Giulio Calcara, Peter Sund & Matti Tolvanen

Cybercrime, Law and Technology in Finland and Beyond

POLICE UNIVERSITY COLLEGE REPORTS 133

CYBERCRIME, LAW AND TECHNOLOGY IN FINLAND AND BEYOND

Giulio Calcara, Peter Sund & Matti Tolvanen

POLIISIAMMATTIKORKEAKOULUN RAPORTTEJA 133

Police University College of Finland
Tampere 2019

Giulio Calcara, Peter Sund & Matti Tolvanen
Cybercrime, Law and Technology in Finland and Beyond

Reports of the Police University College of Finland 133/2019
ISBN 978-951-815-357-6 (printed)
ISBN 978-951-815-358-3 (pdf)
ISSN 1797-5743

PunaMusta Oy, Tampere 2019

ABSTRACT

This book started as a collection of lectures given during the University of Eastern Finland's Summer School of 2016, in the course titled "Internet Crimes". As interest towards this topic increased, different authors from diverse backgrounds subsequently contributed to this collection, eventually forming this book, which has a far wider scope than the original lectures. This book is enthralled in the study of the evolution of technology, its impact on the lives of individuals, and its role in the shaping the law.

The aim of this book is to reflect on the relationship of three distinct concepts: crime, law, and technology. In order to do so, the book explores this relationship by addressing three thematic areas: "Finnish and Nordic Legislation on Cybercrime", "Local and Global Challenges in the Fight against Cybercrime", and "Future Scenarios in Law and Technology." In most contributions, Finland is used as the starting point due to it being among the leading countries in the process of digitalization and modernization of its infrastructures. However, while Finland serves as a starting point, the concepts which are dealt with affect every country, international organization, private entity, and individual in the world.

The first thematic area is tackled by four articles which focus mainly on Finnish and Nordic criminal law, with specific reference to how cybercrime has been regulated in the region. The second thematic area has a wider scope, as it focuses on the challenges in the fight against cybercrime on several levels, namely the Nordic, the European, and the global level. This second thematic area is explored in three articles. The last thematic area is examined by one conclusive article. It focuses on the relationship between law and technology, while exploring future scenarios in the field of cybernetics in detail.

CONTENT

INTRODUCTION

Giulio Calcara and Peter Sund

Cybercrime, Law and Technology in Finland and Beyond started to develop during the University of Eastern Finland's Summer School of 2016. A course titled "Internet Crimes" was organized, and several experts, academics, police and judicial officers, and other practitioners alike shared their knowledge and provided students with up-to-date information on this timely topic. The course proved to be fertile ground for comprehensive and holistic reflection on the diverse, yet, connected issues posed by the evolution of technology, its impact on the lives of individuals, and the shaping of the law. In the end, several lectures and relevant articles were compiled to form this book. While the book uses Finland as a standpoint, it serves a general purpose; these concepts affect every country, international organization, private entity, and individual in the world. The purpose of this book is to reflect on the impact of technology on crime and criminal trends and whether the criminal justice systems provide effective ways of countering them.

It is hard to deny that we are currently experiencing a new industrial revolution,[1] which is steadily leading us towards a new digitalized era. Technology is continuously reshaping society, making the world increasingly interconnected and laws gradually obsolete.[2] As the world changes, the time has come to rethink domestic and international laws. Needless to say, in order to promote appropriate development of the law, law and policy makers, police services, and the legal community in general need to understand how and to what extent technology has modified our reality and, in the end, our way of living. This is not a simple task. As the book wishes to exemplify, 'cyber laws-of-nature are inherently different. Regulation and control is needed, but challenges are substantial. Digitalization and globalization are underpinning it all'.[3]

Currently, Finland is among the leading countries in digitalization.[4] For this reason, the country is an optimal starting point for a project reflecting on law and technology. Recently, the Finnish government has expressed the desire to create a safer cyber environment in order to incentivate a boost in digital businesses and activities and at the same time to assure safety for its citizens.[5] Additionally, the government has clearly recognized the risks present in cyber space and has declared

1 E. Leite, 'Is the law as we know it still fit for purpose?', World Economic Forum, Industry Agenda, 20 January 2016, available online at: https://www.weforum.org/agenda/2016/01/the-rule-of-law-and-the-fourth-industrial-revolution/ (visited 1 March 2018).

2 G. Hadfield, *Rules for a Flat World: Why Humans Invented Law and How to Reinvent It for a Complex Global Economy* (New York: Oxford University Press, 2016).

3 P. Sund, *Global and European Responses to Cybercrime.*

4 B. Chakravorti, A. Bhalla and R. S. Chaturvedi, '60 Countries' Digital Competitiveness, Indexed', *Harvard Business Review*, available online at https://hbr.org/2017/07/60-countries-digital-competitiveness-indexed

5 Ministry of Transport and Communications and the development group for business with information security, *Information Security Strategy for Finland The World's Most Trusted Digital Business Environment*, 19 April 2016, available online at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78416/Publications_9-2016_Information_Security_Strategy_for_Finland.pdf?sequence=1 (visited 09 March 2018).

that they are one of the most severe threats hovering over Finnish society.[6] But it is hard to predict how things will evolve. Even so, while the future is unknown, the present is not bright. Cybercrime is certainly increasing.[7] At the same time, victims have a tendency not to report cybercrime to the police.[8] This could indicate a lack of trust towards the criminal justice system. Even when a cybercrime is reported, the police have less than a 50% chance of solving the case.[9] Taking into account that the Finnish police service in general is a top-performer when compared to its European counterparts,[10] the situation starts to look even gloomier. In order to improve the situation, it will be necessary to review the criminal justice system on all levels by considering, for example, that there are no full-time prosecutors or judges dealing solely with cybercrime in the country.[11]

Yet, the issue of safety in the cyber environment does not weigh solely on the shoulders of Finnish society. An ever-growing number of EU citizens appear to be deeply concerned about becoming victims of cybercrime, and only a fraction of them have trust in the abilities of the public agencies.[12] Even more worrisome and alarming is the apparent widespread acquiescence among the public that we cannot have a safe cyberspace.

However, as previously mentioned, cyberspace is only a small part of a bigger picture that is the advancement of technology. Changes in society tend to occur in parallel with the development of scientific and technical knowledge. New facets of technology such as artificial intelligence, big data and algorithms, Internet of Things (IoT), biotechnology, robotics, and others are rapidly creeping into our everyday lives. They simultaneously pose both unexpected challenges as well as provide vibrant new opportunities for the advancement of society. It is for this reason that, while this book focuses mainly on cybercrime, a section deviates from this narrow topic. This section considers a separate area of technology called cybernetics. It demonstrates, through concrete examples, how different areas of technology have the potential of affecting society on a deep level, thusly forcing the legal community to assess once again the current state of the law and, more in general, of the entire criminal justice system. The developing area of cybernetics offers a poignant insight to a vast set of challenges, both ethical and legal, that lawmakers around the globe could hypothetically face in the future.

---

6 Ministry of the Interior, *National Risk Assessment 2015* (2016), available online at: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/64973/National%20Risk%20Assessment%202015.pdf (visited 09 March 2018).

7 Internet Organised Crime Threat Assessment (IOCTA), *THREAT ASSESSMENT ON INTERNET FACILITATED ORGANISED CRIME* (2011), available online at https://www.europol.europa.eu/activities-services/main-reports/threat-assessment-internet-facilitated-organised-crime-iocta-2011 (visited 13 October 2017).

8 A. Seger, 'Evidence in the Cloud and the Rule of Law in Cyberspace', 7 *Europe's World*, December (2015) available online at http://europesworld.org/?p=10119 ; M. Näsi and M. Tanskanen. *Kyberrikollisuus*, in Valtiotieteellinen Tiedekunta Kriminologian Jaoikeuspolitiikaninstituutti, *Rikollisuustilanne 2016 Rikollisuuskehitys Tilastojen ja Tuktimusten Valossa* (Helsinki: Helsingin yliopisto, Kriminologian ja oikeuspolitiikan instituutti, 2017).

9 E. Mäntymaa, *Kyberrikollisuus moninkertaistunut – yli puolet rikoksista jää selvittämättä*, Yle Uutiset, 20 February 2015, available online at: https://yle.fi/uutiset/3-7809103 (visited 09 March 2018).

10 Statistics Finland, *Finland among the best in the world*, 8 March 2018, available online at https://www.stat.fi/ajk/satavuotiassuomi/suomimaailmankarjessa_en.html (visited 09 March 2018).

