the 'kinetic' in terms of criminal proceeds. In case of the former, advanced technological knowledge was employed, whereas the latter exhibited a very specific distribution of tasks among the members of the group even though the cybercrime itself was not technically sophisticated.

The first, technologically more advanced offence appeared in the Ghost Click case (3-1-1-94-14). Central to the offence was malware called DNS-Changer, which was spread to at least four million computers globally. DNS-Changer allowed the perpetrators to control the victimised computers' DNS settings and re-route users to websites determined by the offenders. Illegal gains were obtained from online marketing and advertising platforms, because users whose systems had been infected with DNS-Changer were re-routed to websites displaying certain advertisements. The Ghost Click operation ran for five years from 2006 to 2011, netting the perpetrators upwards of $22M. Whereas the setup was more complicated in comparison to the other cases in the sample that involved multiple offenders, the most disturbing observation in connection to the

Ghost Click case was a legal one. Ghost Click represents a strand of cybercrimes, or borderline cases, that can be called "licensing crimes". Since people are entitled to authorise third persons to impinge on their (property-related) rights, e.g. it is possible to allow someone else to change settings on one's computer or log in to a social media account, licensing agreements presented to people who download software can be used by criminals to prey on unaware computer users. In the Ghost Click case (3-1-1-94-14), software bundling was used to deliver the DNS-Changer malware. The malware was bundled with a media player or video codec and the accompanying licensing agreement stipulated that installing the software might cause changes in the computer's network settings. This possibility of "licensing crimes" presents a significant problem, because most users either do not read the agreements at all (Bakos, Marotta-Wurgler, and Trossen, 2013; Obar and Oeldorf-Hirsch, 2018) or remain confused about the specific legal implications of such agreements after reading them (Cotton and Bolan, 2011).

The crimes of the second group in case 1-15-2640 (the leader) and 1-15-4923 (other members) were two-fold. The first involved using Western Union (WU) money transfers to send criminal proceeds from Japan to Estonia and elsewhere in Europe to be withdrawn and delivered by money mules (Cases 1-15-2640, 1-15-4923). Additionally, the leader of the group had also obtained credit card information from unknown sources and used this information to make at least 39 illegal purchases in various online stores. The obtained goods were often bought in the name of other group members and then retrieved from post offices. Similar methods were used in cases 1-18-9335 and 1-18-6408, where criminal proceeds from computer-related fraud committed in Germany were used to purchase goods, repackage them and then ship the goods to Estonia to be retrieved by the perpetrators. According to the indictment, the illegally purchased goods were so numerous that some were even stored in the home of a grandmother of one perpetrators' grandmothers (Case 1-18-9335).

In general, offences including multiple perpetrators were geared towards obtaining illicit gains. The distinguishing factors between different ways of committing the offences came down to technological and organisational, including legal, sophistication of the operations.

2.2. AN INDIVIDUAL PERPETRATOR

Offences involving multiple perpetrators were solely geared towards preying on unaware victims, i.e. 'crime had to pay' for it to be undertaken. In contrast, the variation of motives and approaches contained in cases involving an individual perpetrator was significant. Hence, the analysis will follow from the context within which the offences were committed. The categories established were "property-related" and "personal", whereas the latter further divided into "work-related" and "romantic relationships".

2.2.1 Work-related

The second noticeable context where offending occurred pertained to work-related situations, which occurred four times in the sample. For example, in Case 1-18-3022, an accountant who had been using a company provided laptop computer for work-related activities maliciously deleted data and materials required by the company to fulfil certain legal obligations. The materials included documents collected in preparation for an audit, different payment schedules and offers related to the company's clients as well as lease agreement documents. In Case 1-16-4479, an IT contractor providing services to a company had illegally and remotely accessed the computer of his contract partner and taken screenshots of Skype conversations, which the perpetrator later emailed to the company's representative. Although this unauthorised access and data collection was the reason for the offender's conviction, it was not the only disruption caused. Contracting IT services puts the maintenance and administration of certain aspects vital to a company's operations in the hands of third persons. In case these work relationships sour, it is easy for a person with advanced technical knowledge to block access to certain important content and administration tools by changing passwords that allow access. While the perpetrator was acquitted of these offences, the mistake made by the IT contractor was the decision to email the work partner screenshots, audio and video of Skype calls, thus incriminating himself. Similar actions were noticeable in Case 1-16-636, where important evidence for the conviction was also available because the perpetrator went 'one step too far' either due to a lack of self-control or being seemingly oblivious to the possibility of actual prosecution.

Another outstanding work-related case in the sample was Case 1-15-509, where 14 accounts at a public agency were temporarily blocked due to incorrect passwords being entered multiple times. To commit the offence, the perpetrator must have had specific knowledge about accessing the information system in question. The offender had masked their IP by using the Tor network and although circumstantial evidence pointed to a specific former employee, the accused was acquitted because the prosecution failed to properly attribute the attacks. The former employee in question had previously worked for the public agency, had been confrontational with many other employees in the past and supposedly had revenge as the motive for perpetrating the attack. The technical investigation in the case relied heavily on the technical knowledge of the witness from the public agency, who presented necessary system logs and other relevant information. However, the case ultimately fell through due to minute inconsistencies between the times of the attacks and the times when the alleged perpetrator had opened a connection to the Tor network. Hence, publicly available technical tools are often enough to avoid being convicted even if most circumstantial evidence point to a specific perpetrator. Work-related offences showed both disruption and destruction as the purpose for committing punishable acts. Ex-employees who either did not possess advanced technical knowledge or were oblivious to the possibility of prosecution behaved in a way similar to the "romantic relationship" offenders, i.e. they did not try to hide their actions by technological means or even incriminated themselves by submitting materials to the victim that turned out to be crucial for the subsequent conviction.

2.2.2 Romantic relationships

Squabbles of ex-partners and people seeking "romance" also formed a considerable portion of the sample cases. In Case 1-15-8676, the case was dismissed due to a lack of public interest and negligible guilt. The perpetrator had logged into the victim's e-mail account and Facebook account to read messages contained therein. The request to dismiss the case was based on the fact that the entire situation was a family matter and the accused regrets committing the acts. Another 'tongue in cheek' type of romantic pursuit was discussed in Case 1-19-1662. The perpetrator had illegally obtained access to numerous companies' WiFi routers to use the

SIM-card of the router to connect to special tariff numbers. The numbers to be contacted were related to parking services and websites containing adult content. In Case 1-16-3392, the perpetrator had obtained and used the Gmail password of his ex-partner to access the account. Following that, the offender requested password changes and tied these account recovery requests to an account inaccessible for the ex-partner. Again, the Facebook account of the victim was compromised in the process. Similar acts were perpetrated in Case 1-16-4515, where the perpetrator also took pictures of the other persons conversations. Compromising an ex-partners email and/or social media accounts was a general method of gaining access to information the perpetrator had no longer any reason to be aware of. The most significant case related to ex-lovers was 1-16-636. Here, the perpetrator had not simply obtained the ex-partners passwords to specific accounts but had placed a remote access backdoor on the victim's computer. The software used to perpetrate later offences was EasyBits Kids – a piece of software that is targeted to parents who wish to remotely control their child's online activities and computer use. The perpetrator was not satisfied with merely knowing what the ex-partner was communicating. In addition to reading the messages exchanged between the ex-partner and third persons, the perpetrator verbally abused the ex-partner via text messages, both taunting the victim by admitting to 'hacking the accounts' and making lude comments about the ex-partner's choice of new potential partners. With the exception of the outlier router SIM-card case that can be considered personal by proxy due to the nature of services purchased, all court cases dealing with acts arising from real romantic relationships had disruption as their main purpose for committing the offence. However, the disruption only concerned negatively impacting one person, i.e. the ex-partner.