11 H. Tiesmaa, *Kyberrikollisuutta on voitava torjua tehokkaasti*, Akkusastoori: Syyttäjälaitoksessa Tapahtuu (2016), available online at: http://vksv.fi/akkusastoori/material/attachments/akkusastoori/glgQW93DN/Akkusastoori_2_16_low_NETTIVERSIO.pdf (visited 09 March 2018).

12 Special Eurobarometer 464a, *Europeans' attitudes towards cyber security*, European Commission, Directorate-General for Migration and Home Affairs and co-ordinated by the Directorate-General for Communication (2017), available online at: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171 (visited 09 March 2018).

As always, it is crucial that the legal community prepares itself to embrace positive changes in technology, while at the same time being aware of possible drawbacks, ready to counteract them.

This book is divided into three main sections: "Finnish and Nordic Legislation on Cybercrime", "Local and Global Challenges in the Fight against Cybercrime" and "Future Scenarios in Law and Technology". Each section is composed of one or more articles. While the articles are designed to form a coherent part of this book, they have nevertheless been written, and thus can be viewed, independently. Consequently, certain information might be emphasized or assessed differently in different texts. That, in turn, allows for a more precise analysis on the issues outlined in them.

The first section focuses mainly on Finnish and Nordic criminal law and on how cybercrime has been regulated. This section contains four articles. It starts with an article by Matti Tolvanen, which presents in detail how the domestic law of Finland has absorbed the phenomenon of cybercrime. The text focuses specifically on the elements of criminal offences in Finnish criminal law and the underlying principles of criminalization. In addition, relevant case law and the jurisprudence of the Finnish Supreme Court are presented in this context. The section continues with an article by Mika Sutela, which expands on the general theme of Tolvanen while focusing on the sentencing of cybercrime in Finland. The sentencing of cybercrime is a topic which undeniably deserves more attention as it fails at times to fulfil the essential principles of ordinal and cardinal proportionality. The section's third article is by Jussi Tapani. He discusses how the criminal offence of fraud has changed in the cyber context. As a tool to carry out his analysis, he assesses the crime of fraud from three different aspects, which he defines as the 'three generations of cyber fraud'. The scope of the analysis is to provide a general assessment on whether the criminal offence of fraud should have a different normative treatment when it is carried out in cyberspace. The same area of cybercrime is explored by Laura Tammenlehto in the fourth article. She compares Nordic criminal legislation in matters of fraud, with particular reference to the counterfeiting of goods, especially food and spare parts. Tammenlehto shows how the relevant criminal law is not suitable for facing the challenges posed by this online phenomenon in the Nordic countries. Counterfeiting remains a constant threat to the health, safety and finances of individuals and companies alike. The phenomenon deserves a drastic revision from law makers both at the domestic and international level.

In the second section the focus is expanded from the Nordic countries to the global arena and contains three articles. It starts with an article by Peter Sund that serves as an introduction to themes such as cybercrime and cybersecurity and how these phenomena have been approached and tackled on the European and global level. It comprehensively presents the major entities and institutions involved in the response to cybercrime. In addition, the article presents the 'cyber laws-of-nature' with clarity. Such description demonstrates how law makers need to be aware of the complexities of cyberspace and why regulatory efforts need to be calibrated to such an environment. Sund depicts a scenario full of complexities and concludes his article with a simple, yet, defining truth: 'The future of digital security is generated from trust, cooperation and responsibility.'

The second article belongs to Katja Lindroos. The contribution sheds light on the overwhelming emergence of conflicts of fundamental rights in the digital environment. The increasing presence of these kinds of conflicts becomes evident when we examine the process of pursuing criminal activity on the internet. Several case studies are presented and discussed to illustrate and analyse the legal principles underlying the practical resolution concerning the conflicts of rights.

The section's last article belongs to Giulio Calcara and continues on the issue of the European and global response to cybercrime. In doing so, however, it uses a narrower focus by providing an assessment on the role of the main entities involved in international police cooperation in the fight against cybercrime. The nature and complexity of cybercrime is presented and discussed. Subsequently, the article focuses on both the legal and practical challenges that these entities encounter during their activities in this specific crime area, with suggestions for improvement being derived from the context.

The last section, "Future Scenarios in Law and Technology", focuses on the relationship between law and technology while exploring future scenarios in the field of cybernetics. The section consists solely of the article "Neuroscience and Judicial Proceedings, Past and Present. What will the Future Bring?" written by Jordi Nieva Fenoll. The paper provides an in depth insight into the current and potential future uses of neuroscience in judicial proceedings. More specifically, it provides a clear and detailed analysis of the legal issues which might arise from such techniques in the not so distant future. The article presents several hypotheses on how scientific knowledge and techniques might advance and evolve, and it delivers a reflection on the modalities of how and to what extent law and judicial practice should embrace such changes.

FINNISH AND NORDIC LEGISLATION ON CYBERCRIME

CYBERCRIMES IN FINNISH CRIMINAL LAW

Matti Tolvanen

1 Protected Legal Right (Rechtsgut), Criminal Policy Argumentation of Criminalization and Division of Cybercrimes

Information technology is involved in our everyday life. Business activities and transactions with authorities have to a significant extent been transferred to networks. This development has not yet reached its endpoint because increasingly new activities, including teaching, are going to be transferred to the online environment. Criminal law indirectly protects economic and other interests. Punishment itself cannot prevent acts or omissions. The legislator seeks to maintain people's confidence in the security of online transactions and the undisturbed operations of the networks by regulating actions in a network environment as crimes.

Cybercrimes have been characterized as acts that are defined as including different criminal elements and that are committed using information technology. This definition is quite extensive. The object of cybercrime's legal protection has been defined as computer peace, which emphasizes as described above that the network must be able to operate as undisturbed as possible.[1] Making computer safety a basis for legal protection is proper only if it is known what object of legal protection lay hidden behind this term. Computers have sensitive information inside of them, and this is how the criminalization of the misuse of information technology protects people's right to privacy. Computers are fitting for committing traditional property crimes and especially for committing fraud. Therefore, property is one of the objects of protection in criminalization. Recently the online environment has increasingly been misused by violating the online communication of people's honour and freedom (e.g. persecution, illegal threats and incitement to racial hatred). In the networks people commit a wide range of sexual freedom violations, and thus behind the cybercrime criminalization can be seen also sexual sovereignty and sexual health (e.g. sexual offences against child). Complicity (e.g. co-partners, incitement, aiding and abetting in crime) may actually be realized in any type of crime also by taking advantage of the information network.

According to the essential elements of criminal acts, cybercrimes can be divided in several ways. Criminalization is scattered across several criminal code chapters. While applying essential elements of criminal acts, the general conditions of crimi-

1 Antti Pihlajamäki: Tietojenkäsittelyrauhan rikosoikeudellinen suoja, Jyväskylä 2004, p. 55–59.

nal liability in criminal code have to be fulfilled as well. In this article cybercrimes are divided as follows: a) Criminal Code chapter 38 includes data and communication offences, b) cybercrimes involving danger to the public (Criminal Code chapter 34), c) malicious damage crimes (Criminal Code chapter 35), d) property crimes (Criminal Code 36:1 and 2, 37:8, 33:1, 28:7 and 30:4), e) network sexual offences (Criminal Code chapters 17 and 20) and f) crimes against honour and freedom (Criminal Code chapter 11,24 and 25). From viewpoint of criminal responsibility's general doctrine, the most current regarding cybercrimes are intent, consequence and danger, uniting and concurrence of offences.

The aim of this presentation is to provide an overview of certain types of crimes committed which using information technology. The presentation is not comprehensive, and the aim is to look at the essential elements of the main types of crimes. In doing so, the focus is on the systematization of the essential elements of the crimes. Due to limited space, problems associated with interpreting individual types of crimes receives less attention.

2 Data and Communication Offences (Criminal Code Chapter 38)

2.1 Data and Message Interception

The basic form of the data and communication offences is the message interception, which is regulated in Criminal Code chapter 38 section 3. The law prescribes following a person who unlawfully (1) opens a letter or another closed communication addressed to another or by hacking obtains information on the contents of an electronic or other technically recorded message which is protected from outsiders or (2) obtains information on the contents of a telephone call, telegram, transmission of text, images or data, or another comparable tele-message that is transmitted by telecommunications or an information system or on the transmission or reception of such a message shall be sentenced for message interception to a fine or to imprisonment for at most two years. Attempting this crime is also punishable.

The first prerequisite for this crime is unlawfulness. Seen in practical terms, only the sender and the recipient have the right to the message's content. According to the law of coercive means, also an official authority such as the police may have the right to the message's content. There are two means of acting mentioned in the law: opening closed messages or obtaining the information by hacking. Another technique is to obtain information from the message transmitted. This method of acting does not require hacking as to obtain information unlawfully is punishable.

It is not required that the criminal act causes any harm or even danger of harm. These types of crimes in Finnish legal doctrine are defined as pure tort crimes; in other words acting as such may fulfil the elements of crime.[2] Message interception is punishable only as intentional, and the perpetrator must consider the facts underlying criminal liability as being more probable (Criminal Law chapter 3 section 6). Purpose of violation is not required.

Electronic mail (email) has been considered problematic when applying this regulation. Regarding e-mails, the requirement for criminal responsibility is that the message is technically protected from outsiders and that someone unlawfully

2 Jussi Tapani–Matti Tolvanen: Rikosoikeuden yleinen osa, Vastuuoppi, Helsinki 2013, p. 176–177.

unlocks this protection. There is a possibility under certain conditions to open an employee's email without his presence in the work place (Act on the Protection of Privacy in Working Life 759/2004, sections 18-20). The general requirement for opening an email is the necessity to carry out the duties defined by the law.

Criminal Code chapter 38 section 4 is enacted in regard to aggravated message interception where the maximum punishment is imprisonment for three years. The basis for qualification is that the offender commits the offence by making use of his or her position in the service of an institution referred to in the Telecommunications Act, a cable operator referred to in the Cable Transmission Act (307/1987) or a public broadcasting institution, or his or her other special position of trust. Second, the act may be aggravated if the perpetrator uses a computer program or special technical equipment, which is designed for committing a crime, or otherwise commits the crime using a specially planned manner. Third, the offence may be aggravated if the message, subject of the offence, is particularly confidential or the act significantly violates protection of privacy. In addition, one prerequisite is that the act is aggravated as a whole.

2.2 Interference with Communications

Criminal Code chapter 38 section 5 regulates as punishable the interference with communications. The law determines the crime in the following way: A person who by tampering with the operation of a device used in postal, tele-communications or radio traffic, by maliciously transmitting interfering messages over the radio or telecommunication channels or in another comparable manner un-lawfully prevents or interferes with postal, telecommunications or radio traffic, shall be sentenced for interference with communications to a fine or to imprisonment for at most two years. In addition, an attempt of this crime is punishable.

Telecommunication interference is also a pure act crime and punishable only if the act is intentional. It is also a crime to interfere in a device's operation, which is more closely defined in law, sending disturbing messages or other unlawful mail traffic, disturbing or blocking telecommunications or radio communications. Although the word 'malicious' has been used in one form of act, the motive itself has no relevancy in regard to punishment.

Aggravated interference with communications has been defined as a crime under Criminal Code chapter 38 section 6. The first criterion for qualification is that the offender holds a special position of trust in a media institution. Second, the act may be defined as aggravated if the offence prevents or interferes with distress signals, which are used to secure human life. Third, the law determines (Criminal Code 38:6.1, 3) which equipment or programs used for harassment is applicable as a qualification basis. In addition, the offence committed as part of an organized criminal group may be a legal basis to define an act as aggravated. The act is also aggravated if it causes serious impediment or economic loss. Specially, one qualification basis is at hand if the offence is directed to a function that is important to society and that is comparable to these. The interference with communications has to be aggravated also when assessed as a whole.

The legal field of punishment is quite extensive because petty interference with communications and an attempting this crime are punishable (Criminal Code 38:7). It is possible to define a crime as a petty interference with communications if the interference with communications, in view of its nature or the extent or the other circumstances of the offence, is minor in significance when assessed as a whole.

2.3 Interference in an Information System

Criminal Code chapter 38 section 7a regulates the following: A person who in order to cause detriment or economic loss to another, by entering, transferring, damaging, altering or deleting data or in another comparable manner unlawfully prevents the operation of an information system or causes serious interference in it shall be sentenced for interference in an information system to a fine or to imprisonment for at most two years. An attempt of this crime is punishable.

The requirement of criminal liability is that the offender intends to cause a consequence which is referred to in the law. In legal writing, this kind of intent has been defined as an advanced claim of intent. It is not sufficient that the offender more likely thinks that his action may cause a consequence which is prohibited by the law. The offender must intend to cause detriment or economical loss to another. Techniques defined by law are entering, transferring, damaging, altering or deleting data or in another comparable manner that unlawfully prevents the operation of an information system or that causes serious interference in it. According to the explicit wording of the law, the list of methods to do this is not exhaustive. The common feature of the methods is that the offender causes interference either by using information from outside the systems or by interfering with the usage of the information inside the system. Data refers to essential elements, the information system or its storage platform or the data, which can be entered into it. The damage caused by different types of techniques may be the same because even a small change in data might lead to a serious disturbance. Unlawfulness refers to the fact that the offender has no right to interfere with the subject matter of the act. Not every act meets the essential elements of the crime; in order to fulfil the elements of the crime the act must prevent the information system's operation or cause a serious disturbance. The benchmark is the system's normal operation, which generally has minor disturbances. A serious disturbance means the same as a substantial slowdown of the system or an essential reduction of the system's activity.

Criminal Code chapter 38 section 7b prescribes aggravated interference in an information system. The aggravated act is defined as follows: The interference in an information system is when a (1) particularly significant detriment or economic loss is caused or (2) the offence is committed in a particularly methodical manner or (3) the offence is committed as part of an activity that has to a significant degree affects an information system through the use of a device, computer program or set of programming instructions as referred to in Chapter 34, section 9(a), paragraph 1, subparagraph (a) or a password, access code or other corresponding information as referred to in subparagraph (b) or (4) the offence is committed as part of an organized criminal group as referred to in Chapter 6, section 5, paragraph 2, (564/2015) or (5) the offence is directed at an information system, the damaging of which could endanger the energy supply, general health care, national defense, the administration of justice or another function that is important to society and that is comparable to these and where the interference in an information system is aggravated also when assessed as a whole.

2.4 Computer Break-in

Computer break-in, better known as hacking, is a kind of basic form of cybercrime.[3] This section applies only to acts that are not subject to an equally severe or more severe penalty provided elsewhere in the law. This is quite a customary subsidiary clause in Finnish criminal law. Criminal Code chapter 38 section 8 prescribes this in the following way: A person who by using an access code that does not belong to him or her or by otherwise breaking a protection system unlawfully hacks into an information system where information or data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a computer break-in to a fine or to imprisonment for at most two years. Also a person who, without hacking into the information system or a part thereof, (1) by using a special technical device or (2) otherwise by by-passing the system of protection in a technical manner, by using a vulnerability in the information system or otherwise by evidently fraudulent means unlawfully obtains information or data contained in an information system referred to in subsection 1, shall be sentenced for a computer break-in. An attempt of this crime is punishable.

The subject of the matter is the information system or its protected part. The provision applies to information systems where data has been processed, stored or transferred electronically. The information system means the equipment that certain organizations use in their data processing and data transferring. Unlawfulness means the person has no right to access the system or part of it. In the same company, there may be system components that only one employee has access to. The subject matter may be also in the memory of the computer as well as being transferred over a data transfer line. The first technique relevant in such an act is to use an access code that does not belong to the offender or to otherwise unlawfully break a protection system and hack into an information system. It is not relevant how the offender attained knowledge of the access code. It is sufficient that the offender illegally uses the access code. The subject matter is an information system where information or data is processed, stored or transmitted electronically or in a corresponding technical manner or into a separately protected part of such a system. Intrusion means that the prerequisite for criminal liability is the act of the offender. If someone takes advantage of an occasional disturbance in the security system or of another legally authorized access code, this does not constitute penetrating into the system in the meaning of this chapter.

When using the other technique in the chapter, the offender does not break into the information system or into its parts. The criminal act is realized by using a special technical device or otherwise by bypassing the system of protection in a technical manner by using a vulnerability in the information system or otherwise and by evidently fraudulent means unlawfully obtaining information or data contained in the information system.

We do not have many precedents concerning cybercrimes. There is actually one good precedent from the Supreme Court (2003:36) about an attempt of cybercrime.[4] The criminal act of the perpetrator was at the same time fulfilling the essential elements of an attempt of cybercrime and criminal damage. Defendant (A) had tried to break the security system in order to illegally invade a certain cooperative society's information system. Defendant (A) had used a special computer program for

3 Pihlajamäki 2004, p. 123–141.

4 Matti Tolvanen: Tietomurto, yrityksen rangaistavuus ja rikokseen perustuva vahingonkorvaus, KKO:n ratkaisut kommentein I/2003, p. 256–264.

scanning all the addresses from the cooperative's connected network. The purpose of (A) was to find an open web-server. Scanning had not passed the firewall of the cooperative's information system. If defendant (A) had found an open server, he would have been able to gain access to the internet. This would have appeared as if the connection had come from this server.