2.2.3 Other predatory offences

Aside from the "personal" category of offences, "property-related" crimes committed by individual perpetrators varied significantly with no one shared aspect connecting the different acts. For example, in Case 1-17-10795, the accused who was 70 years old at the time of sentencing had used a signal amplifying antenna, his laptop and special software to jam the central device of a radio alarm system. His actions caused significant proprietary damage to the security company and the indictment showed

no specific motivation on behalf of the accused to commit such an act. In general, blocking relevant signals from reaching the alarm devices could be used to temporarily knock out a modern security system, but the case materials show no such intent from the perpetrator. Other cases involved storing and using malware (Case 1-17-6114), storing malware and illegally obtained credit card information on one's computer (Case 1-19-1669) or storing and using illegally obtained credit card information (Case 1-19-3674). While offences that involved an individual perpetrator but did not fit under the "personal" category seemingly have no 'red line' connecting them, these are all opportunistic predatory crimes that have disruption, destruction or proprietary gain as their purpose. Overall, these acts were of a higher technical sophistication than those under the "romantic relationship" category, as the latter are characterised by visceral reactions more so than detailed and poised conduct, i.e. offences in the "romantic relationship" category were perpetrated by any means necessary as long as a certain goal was achieved.

3. LEGAL ANALYSIS

On one hand, the primary problem surrounding cybercrime offences listed in the Estonian PC is simple: many different offence descriptions with identical maximum sentences and minimal differences in their constitutive elements. Yet, this problem is simultaneously difficult to overcome, because the provisions have already been amended multiple times, including important substantive changes in offence descriptions. This legislative indecisiveness was highlighted in Supreme Court ruling 3-1-1-94-14 (p. 175). The court had to admit that the perpetrators would have skated scot free according to an earlier version of a provision, but not according to a later wording – before 24.03.2008, the perpetrators would have had to cause significant damage in order to be prosecuted pursuant to PC §206.

While the precise reason for such legislative ambiguity over the years is not clear, a closer look at the system of provisions in the PC itself provides some insight. In their current form, the four provisions for which case law data was collected have all been incorporated into the PC due to international obligations, derived from a combination of the Council of Europe's Convention on Cybercrime (ETS No. 185) and the EU Directive on attacks against information systems. However, seemingly little thought has gone into establishing provisions that provide adequate legal protection, can withstand the rapidly changing nature of cybercrime and are more readily comprehensible to the professionals applying them, given that these professionals do not necessarily possess specialist technical knowledge. In the following section, all four main provisions and §213 are analysed in turn, ending with §206 that could potentially become the central cybercrime provision if properly modified.

3.1 PC §207 (THE 'DENIAL OF SERVICE' PROVISION; DIRECTIVE ART 4, CONVENTION ART 5)

For PC §207(1) to be applied, the perpetrator has to illegally interfere with or hinder the functioning of a computer system. Leaving aside the

meaning of 'illegal' and 'computer system', the former of which will be addressed below, the deciding judges need to distinguish between interference and hindering. In 3-1-1-94-14, interference and hindering were interpreted to occur when a computer system is not functioning as intended, with interference being less intensive than hindering. Regardless of whether the system under question is relatively simple or highly complex, the wording of §207 requires a judge, and the prosecutor when preparing the indictment, to assess technical questions. Multiple parameters can be used to determine if a system is functioning 'as intended', including technical and cybersecurity standards as well as specific service level agreements. Among other things, this is a burden on the criminal justice system, because it requires additional technical investigation. The primary problem, however, is that the people preparing indictments and delivering decisions do not possess advanced technical knowledge (Ministry of Justice 2019). The reason for the existence of §206 and §207 is that the former deals with attacks 'against data', the latter with attacks against information systems or computer systems. To clarify, Art 1(a) of the Convention speaks of 'computer systems', while the Directive defines 'information system' in Art 2(a), both meaning the functionality achieved from a combination of hardware and software. Attacks against data comprise unlawful or unauthorised data processing activities and are therefore conceptually easy to distinguish, because the emphasis is on determining what is or is not illegal in each case. The processing activity is illegal if no basis for it exists under law or the person engaging in the activity is not authorised to do so by whomever has the right to provide authorisation. Essentially, §207 is a qualification of §206 for cases where, in addition to illegal data manipulation, the activities also affected the proper functioning of an information or computer system. Given that both offences carry an identical sanction, the purpose of their separate existence remains unclear. Furthermore, there are two conceivable ways in which a person can interfere with or hinder the functioning of a computer system. The first option is to use physical force to render the system unusable. If the damage is significant enough, this action would fall under PC §203. The other option is reflected in §207, where a system's functioning becomes affected through receiving some form of transmission, e.g. transmitting arbitrary data to block channels on the receiving device. This activity was present in Case 1-17-10795, where the perpetrator used his laptop, specific software and a signal amplifying antenna to jam, i.e. block other incoming signals, on