Defendant (A) considered that he had not committed an attempt of a cybercrime because his intention was only to find open servers. Defendant (A) considered further that the act did not fulfil the essential elements of attempting a cybercrime because accessing the system does not require breaking the security system in the way mentioned in the case. Defendant (A), who had been 17 years old at the time of the criminal act requested settlement for damages in case he would be found guilty of a criminal offence.

The Supreme Court sentenced (A) to a penalty for an attempt of cybercrime and ordered him to pay 20,000,00 FIM to the cooperative society and 55,000,00 FIM to the company belonging to the same group which had been equivalent to the information systems. The Supreme Court did not settle the damages but considered (A) to be liable to compensate the damages in their entirety.

Defendant (A) explained that his intention was not to invade the system but only to find open servers. The Supreme Court stated that according to the legislative history the invasion of the system does not require any specific purpose. The provision is also applicable if the invasion of the information system happens for amusement. In the government proposal, the punishability of an attempt has been argued to be worthy of criminal sanction as follows. Criminalization concerns interfere in the reliability and the security of the information system's access code The simple identification of an access code or another attempt to break into the security system is already punishable if the act is meant to break into the information system. The wording 'break into' refers to the unlawfulness of passing the security system.

The aim of port scanning is to investigate the operative programs of the information system data ports and operating systems and their vulnerability. Therefore, the scanning is performed over the network to find the 'doors' of the target machine and to test if one of them is open. Programs have been developed for this purpose, which can for example return a report from the scanned target machine, its communication ports, software and its security threat. The method is used legally to research an information system's security.

With the port scanning program it is possible to get information which enables unauthorized access to the system. The program systematically investigates potential gaps and weak items in the system. Thus, it is possible to break the information system's security structure with the obtained information. The Supreme Court emphasized that an attempt of cybercrime will be fulfilled when the user of the program tries to acquire knowledge which enables unauthorized access into the information system with the intent to invade it.

The Supreme Court has defined in the case KKO 2003:36 the range of the punishable attempts of data breach. Hacking and breaking into information systems is a serious problem because delicate information has been transferred electronically. The provisions on data breach are aimed to secure the so-called computer peace, i.e. an information system against external intrusion and to secure the privacy of a computer working from external surveillance when not a question about tapping or illicit viewing. The court decisions have a guiding function, especially the precedents of the Supreme Court. Those who violate the norms will be punished in order to assure those people who obey the law that society is able to maintain the normative system that has been set. Information security is best promoted through

technical arrangements. However, criminal law enforcement is needed as well, and the problems created by the new information technology emphasize its need. In the field of information technology, the ethical normative is in fermentation because of rapid development, and the limit between what is allowed and what is forbidden is not always clear. In problematic situations, it is therefore important that the Criminal Code is able to provide clear norms as a basis for human behavior. If people see, that an individual breaks the norms without consequences their confidence in the security of data may collapse. Even unintentional hacking of access codes to a system is punishable because it is impossible to distinguish those who are striving to get economic profit from those who seek to abuse or harm the system. There are no valid reasons for unlawful and systematic break-in attempts. In this type of crime, the risk of being caught has central relevance. However, the magnitude of an actual punishment may not be so central.

There is also the aggravated form of the computer break-in in the Criminal Code chapter 30 section 8a. If the computer break-in is committed (1) as part of an organized criminal group referred to in Chapter 6, section 5, paragraph 2, (564/2015) or (2) in a particularly methodical manner, and the computer break-in is aggravated also when assessed as a whole, the offender shall be sentenced for an aggravated computer break-in.

2.5 Offence Involving a System for Accessing Protected Services

An offence involving a system for accessing protected services is punishable under Criminal Code chapter 38 section 8b. It is punishable if a person who, in violation of the prohibition laid down in section 269, subsection 2 of the Information Society Code (917/2014), for commercial purposes or so that the act is conducive to causing considerable detriment or loss to a provider of protected services, produces or imports, offers for sale, rents out or distributes a system for accessing protected services, or advertises, installs or maintains the same. This criminal provision is secondary. It applies only if there is no other more severe or equally severe penalty provided elsewhere in law for the act.

2.6 Data Protection Offence

People's personal data is increasingly stored and processed in information systems. The registers also contain sensitive information about for example the state of human health. Criminal Code chapter 38 section 9 determines a date protection offence in the following way: If a person who intentionally or grossly negligently (1) processes personal data in violation of the provisions of the Personal Data Act (523/1999) on the exclusivity of purpose, the general prerequisites for processing, the necessity and integrity of data, sensitive data, identification codes or the processing of personal data for specific purposes, or violates a specific provision on the processing of personal data, (480/2001) or (2) by giving false or misleading information prevents or attempts to prevent a data subject from using his or her right of inspection or (3) conveys personal data to states outside the European Union or the European Economic Area in violation of Chapter 5 of the Personal Data Act and thereby violates the privacy of the data subject or causes him or her other damage or significant inconvenience.

The exact content of this provision is determined in the Personal Data Act (523/1999). The Personal Data Act section 3 defines the relevant legal concepts for applying this law. *Personal data* means any information on a private individual and any information on his/her personal characteristics or personal circumstances where these are identifiable as concerning him/her or the members of his/her family or household. *Processing of personal data* means the collection, recording, organization, use, transfer, disclosure, storage, manipulation, combination, protection, deletion and erasure of personal data, as well as other measures directed at personal data. *Personal data file* means a set of personal data, connected by a common use and processed fully or partially automatically or sorted into a card index, directory or other manually accessible form so that the data pertaining to a given person can be retrieved easily and at reasonable cost. *Data subject* means the person to whom the personal data pertains.

The offender may be the controller of the register or his/hers representative or employee. However, the law does not have a limited scope for these parties. Anyone, like a database administrator or user, having access to personal data may become involved in principle as an offender.

There are three types of criminalized acts defined in this chapter. First, it is prohibited to process personal data violating the provisions of the Personal Data Act. The key term is the state of being bound by the purpose of use. The Personal Data Act precisely specifies the purpose of who is entitled to process personal data and for what purpose. The law particularly protects sensitive information, and for processing personal data it is generally required that it is necessary to accomplish an individual task. Processing this information is prohibited everywhere else than in the determined purpose of the Personal Data Act section 12. In addition, in different branches of legislation there are special provisions for processing personal data (for example Act on the Processing of Personal Data by the Police 761/2003).

In another case of the data protection offence the offender intentionally or grossly negligently by giving false or misleading information prevents or attempts to prevent a data subject from using his/her right of inspection. The third method is if the offender conveys personal data to states outside the European Union or the European Economic Area in violation of Chapter 5 of the Personal Data Act.

On the subjective side, the prerequisite for criminal liability is intent or gross negligence. The offender who proceeds intentionally considers the underlying facts of criminal liability as being quite probable. According to Criminal Code Chapter 3 section 7 subsection 2 it is defined as to whether or not negligence is deemed gross (gross negligence) and is decided based on an overall assessment. In the assessment, the significance of the duty to take care, the deliberateness of the taking of the risk and other circumstances connected with the act and the perpetrator are taken into account.[5]

In addition, the prerequisite for criminal liability is that the act violates the privacy of the data subject or causes him/her other damage or essential harm. Therefore, in order to impose criminal liability, it is required as a consequence originating from the criminal act. The Personal Data Act section 48 has provided as punishable slight data protection offences as a personal data violation.

5 Tapani–Tolvanen 2013, p. 197–282.

2.7 Identity Theft

This crime is the latest criminalization in regard to information technology. Stealing a third party's personal information was not previously punishable unless the personal data was used for example in fraud offences. In the identity theft a person who in order to deceive a third party unlawfully uses the personal information, access codes or other corresponding identifying information of another and in this manner causes economic loss or more than petty impediment to the person to whom the information belongs.

Despite the criminal title the criminal liability is not realized by the fact that someone takes over another's personal information without lawful right. The first prerequisite for criminal liability is the purpose of misleading. Another precondition is the unlawful use of another's personal data. The third criterion is that the act causes financial damage or minor damage to the complainant.

The identity theft is usually a pre-crime to another offence. A typical crime caused by identity theft is a subscription crime where someone else's personal data are used to order goods or services for the offender who is unwilling to pay for the purchases or services. The identity theft may also lead to acts where other personal data are used in social media forums unlawfully in a way that obviates the holder.

2.8 Definitions

Criminal Code Chapter 38 section 13: When applying sections 2, 6, 7(a), 7(b) and 8, 'information system' refers also to the following, as referred to in article 2(a) of Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (hereinafter the Directive on Attacks against Information Networks: (1) a device or group of interconnected or related devices, one or more of which have been programmed for automatic processing of data; and (2) data stored, processed, retrieved or transmitted by the device or group of devices for the purpose of its or their operation, use, protection and maintenance.

When applying sections 3, 7(a) and 8, 'data' refers also to the following, as referred to in article 2(a) of Directive 2013/40/EU of the Directive on Attacks against Information Networks: (1) a representation of facts, information or concepts in a form suitable for processing in an information system; and (2) a program suitable for causing an information system to perform a function.

2.9 Corporate Criminal Liability and Forfeiture

The provisions on corporate criminal liability apply to message interception, aggravated message interception, interference with communications, aggravated interference with communications, computer break-in, aggravated computer break-in, interference in an information system and aggravated interference in an information system (Criminal Code 38:12).

A system for accessing protected services, as referred to in section 8(b, offence involving a system for accessing protected services), shall be ordered forfeit to the State.

2.10 Right to Bring Charges

Criminal Code Chapter 38 section 10 prescribes that if the object of a secrecy offence or a secrecy violation is information relating to the personal or financial circumstances or the business of an individual, the public prosecutor may not bring charges for the act, unless the injured party reports it for the bringing of charges or unless the offender has committed the offence in the service of a public postal or telecommunications institution or unless a very important public interest requires that charges be brought.

The public prosecutor may not bring charges for message interception, aggravated message interception, interference in an information system, computer break-in or an offence involving an illicit device for accessing protected services, unless the injured party reports the offence for the bringing of charges or unless the offender has committed the offence in the service of a public postal or tele-communications institution or unless a very important public interest requires that charges be brought.

The public prosecutor shall hear the Data Protection Ombudsman before bringing charges for a secrecy offence, secrecy violation, message interception, aggravated message interception or computer break-in, where the object of the offence is a personal data file, or for a data protection offence. When hearing such a case, the court shall reserve the Data Protection Ombudsman an opportunity to be heard. The prosecutor may bring charges for identity theft only if the injured party reports the offence for the bringing of charges.

3 Endangerment of Data Processing

Criminal Code Chapter 34 legislates about endangerments. Chapter 34 sections one and three of the acts are connected with information technology. Chapters 9a and 9b regulate especially about endangerment of the data processing and its preparation.

Criminal Code chapter 34 section 1 provides for punishable criminal mischief. One of its forms is the damaging of communication connections: also a person who damages or destroys property or unlawfully interferes in the operation of production, supply or *communications channels*, so that serious danger is caused to the power supply, public health care, defence, administration of the law or another correspondingly important societal function shall be sentenced for criminal mischief. An attempt is punishable. Aggravated criminal mischief is enacted in Criminal Code Chapter 34 section 3.

Criminal Code 34 Chapter 34 section 9a stipulates punishable endangerment of data processing. A person who, in order to impede or damage data processing or the functioning or security of an information system or telecommunications system, (1) imports, obtains for use, manufactures, sells or otherwise disseminates or makes available (a) a device or computer program or set of programming instructions designed or altered to endanger or damage data processing or the functioning of an information system or telecommunications system or to break or disable the technical security of electronic communications or the security of an information system, or (b) an information system password, access code or other corresponding information belonging to another, or (2) disseminates or makes available instructions for the production of a computer program or set of programming instructions referred to in paragraph (1).

The danger may be caused by infecting the information system with viruses. However, there is no definition for a virus, and the term is not used in law There are known to be over 100,000 viruses, and the number is growing. Therefore combating viruses may sometimes seem quite frustrating. Viruses may affect the data processing in many different ways. Part of the system is infected while starting the system, some of the viruses spread through the program files and some through attachments. Part of the viruses tend to prevent antivirus programs from running. Along with viruses, the contamination of information systems by other malware (such as the so-called Trojans) fulfils the essential elements of crime.

Malware causes different types and different levels of damage. Dangerous or highly dangerous malware destroy or modify existing files. Even less dangerous malware cause harm and costs to the user by slowing down the use of information systems. In legal writing, it has been considered that there is no reason to set a high verge because of the harmfulness of the programs. Expenses also arise from virus protection and cleaning information systems from viruses. In the worst case scenario, viruses may endanger vital functions of society such as energy systems or medical care. Just as worse, malware can be used as a form of cyber warfare.

The first criterion for punishability is to cause harm or damage to the data processing or to the information and communication system or its security. As far as the criteria of a criminal act are concerned, the question is about malware importation, supplying, production, selling and other donations. Selling is a basis for compensation, but spreading the malware without asking for compensation is punishable. It is also a crime to acquire an information system password, access code or other corresponding information belonging to another person. It has been enacted as an independent way of committing this crime to spread or make available a guide for the production of computer programs or a program command series, which are mentioned above. Making it available means placing a virus program into the network, which can be freely copied. In all cases the resulting active action, that the computer virus, technical device or intrusion program are transferred to another person's usage, is punishable.

The tools for cybercrime can be used legally for designing information systems and their protection. Malware is also allowed for this type of test. In criminal investigation, prevention and education it may be legal to use cybercrime devices.

Criminal Code Chapter 34 section 9a is applicable unless an equally severe or more severe penalty for the act is provided elsewhere in the law. It is therefore a secondary offence. The provision of the application can be displaced by the fact that the act also provides essential criteria for the act of criminal mischief. In the same way as data processing fraud, the essential elements of Criminal Code 36:1.2 disregard the essential elements of Criminal Code chapter 34 section 9a. Similarly, the essential elements of Criminal Code 35:3a regarding damage to date also displace the essential elements of Criminal Code Chapter 34 section 9a, but regarding petty damage to data Criminal Code chapter 34 section 9a can be simultaneously applied.

The provision of Criminal Code Chapter 34 section 9b are the essential elements of the type of preparatory act. In this act, the possession of a data system offence device has been legislated as punishable. The law prescribes it as follows: This is when a person who in order to cause impediment or damage to data processing or to the operation or security of a data or communications system has possession of a device, computer program or set of programming instructions as referred to in section 9(a), paragraph 1(a) or a password, access code or other corresponding information as referred to in subparagraph b. Therefore, it is punishable to possess a device or information which is suitable for the offence referred to in Criminal Code Chapter 34 section 9a.

This is one of the few crimes in which the possession of information has been legislated as punishable. Possession does not only mean physical possession, but other rights of disposition to the instrument or program can be considered possession purposed in this decree. The prerequisite for punishment is the intent to cause harm or damage to data processing or to the information and communication system's security.

Cybercrimes involving danger to the public are punishable only by intent, and they have increased criminal liability and the purpose of causing the consequences described in the essential elements. The provisions on corporate criminal liability apply to an endangerment of data processing (Criminal Code 34:13).

4 Criminal Damages

Criminal Code Chapter 35 prescribes on criminal damages and has its own essential elements for damages involving cybercrime. Damage to data has been enacted as a crime in Criminal Code chapter 34 section 3a. A person who, in order to cause damage to another, unlawfully destroys, demolishes, hides, damages, alters, renders unusable or conceals data recorded on an information device or another recording or data in an information system, shall be sentenced for damage to data. An attempt of this crime is punishable.

In these essential elements, also the prerequisite for criminal liability is an intention to cause damage and the fact that the act really causes harm to another. The second criterion for punishment is the unlawfulness of the act. The methods of performing the criminal act have been mentioned as causing damage to another and unlawfully destroying, demolishing, hiding, damaging, altering, rendering unusable or concealing data recorded on an information device or another recording or data in an information system.

Aggravated damage to data has been stipulated in Criminal Code Chapter 35 section 3b following: If the damage to data (1) causes particularly serious harm or economic loss,(2) is committed as part of the activity of an organized criminal group referred to in Chapter 6, section 5, subsection 2,(3) is committed as part of activity that has affected a significant amount of information systems through the use of a device, computer program or set of programming instructions referred to in Chapter 34, section 9(a), paragraph 1, subparagraph (a) or a password, access code or other corresponding information referred to in subparagraph (b), or(4) is directed at an information system, the damaging of which could endanger the energy supply, general health care, national defence, the administration of justice or another function that is important to society and that is comparable to these, and the damage to data is aggravated also when assessed as a whole, the offender shall be sentenced for aggravated damage to data. An attempt of this crime is punishable.