an alarm system's central unit, causing significant proprietary damage. Since cybercrime provisions do not explicitly exclude the use of physical force in disrupting the functioning of information systems, but focus specifically on signal transmissions, then a qualifying provision concerning attacks against information systems that carries a maximum sentence identical to an attack perpetrated against data is entirely unnecessary. The manner of achieving the intended results are identical in PC §206 and §207, always initiated by some form of unauthorised (arbitrary) data transmission.

3.2 PC §216[1] (THE 'PREPARATION PROVISION'; DIRECTIVE ART 7, CONVENTION ART 6)

PC §216[1] is the clearest sign that computer-related offences in the PC ought to be considered as stages in an iterative delict. While this notion is certainly obfuscated by the speed with which commission stages of cybercrimes advance from one legally relevant state to another, the iterative nature of the offences can still be gleaned. In Case 1-17-8208, the accused was convicted of offences under PC §216[1], §217 and §207, although the actions of the accused related solely to changing the content of a single website, i.e. altering the text, images and design of the website. The preparation was not broad, because it pertained to placing a remote backdoor to one administrator system, access was illegally obtained by using that same specific backdoor and the final act was website defacement, i.e. malicious alteration of website content. If the preparation was clearly connected and limited to one specific final act, then the reason for also convicting the person under the 'preparation provision' remains unclear, unless the judge and prosecutor (and the defence) failed to understand that the committed individual acts were stages in an iterative delict. To clarify, two significant sequences of offences that possess an iterative nature in the PC are counterfeiting money and cybercrimes. Perhaps the iterative nature of the wrongdoing is easier to grasp in counterfeiting, where the completed act would render it unnecessary to also convict a person under a provision concerning the preparation for the final offence. Based on the sample, there are two primary ways in which an offence under PC §216[1] is committed: being in the possession of or placing a device necessary for copying credit card information at the ATM

or payment terminal (e.g. Case 1-14-6731) and storing illegally obtained credit card information on a data storage medium (e.g. Case 1-19-3674). Other cases involved the possession of user information, i.e. usernames and passwords (Cases 1-15-8782 and 1-16-3392), or malware (Case 1-19-1669). The wording of PC §216[1] requires the prosecution to prove that the perpetrator possessing the device, program or data had the intention of using it to commit an offence. The explanatory report preceding the current version of offence descriptions in the PC (Explanatory Report 554 SE, 2013) stated that previous wordings of the provisions were too vague and could also allow for the prosecuting of cybersecurity experts who are in the possession of malware due to the nature of their daily work, yet lack the intention of committing an offence. The same can be stated about any devices that can, but do not necessarily have to be, used to commit cybercrimes. While the idea behind PC §216[1] is useful with regard to curbing the commission of cybercrimes in earlier stages, it is dysfunctional in practice. This is precisely because the prosecutor always needs additional proof of intention regarding future crime commission that can, for example, manifest in the form of communication pertaining to planned criminal conduct or apprehending offenders in the process of committing the actual crime. Here, the legislator could consider modifying PC §206, i.e. attacks against data, to also include 'obtaining' into the wording. Skimmers, other similar devices, malware as well as illegally obtained 'means of protection', e.g. passwords or credit card information, are all ultimately used for data manipulation. Data manipulation is expressed in specific data processing related actions, such as those listed in Art 4(2) of the General Data Protection Regulation (Regulation, 2016), including collection, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Following from this comprehensive list, if the perpetrator illegally obtains or intends to obtain data, all of the abovementioned cases are covered and do not require PC §216[1] as a separate provision. In cases where data has been collected already, the modified PC §206 requirements have been fulfilled. In other instances, a case for an attempted attack against data could be presented, if the perpetrators were unable to complete the offence, but had (unsuccessfully) tried to use malware against someone's system or already placed devices such as skimmers without receiving any data.