If the damage to data, when assessed as a whole, with due consideration to the minor significance of the damage or the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for *petty damage to data*.

The provisions on corporate criminal liability apply to damage to data and aggravated damage to data (Criminal Code 35:8).The report of, prosecution for or punishment for *petty damage to data* may be waived if the suspect or the offender has compensated the damage and the compensation is deemed a sufficient sanction (Criminal Code 35:7).

5 Cyber Crimes as Property Crimes[6]

Criminal Code Chapter 36 section 1-3 l prescribes about fraud. The basic form of the offence has been enacted in Chapter 36 section 1 subsection 1 as follows: A person who, in order to obtain unlawful financial benefit for himself or herself or another or in order to harm another, deceives another or takes advantage of an error of another so as to have this person do something or refrain from doing something and in this way causes economic loss to the deceived person or to the person over whose benefits this person is able to dispose, shall be sentenced for fraud.

Cybercrime fraud was added to the Criminal Code in 1990 as a part of the comprehensive reform of the Penal Code. The provision was revised in 2003. Committing fraud by using information technology has been imposed as punishable in its own form in the Criminal Code Chapter 36 section 1 subsection 2. According to the act also a person who, with the intention referred to in subsection 1, by entering, altering, destroying or deleting data or by otherwise interfering with the operation of a data system, falsifies the end result of data processing and in this way causes another person economic loss, shall be sentenced for fraud. An attempt of this crime is also punishable.

It is not intent by simply misleading *people* when committing computer fraud. It is essential that for this type of crime to take place that when distorting the truth of the data processing the actor might cause financial loss to another. The punishability of computer fraud also requires the purpose of obtaining unjustified financial advantage for him/her or damage to another. This is an increased requirement of intent. The methods of acting are entering, altering, destroying or deleting data. Data means information in an electric form or information which is suitable to be processed as such in an information system. The definition of the methods is not exhaustive. In addition, other intervention into the information system than already mentioned in the provision may realize the essential elements of computer fraud. It is essential that the operation may cause distortion to the results while processing the information and because of that it may cause economical damage. In the intention of fraud, entering the *right* information in order to distort the result is punishable if it causes economical loss.

The misuse of a slot machine or the unauthorized use of it is punishable as *payment fraud*. If, for example, a fuel automat is able to be operated with no money or payment instrument the act is punishable as a theft.

Cybercrime might be also aggravated (Criminal Code 36:2). A person commits the crime if the fraud (1) involves the seeking of considerable benefit, (2) causes considerable or particularly significant loss, (3) is committed by taking advantage of special confidence based on a position of trust or (4) is committed by taking advantage of a special weakness or other insecure position of another, and the fraud is aggravated also when assessed as a whole. In addition, an attempt of aggravated fraud is punishable.

By using information technology, it is possible to commit the essential elements of a forgery crime (Criminal Code 33:1). A person who prepares a false document or other item in order for it to be used as misleading evidence, or who uses a false or falsified item as misleading evidence, shall be sentenced for forgery.

The definition in Criminal Code Chapter 33 section 6 extends punishability outside of the paper-based documents. For the purposes of Penal Code, an item refers to a document and its facsimile, a mark, a stamp, license plate, audio or video re-

6 Pihlajamäki 2004, p. 191–213.

cording, a recording produced by a plotter, calculator or other comparable technical device and a recording that is suitable for data processing if it is used or can be used as legally relevant evidence of rights, duties or facts.

An item is false if, when used as evidence, it is conductive to giving a misleading conception of its origin or of the identity of the person who issued it. An item is falsified if its contents have been unlawfully altered in respect of a datum that has probative relevance. In addition, aggravated and petty forgery are legislated in the Criminal Code Chapter 33 sections 2 and 3. These essential elements as well as the criminalization of possession of forgery materials are possible to implement in the online environment by taking into account the definition of the regulation. The provisions on corporate criminal liability apply to forgery, aggravated forgery and possession of forgery instruments (Criminal Code 33:7).

Business espionage has been legislated as punishable in the Criminal Code Chapter 30 section 4. A person who unlawfully obtains information regarding the business secret of another (1) by entering an area closed to unauthorized persons or accessing an information system protected against unauthorized persons, (2) by gaining possession of or copying a document or other record, or in another comparable manner, or (3) by using a special technical device with the intention of unlawfully revealing this secret or unjustifiably utilizing it shall, unless a more severe penalty has been provided elsewhere in law for the act, be sentenced for business espionage.

One of the most significant actions is penetration to the files where the offender has no right to access. In addition, other business secrets, which are enacted in Criminal Code Chapter 30, are usually carried out by using the network environment.

The provision of Criminal Code Chapter 28 section 7 of unauthorized use was perhaps the first criminal *corpus delicti* applied to the illegal computer network. Unauthorized use has been legislated in the following way: A person who without authorization uses the movable property or the non-movable machine or equipment of another shall be sentenced for unauthorized use to a fine or to imprisonment for at most one year. An attempt is punishable. Use of an Internet connection through an unprotected wireless computer network is not deemed unauthorized use.

Criminal Code Chapter 37 section 8 legislates of means of payment fraud. The act has been determined as following: A person who in order to obtain unlawful economic benefit for himself or herself or another (1) uses a means of payment without the permission of the lawful holder, in excess of his or her right based on such permission, or otherwise without lawful right, or (2) transfers a means of payment or means of payment form to another in order to have it used without lawful rights shall be sentenced for means of payment fraud. In addition the law prescribes as punishable the exceeding of an account holder's credit limits or cover of an account. Means of payment refers to bank cards, debit cards, credit cards, checks and other objects and records which can be used in payment or for withdrawal or account transfer, or the use of which is essential for this purpose (Criminal Code 37:12) .

6 Information Technology and Sex Offences

Sexual offenders have found an operating environment in an information network. The Finnish Criminal Code Chapter 20 legislates on sex offences. Criminal Code Chapter 17 also prescribes essential elements where acts with a strong sexual stamp have been criminalized.

According to the Criminal Code Chapter 17 section 18 a person who manufactures, offers for sale or for rent or otherwise offers or makes available, keeps available, exports, imports to or transports through Finland to another country or otherwise distributes pictures or visual recordings that factually or realistically depict (1) a child, (2) violence or (3) bestiality shall be sentenced for *distribution of a sexually offensive picture*. The aggravated form of the offence has been legislated in Criminal Code Chapter 17 section 8a. Punishable is also illegal exhibition or distribution of video programs to a minor under 18 years old (Criminal Code 17:18b) and possession of a sexually offensive picture depicting a child (Criminal Code 17:19). These crimes are increasingly being revealed in the online environment.

Criminal Code Chapter 20 section 6 and 7 legislates on sexual abuse of a child and aggravated sexual abuse of a child. The punishability of sexual abuse of a child has been defined as following: A person who by touching or otherwise performs a sexual act on a child below the age of 16 years, said act being conducive to impairing his or her development, or induces him or her to perform such an act, shall be sentenced for sexual abuse of a child. The sexual act has been defined in Criminal Code Chapter 20 section 10 subsection 2 as follows: For the purposes of this Act, a sexual act refers to an act which, with consideration to the offender, the person at whom the act was directed and the circumstances of commission, is sexually significant. The essential elements of the crime are possible to implement in the network environment. The Supreme Court has taken a stand on sexual abuse of a child in the network in two quite new precedents.

In the Supreme Court case (KKO 2017:51)[7] offender (A) was active on the Internet with several false profiles and had sexual conversations with 18 children aged 10-15 years. Offender (A) had asked the children to send intimate photos of themselves or to use a webcam to film themselves. In two cases offender (A) had received nude pictures, which he had saved on his computer. In addition, offender (A) had shared pornographic pictures on the Internet. In this case, (A) had committed 21 different offences, and it was the task of the Supreme Court to only decide on the question of just punishment. The Supreme Court decided to sentence (A) for conditional imprisonment to one year and one month. There has been no evaluation in the Supreme Court decision about the sexual abuse of a child which has taken place via the Internet and mainly through words and speech. From this point of view, this is a significant precedent. However, the most interesting issue about this article is in an analysis of what (A) had done. This is a very typical case of the sexual abuse of a child that has been revealed in the online environment.

Over three years and nine months (A) had sent over 1800 messages in different chat forums to 18 children. At the minimum, children had received messages on only one day and at the maximum on over 50 different days. Typically, offender (A)'s connection with one child lasted about five months and contained nearly 100 messages. At any one time (A) had had contact with 4 to 7 different children. He started a conversation with new children after a former contact had ended. At the time of offender (A)'s first contact, one of the children had been 10 years old, one 11 years old, three 12 years old, four 13 years old, six 14 years old and three 15 years old. The detailed description of the actions is given in paragraphs 2 to 6 in the Supreme Court judgment. The acts had been varied in their blameworthiness and intensity.

The Supreme Court had based punishment on paragraph 4 in the judgment and considered that a fair punishment for the act would be seven months in prison. In

7 Matti Tolvanen: Rangaistuslajin valinta lapseen kohdistuneessa seksuaalirikoksessa, KKO:n ratkaisut kommentein II/2017.

committing this very serious offence, offender (A) had sent messages about sexual interaction via Internet chat forums to children aged 12-15 in the time period between 8 May 2009 and 17 March 2012. When sending messages (A) had posed as five different people: a young girl, a woman over 30 years old, a man and two different teenage boys. The child was not aware that she had been discussing with the same person all the time. Offender (A) had described in detail the sexual acts he could perform with the child in his messages. In addition, offender (A) had made the child send similar messages to him, and after that he had made the child send naked pictures of herself to show him or herself partly naked on the webcam. Offender (A) had also sent nude pictures to the child.

In the Supreme Court case (KKO 2017:50) concerned the interpretation of the essential elements of sexual abuse of a child. The age and relationship between the offender and victim will have an impact on what kind of act can be considered sexually essential or sexual in general (HE 6/1997 vp 189). In this case 32-year-old (B) and a 13-14-year-old and a 15-year-old had been in conversation without knowing each other and without prior conversation. The discussion forum had been an Internet site where sometimes issues of sexuality might be discussed. Offender (B)'s messages had contained (point of charge 18 and 21) direct proposals for sexual intercourses, intimate inquiries and direct references to sexual acts.

Offender (B)'s messages had been extremely personal from both children's point of view because the messages had contained descriptions of the sexual acts which (B) would like to do to the child or what he wanted the child to do to him. From the beginning of the conversation (B) started to discuss about the sexual experiences of all children and would return repeatedly to the subject. The discussions had been thoroughly sexually charged and were started and directed by offender (B). Thus, the acts of (B) had to be considered sexually essential. The Supreme Court considered that (B) had to be able to understand the possible detrimental effects on children by the content, tone and personality of the messages. The actions of offender (B) are conductive to harming the development of both children. (B) committed sexual abuse of a child.

In the Criminal Code Chapter 20 section 8b there has been enacted as punishable the preparation for the commission of sexual abuse of a child, which is solicitation of a child for sexual purposes. It has been determined as following: A person who suggests a meeting or other contact with a child so that it is apparent from the contents of the suggestion or otherwise from the circumstances that the intent of the person is to prepare sexually offensive pictures or visual recordings of the child in the manner referred to in Chapter 17 section 18 subsection 1, or to subject the child to the offence referred to in section 6 or 7 of this Chapter, shall be sentenced for solicitation of a child for sexual purposes. Unless a more severe sentence is provided in law for the act, also a person who solicits a person below the age of 18 years to engage in sexual intercourse or in another sexual act in the manner referred to in section 8(a) or to perform in a sexually offensive organized performance shall be sentenced for solicitation of a child for sexual purposes.

In the Supreme Court, case (KKO 2017:50) was also a question about the interpretation of Criminal Code Chapter 20 section 8b. According to the provision, solicitation of a child for sexual purposes is about criminal offence, which temporarily precedes attempts of sexual and other crimes, which are mentioned in the essential elements. The Supreme Court considered that the proposal or any other interaction must be concrete by nature in the provision. From the proposal or other circumstances should transpire the date and place of the meeting. Based on the information it should be pointed out that the meeting is not improbable or fulfilling the plan is not

practically impossible. It is already punishable if the offender has proposed intercourse. The purpose of the offender should come out from the external and objectively detectable circumstances.

The Supreme Court explained by using paragraph 18 in the ruling on offender (B)'s act. The Supreme Court considered that the details of personally planned appointments were defined sufficiently concretely to fulfil the essential elements. Instead, the Supreme Court dismissed the prosecution as far as the question was about offender (B)'s suggestion to discuss with the child via web camera. It was still unclear whether the child had the tools required for the webcam connection.

In the Criminal Code Chapter 20 section, 8c enacts the punishability following a sexually offensive performance of a child. A person who follows an organized performance, in which a person below the age of 18 years performs in a sexually offensive manner, shall be sentenced for following a sexually offensive performance of a child.

7 The Protection of Honour and Privacy in Network

People's increasing activity in the network environment has led to situations where the police receive new types of network crimes to investigate. There are cases where a single person or a whole group of people has been threatened, bashed or slandered. Ethnic agitation has been legislated as punishable in the Criminal Code Chapter 11 Section 10 (aggravated form of the crime in Section 10a). The essential elements of Chapter 11 in the Criminal Code are as follows: A person who makes available to the public or otherwise spreads among the public or keeps available for the public information, an expression of opinion or another message where a certain group is threatened, defamed or insulted on the basis of its race, skin colour, birth status, national or ethnic origin, religion or belief, sexual orientation or disability or a comparable basis, shall be sentenced for ethnic agitation.

The Supreme Court has one preliminary ruling of applying the essential elements (KKO 2012:58). Offender (A) had published on his own internet site a post which had an insulting statement concerning Islam and Muslims. The prosecutor's indictment was based on following statements: 'Prophet Muhammad was a pedophile, and Islam as a religion is sanctifying pedophilia, so it is a pedophile religion. Pedophilia is the will of Allah.'

The Supreme Court considered that the abusive and blasphemous statements could easily raise intolerance, scorn and even possible anger towards the ethnic group concerned in the statements. Those statements are then understood as statements similar to so-called hate speech, which does not deserve being protected under freedom of speech. It is justified to target the presenter of such statements with criminal consequences. Thus, (A) was found guilty of ethnic agitation.

The Supreme Court considered that the abusive allegations such as those (A) had posted were not authorized by offender (A)'s claimed purpose of sorting out the boundaries of free speech or the authorities' inconsistent actions. It would have been possible to present even strong critique concerning these questions without dishonouring Islam's holy values. The concerned, blasphemous slogans, which mark the whole religious group and its sanctified subjects very negatively, are not promoting conversation about religions or social questions, and instead they promote and strengthen religious intolerance and prejudice. To maintain public order and social

peace, it is justified to interfere with the presenter's freedom of speech in regard to the statements and apply criminal consequences.

Taking into consideration the contents of the statements and the way of presentation, Offender (A) had without doubt understood the blasphemous and defamatory nature of the statements. Also, in relation to offender (A)'s stated pursuit of testing the boundaries of free speech by 'throwing the bait' the prosecutor points out that (A) has understood that his statements will offend the Muslim's religious feelings in accordance with the essential elements. It also refers to a conscious act to offend as (A) has twice presented the statements with a specific style. Thus, when presenting the statements, (A) had acted according to the purpose to offend as stated in the Criminal Code Chapter 17 Section 10 and had perpetrated the violation of faith.

In one case, the Kouvola Court of Appeal (2012:9) has the task to interpret the meaning of Criminal Code Chapter 11 section 10. Offender (A) had posted a blog post online and said that Muslim immigration causes more robbery, drugs, rape, pedophilia and even terrorism. The text was general and discriminative because it was directed towards all Muslims and not just extremists, and as such the whole population was considered to be criminals and bad towards others. The text alleged that for these uncontrolled reasons Muslim immigration would have negative impacts.

According to offender (A), he wanted to speak out about immigration with his writing. The Court of Appeal considered that the writing does not bring out the problems in a proper tone and instead has caused problems, which are involved with immigration as a negative phenomenon. Such expressions are conductive to an increase intolerance, disdain and even anger towards Muslims.

It could be argued that the topic of the article raised interest among the public and was a political statement, therefore it should be considered more allowable. However, taking into consideration the principles of the European Court of Human rights' (ECHR) recommended decisions, the article did not stay within the limits of the freedom of expression concerning strict criticism of immigration policy. Offender (A)'s position, as a politician did not reduce his responsibility. Labelling a whole population as criminal is not a permitted provocation within the limits of the freedom of speech.