Although PC §213 (computer-related fraud) was not included in the case law search, it nevertheless was prominent in cases related to PC §216[1] and categorised under acts committed with the aim of obtaining illicit gains. As a *sui generis* derivation from the offence of fraud, i.e. PC §209, the defining characteristic of computer-related fraud is that computers cannot be deceived like humans. There are no other differences between the two offence descriptions, as both prescribe sanctions for causing proprietary damage to another person with the aim of obtaining proprietary benefit from the same act. With the suggested changes to PC §206 and the removal of PC §216[1] altogether, the legislator could consider absorbing PC §213 into the general offence of fraud as the second alternative. For example, the offence of extortion (PC §214) uses a similar construct, employing the alternatives 'threatening to' or 'by use of violence' in explaining how a person must be coerced, or proprietary benefits transferred, to prosecute the conduct as criminal extortion. The illegality of specific acts for which the PC prescribes sanctions would not change, but the law would be decluttered. Furthermore, the nature of fraud has changed in general and, considering Estonian crime statistics (Ministry of Justice, 2019) as well as news regarding major developments in the crime statistics for England and Wales (2018), computer-related fraud is merely a part of the 'new normal'.

3.3 PC §217 (THE 'ILLEGAL ACCESS' PROVISION; DIRECTIVE ART 3, CONVENTION ART 2) AND PC §206 (THE 'ATTACKS AGAINST DATA' PROVISION; DIRECTIVE ART 5, CONVENTION ART 4)

Illegally obtaining access to a computer system by removing or circumventing a protective measure has thus far been considered the 'central' cybercrime provision (Case 3-1-1-94-14, p 186). Obtaining access to a computer system is part and parcel for committing many cybercrimes, but there were numerous cases in the sample which did not require 'using' the system to be successfully perpetrated. To consider something as central would require the phenomenon to manifest in each case and, based on the sample, that is not true for PC §217. For example, jamming signals (e.g. Case 1-17-10795) or committing DDoS attacks do not require access

to the system in order to negatively affect it. Stolen credit card information can be obtained from other perpetrators (e.g. Case 1-18-9335), from anonymous communication via darkweb marketplaces (Case 1-15-2640), but could also be obtained through deceptive acts such as *phishing*, i.e. employing social engineering tactics to convince victims to hand over their data either via email, fake websites or fraudulent links in SMS messages. Furthermore, both 'removal of' and 'circumventing' the means of protection by digital means is already an attack against data. In the cases analysed, removal of a protective measure meant either the unauthorised insertion of a password (e.g. Cases 1-15-8782 and 1-16-3392) or a credit card number (e.g. Cases 1-13-7311 and 1-15-2640). Circumventing a protective measure was achieved by installing a backdoor into the system (Case 1-17-8208). With the former, if passwords or credit card information has been illegally obtained, it is already an attack against data. If the passwords are then used, then the violation is simply more intense, and in case unauthorised credit card use occurs, then we must move on to analysing an attempted or concluded offence of (computer-related) fraud. Unauthorised use of a means of protection can be considered as illegal interference with computer data, because the person either should not have been in possession of it in the first place (i.e. obtaining is illegal) or, knowing it does not belong to him or her, should not have used it. In a technical context, circumventing a protective measure requires some form of unauthorised data transmission to occur, e.g. trying to infect or successfully infecting a system with malware, which means that the act prior to obtaining access was already illegal. This is a major reason why augmenting PC §206 ought to be considered by the legislator. Plenty of questionable actions take place before access to a system is obtained, if obtaining access in the strict sense is necessary at all. By creating a central 'attacks against data' provision, there would be no need for:

- §217: obtaining access is already data manipulation.

- §207: interfering with or hindering the functioning of a computer system affects accessibility to data contained therein and is thus an attack against data in the form of restricting access.

- §216[1]: when unauthorised data collection has occurred, an 'attack against data' has been committed, and attempting to collect data

without a legitimate reason is also an attempted attack against said data.

Although this would not apply to its current wording, the central cybercrime provision in the PC ought to be §206, i.e. attacks against data. Using the comprehensive list of data related actions available from the GDPR would allow flexibility in applying the provision. The key aspects to prove and assess in court would be whether the data related action was illegal or not. This would shift the analysis back towards legal questions and away from complex technical descriptions. According to the current test, illegality of an action can be confirmed if there is no provision allowing it or the action has not been authorised by a person entitled to do so. Since all of the current computer-related offences require intent from the perpetrator, mishaps or human error (negligence) are excluded from viable cases. The perpetrator must have envisioned his or her actions prior to committing them. The proximity of the four provisions mechanically spreads out legally relevant acts that are very closely related if not entirely the same, i.e. all pertain to attacks against data one way or another. The provisions also exclude physical attacks (see section 3.1 about PC §203) and only implement a machine-like distinction between an information system and data. This speaks more to the inadequate amount of thought given to formulating the provisions upon adoption into domestic law rather than a specific legal or social need to make such distinctions. The issue does not stem from the international origin of the provisions, but a lack of domestic assessment regarding the severity of such offences and whether these different punishable acts should carry different maximum sentences. A clear example here is the distinction between §206 and §207. The latter is supposedly a qualification of §206 that ought to carry a heavier sentence, yet both offences carry a maximum sentence of three years imprisonment (Hirsnik, 2014). Since §217, i.e. the illegal access provision, also carries a maximum sentence of three years imprisonment, assessing the way in which the legislator has (or has not) analysed the injustice embedded into these punishable acts is difficult. If the current maximum sentences are retained, then combining §206, §207 and §217 into a single provision is recommended, given the substantive proximity of these provisions.

As shown above with Case 1-17-8208 (Section 3.2) and considering this similarly holds true for cases involving PC §216[1] followed by PC §213 (e.g.

Case 1-19-3674), the courts do not really distinguish between the legal significance of offences that correspond to the preparation provision followed by a delict damaging someone's rights. The preparation provision ought to be evoked only when there is no further damage caused (Sootak and Pikamäe, 2015, §216[1]). It is the same for both computer-related fraud perpetrated with the use of stolen credit card information and skimmer cases. Once the perpetrator(s) commence(s) actions that can be considered as corresponding to fraud, or any other computer-related offence, the preparation provision should no longer be used, and an attempt of the damaging offence should be analysed instead. Furthermore, the application of PC §216[1] in its current form is limited, because it cannot be used in cases involving *phishing* where the perpetrators are not after credit card information or passwords. However, these instances can be equally damaging, for example when people disclose personal information or facts to offenders who have no legal basis for requesting such information.

The current cybercrime provisions in the PC are used rarely, and in more complicated cases, their application relies heavily on witnesses who possess advanced technological knowledge.

CONCLUSION

The study was undertaken to obtain a better understanding of the Estonian cybercriminal in action based on court judgements and decisions available from 2014-2019. Although the sample of cases was small (N=42), interesting patterns were gleaned from the judgements and decisions analysed.

For the most part, crimes involving multiple offenders were distinguishable solely based on the level of technological and organisational sophistication employed, since all such crimes were motivated by proprietary gains. In contrast, individual perpetrators varied significantly in terms of crime contexts and motivations for the offences. When the offences involved ex-partners of a past romantic relationship, the perpetrators used any means necessary to covertly observe the actions and communications of their ex-partner. Individual perpetrators committing offences determined as "personal" also showed a tendency for self-incrimination by taunting the victim or forwarding them materials that were later used as permissible evidence. Predatory crimes outside the "personal" category were opportunistic and varied significantly in technological sophistication. Such offences also had no shared aspect in terms of the underlying motivation for committing the crimes.

Convictions in many of the cases, e.g. the use of skimmers, stemmed from the possibility of observing the perpetrators in action or even receiving relevant hints from regular people. In at least two cases, convictions were possible because the perpetrators had communicated materials to the victims that could later be used as evidence in court. More complicated cases seemed to rely heavily on evidence provided by other law enforcement agencies or witnesses who possessed advanced technical knowledge.

The findings of the above socio-legal analysis indicate that in terms of substantive criminal law in Estonia, the current system of provisions analysed in the article includes offences that are substantively very closely related and is thus more a result of machine-like adoption of international instruments rather than following from the thoroughly

analysed essence of cybercrimes. Whether related to romantic relationships, work or illegally obtaining proprietary gains, the perpetration of 'true cybercrime' is really only focussed on causing real-world impact through data manipulation and thus the legal provisions enacted to protect against these infractions ought to reflect the notion properly and clearly. The current mechanical distinction between offence descriptions that are indeed very closely related in terms of substance is entirely unnecessary, which can primarily be gleaned from such a small number of cases for each separate provision as well as the fact that the provisions often appear together in the indictments.

Contact:

Kristjan Kikerpill
E-mail: kristjan.kikerpill@gmail.com

REFERENCES AND SOURCES

Atkins, B. and Huang, W. (2013) 'A Study of Social Engineering in Online Frauds', *Open Journal of Social Sciences*, 1(3).

Bakos, Y., Marotta-Wurgler, F., and Trossen, D. R. (2014) 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts', *New York University Law and Economics Working Papers*, 195.

Bossler, A. M., and Holt, T. J. (2009) 'On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory', *International Journal of Cyber Criminology*, 3(1).

Case 1-13-7311, 09 June 2014.

Case 1-14-1081, 05 February 2014.

Case 1-14-3726, 22 April 2014.

Case 1-14-6731, 14 August 2014.

Case 1-15-2640, 20 June 2017.

Case 1-15-4923, 02 September 2015.

Case 1-15-509, 15 April 2016.

Case 1-15-8676, 09 November 2015 (decision).

Case 1-15-8782, 02 December 2015.

Case 1-16-3392, 18 May 2016.

Case 1-16-4479, 28 February 2017.

Case 1-16-4515, 14 June 2016.

Case 1-16-636, 07 March 2016.

Case 1-17-10795, 30 November 2017.

Case 1-17-6114, 21 July 2017.

Case 1-17-8208, 25 September 2017.

Case 1-18-3022, 08 November 2018.

Case 1-18-6408, 30 November 2018.

Case 1-18-9935, 19 December 2018.

Case 1-19-1662, 03 April 2019.

Case 1-19-1669, 13 March 2019.

Case 1-19-3674, 20 May 2019.

Case 3-1-1-94-14, 22 June 2015. Supreme Court of Estonia (Criminal Chamber).

Cotton, H., and Bolan, C. (2011) User Perceptions of End User License Agreements in the Smartphone Environment, *Proceedings of the 9th Australian Information Security Management Conference*, 05-07 December. Perth, Western Australia.

Convention on Cybercrime. (2004) Council of Europe Treaty No. 185, 01 July.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. (2013) *OJ L 218, 14.8.2013*.

Dizon, M. (2016) 'Breaking and Remaking Law and Technology: A Socio-techno-legal Study of Hacking', *Doctoral Thesis*. [Online source] Available from: https://pure.uvt.nl/ws/portalfiles/portal/12403280/Dizon_Breaking_28_06_2016.pdf [Accessed 31.08.2019].

European Commission. (2017) *Special Eurobarometer 464a: Europeans' Attitudes Towards Cyber Security*.

Explanatory Report SE 554. (2013) *Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 554 SE*, 09 December 2013.

Felson, M., and Boba, R. L. (2010) Crime and Everyday Life, 4th Ed. Sage Publications.

Gallagher, S. (2019) 'Ransomware strike takes down 23 Texas local government agencies', *Ars Technica*. [Online source] Available from: https://arstechnica.com/information-technology/2019/08/ransomware-strike-takes-down-23-texas-local-government-agencies/ [Accessed 31.08.2019].

Newman, L. H. (2018) 'Atlanta spent $2.6M to recover from a $52 000 ransomware scare', *Wired*. [Online source] Available from: https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/ [Accessed 31.08.2019].

Hacquebord, F. (2011) 'Esthost Taken Down – Biggest Cybercriminal Takedown in History', *Trend Micro*, 09 November. [Online source] Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/esthost-taken-down-biggest-cybercriminal-takedown-in-history/ [Accessed 31.08.2019].

Heller, N. (2017) 'Estonia, the Digital Republic', *The New Yorker*, 11 December. [Online source] Available from: https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic [Accessed 31.08.2019].

Hirsnik, E. (2014) 'Arvutikuritegevuse regulatsioon Eestis: karistusõiguse revisjoniga toimunud muudatused ja lahendamata jäänud probleemid', *Juridica*, VII.

Hutchings, A., and Hayes, H. (2009) 'Routine Activity Theory and Phishing Victimization: Who Gets Caught in the 'Net'?'. *Current Issues in Criminal Justice*, 20 (3).

Kikerpill, K., and Siibak, A. (2019) 'Living in a Spamster's Paradise: Deceit and Threats in Phishing Emails', *Masaryk University Journal of Law and Technology*, 13(1).

Krebs, B. (2015) 'Chip Card ATM 'Shimmer' Found in Mexico', *KrebsOnSecurity*, 11 August. [Online source] Available from: https://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/ [Accessed 31.08.2019].

Kuckartz, U. (2019) Qualitative Text Analysis: A Systematic Approach. In: Kaiser G., Presmeg N. (eds) Compendium for Early Career Researchers in Mathematics Education. ICME-13 Monographs. *Springer: Cham*.

MacDonald, J. (2017) 'The New Card Skimming is called 'Shimming'', 03 May. [Online source] Available from: https://www.creditcards.com/credit-card-news/new-card-skimming-is-called-shimming.php [Accessed 31.08.2019].

Lavorgna, A. (2015) 'The Online Trade in Counterfeit Pharmaceuticals: New Criminal Opportunities, Trends and Challenges', *European Journal of Criminology*, 12(2).

LexisNexis Risk Solutions. (2019). EMEA Cybercrime Report.

Leukfeldt, E. R. (2014) 'Cybercrime and Social Ties. Phishing in Amsterdam', *Trends in Organized Crime*, 17(4).

Leukfeldt, E. R., and Jansen, J. (2015) 'Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands', *International Journal of Cyber Criminology*, 9(2).

Leukfeldt, E. R., and Yar, M. (2016) 'Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis', *Deviant Behavior*, 37(3).

McGuire, M. 2018. Into the Web of Profit – Understanding the Growth of the Cybercrime Economy. *Bromium*.

Ministry of Justice, Republic of Estonia. (2019) *Kuritegevus Eestis 2018*.

Obar, J. A., and Oeldorf-Hirsch, A. (2018) 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services', *Information, Communication & Society*, DOI: 10.1080/1369118X.2018.1486870.

Penal Code. (2001) 2001/61, 364, Estonia: *Riigi Teataja* (State Gazette). In Estonian. English translation. [Online Source] Available from: https://www.riigiteataja.ee/en/eli/509072018004/consolide [Accessed 31.08.2019].

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *OJ L 119, 4.5.2016*.

Reynolds, M. (2016) 'Welcome to E-stonia, the World's Most Digitally Advanced Society', *WIRED*, 20 October. [Online source] Available from: https://www.wired.co.uk/article/digital-estonia [Accessed 31.08.2019].

Reyns, B. W. (2013) 'Online Routine and Identity Theft Victimization: Further Expanding Routine Activity Theory Beyond Direct-contact Offenses', *Journal of Research in Crime and Delinquency*, 50(2).

Sootak, J., and Pikamäe, P. (2015) Karistusseadustik: kommenteeritud väljaanne (The Penal Code: Commented Edition), *Juura*: *Tallinn*.

Soudjin, M. R. J., and Zegers, B. C. H. T. (2012) 'Cyber Crime and Virtual Offender Convergence Settings'. *Trends in Organized Crime,* 15(2-3).

Torbet, G. (2019) 'Baltimore ransomware attack will cost the city over $18 million', *Engadget*, 06 June. [Online source] Available from: https://www.engadget.com/2019/06/06/baltimore-ransomware-18-million-damages/ [Accessed 31.08.2019].

Van Hoecke, M. 2011. Legal Doctrine: Which Method(s) for What Kind of Discipline? *in* van Hoecke, M (Ed). Methodologies of Legal Research – Which Kind of Method for What Kind of Discipline? *Hart Publishing*.

Wall, D. S. (2008) 'Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime', *International Review of Law, Computers and Technology*, 22(1-2).