Due to the earlier mentioned reasons, the Court of Appeal considered that the writing was conductive to cause contempt, intolerance and even anger towards Muslims. Thus, in the writing, (A) had replied and disparaged Muslims and the text fulfils the elements of an incitement crime.

The online environment appears to be a good seedbed for crimes violating honour and a person's private life. The basic rule of criminalization regarding the violating of private life is legislated in Criminal Code Chapter 24 section 8. It enacts as punishable the dissemination of information violating personal privacy as follows: A person who unlawfully (1) through the use of the mass media, or otherwise by making available to many persons disseminates information, an insinuation or an image of the private life of another person, so that the act is conducive to causing that person damage or suffering, or subjecting that person to contempt, shall be sentenced for dissemination of information violating personal privacy to a fine; (2) the spreading of information, an insinuation or an image of the private life of a person in politics, business, public office or public position, or in a comparable position, does not constitute dissemination of information violating personal privacy if it may affect the evaluation of that person's activities in the position in question and if it is necessary for purposes of dealing with a matter of importance to society; and (3) presentation of an expression in the consideration of a matter of general importance shall also not be considered dissemination of information violating personal privacy

if its presentation, taking into consideration its contents, the rights of others and the other circumstances, does not clearly exceed what can be deemed acceptable.

This provision is also supplemented by the essential elements of defamation in the online environment (Criminal Code 24:9). Defamation shall be committed if a person (1) spreads false information or a false insinuation of another person so that the act is conducive to causing damage or suffering to that person, or subjecting that person to contempt, or (2) disparages another in a manner other than referred to in the paragraph. Criticism that is directed at a person's activities in politics, business, public office, public position, science, art or in a comparable public activity and that does not obviously exceed the limits of propriety does not constitute defamation. Presentation of an expression in considering a matter of general importance shall also not be considered defamation if its presentation, taking into consideration its contents, the rights of others and the other circumstances, does not clearly exceed what can be deemed acceptable.

Does a person who combines two individually public cases together commit a crime? Let us think about a case, where offender (A) has performed his prison sentence for a rape crime. The judgment is public; at least the part concerning the judicial decision. Offender (B) obtains the judgment by ordering it from the District Court. Let us assume that at the time of the judgment, the media has widely exaggerated about the case, and the media has revealed the name of the convicted person. Offender (A) has also published his picture on his Facebook profile. Now (B) combines the judgment with the picture and starts to share the judgment combined with the picture on his own Facebook post. At least in one case the Court of Appeal has stated that (B) has committed a criminal act, although the information he shared was public (Court of Appeal of Eastern Finland 16.2.2016 R 15/677). It was essential in the case that (A) had already reconciled the crime, and it seems that offender (B)'s motive was to make people despise (A), although (B) justified his actions by saying he was protecting potential victims.

The network environment unfortunately seems to suit well the use of harassing communications (Criminal Code Chapter 24 Section 1a). In the Criminal Code, it is described as follows: 'a person who, with intent to disturb, repeatedly sends messages or calls another so that the act is conducive to causing said other person considerable disturbance or harm, shall be sentenced for *harassing communications*.' This kind of procedure can also fulfil the essential elements of *stalking* (Criminal Code Chapter 25 Section 7a). A person who repeatedly threatens, observes, contacts or in another comparable manner unjustifiably stalks another so that this is conducive towards instilling fear or anxiety in the person being stalked perpetrates stalking.

SENTENCING OF CYBERCRIMES IN FINLAND

Mika Sutela

1 Introduction

Cybercrime is the threat of the bit world which touches our everyday lives.[1] The number of cybercrimes has significantly increased in Finland over the last few years. As Näsi and Tanskanen (2017) state, cybercrime is not an actual legal term but an umbrella term often used in the empirical research for all online crime and criminal behaviour.[2] The spectrum of criminal acts considered as cybercrimes is wide.[3] A thumb rule is, in principle, that different forms of cybercrime are committed or take place in the electronic information system environment.[4] Among the key elements of cybercrime are internationality and anonymity.[5] Online crime is often international because, unlike many conventional crimes, the internet does not have certain physical limitations.[6]

Cybercrime can be defined as crimes that can be committed through the use of information communications technology devices, where the devices are both the tool for committing the crime and the target of the crime; or traditional crimes which are changed significantly by information communications technology in terms of scale and reach.[7]

A big part of cybercrime is based on the so–called traditional crime types such as fraud, threatening behaviour and sexual harassment with the difference that the criminal act has taken place online or by other way using information and communication technology.[8] Property crime is one of the most common cyber–related crimes. Most such crimes are fraud and means of payment offences, but for example money laundering is also included in this category.[9]

Over recent decades an increasing number of cases involving cybercrime have been reported to the police and have come before the courts.[10] It is important, however, to notice that the number of cybercrimes that actually take place and the number

1 J. Limnell, 'Kyberrikollisuus on liian helppoa', Blog of Sitra, 12 December 2013. Available at https://www.sitra.fi/blogit/kyberrikollisuus-liian-helppoa/ (last visited 3 November 2017).

2 M. Näsi and M. Tanskanen, 'Kyberrikollisuus', in *Rikollisuustilanne 2016. Rikollisuuskehitys tilastojen ja tutkimusten valossa.* (Katsauksia 22/2017. Helsingin yliopisto, Kriminologian ja oikeuspolitiikan instituutti), available online at https://helda.helsinki.fi/handle/10138/191756 (visited 22 September 2017), 147–159 at 147.

3 See, e.g. M. Yar, *Cybercrime and Society*. (2nd edn., Sage Publications Ltd., 2013).

4 Näsi and Tanskanen, *supra* note 2, at 147.

5 Ibid., at 147.

6 Ministry of the Interior, Finland, 'Information networks and crime', available at http://intermin.fi/en/police/cybercrime (last visited 2 November 2017).

7 *National risk assessment of money laundering and terrorist financing 2017*, Policy paper, HM Treasury, Home Office, available online at https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017 (visited 9 October 2017), 21–22.

8 Näsi and Tanskanen, *supra* note 2, at 147.

9 Ministry of Interior, *supra* note 6.

10 See R. G. Smith, 'Cyber Crime Sentencing: The Effectiveness of Criminal Justice Responses', Conference paper. Crime in Australia: International Connections. Australian Institute of Criminology International Conference. Hilton on the Park, Melbourne, Australia, November 2004, available online at http://www.aic.gov.au/media_library/conferences/2004/smith.pdf. (visited 10 October 2017).

that are reported to the police are far more than the number that go to court.[11] Most cybercrime is not reported to the police and most offences that the police investigate remain unsolved or are only partly solved.[12] Only a small part of online cybercrime will come to the attention of the police.[13]

Nicole Roberts (2014) states that legislation has not been able to keep pace along with the rapid advance of technology, and there is a great deal of ambiguity on how the perpetrators of cybercrimes should be punished. Some people argue that the sentences for cybercrimes are far too lenient; this often allows criminals to profit from their offences and fails to deter other criminals from committing similar crimes.[14]

The aim of this article is to examine the sentencing of cybercrimes. On a more specific level, punishments for cybercrimes and cyber-related crimes sentenced by Finnish district courts in 2010–2016 are examined from a quantitative point of view. The examination is descriptive in nature. The data source is Tilastokeskus (Statistics Finland).

Following this introduction, chapter 2 presents Finnish criminal legislation for cybercrimes and sentencing. In chapter 3 the sentencing practice of cybercrimes in Finnish District Courts in the 2010s is described based on the official Finnish justice statistics. Chapter 4 concludes the article.

2 Criminal Legislation

2.1 Cybercrimes

This chapter presents a general overview of the Finnish legislation of cybercrimes. The offences include the following:

- Defamation (24:9 §)
- Aggravated defamation (24:10 §)
- Money laundering (32:6.1 §)
- Aggravated money laundering (32:7.1 §)
- Fraud (36:1.1-2 §)
- Aggravated fraud (36:2.1 §)
- Means of payment fraud (37:8 §)
- Aggravated means of payment fraud (37:9 §).
- Interference with communications (38:5.1 §),
- Interference in an information system (38:7a.1 §) and
- Computer break-in (38:8.1-2 §).

11 Ibid., at 3.
12 Ministry of Interior, *supra* note 6.
13 Näsi and Tanskanen, *supra* note 2, at 149.
14 N. Roberts, 'Cybercrimes: Does the Punishment Actually Fit the Crime?' *Law Street Media* (2014), available at https://lawstreetmedia.com/blogs/crime/cybercrimes-punishment-actually-fit-crime/ (visited 3 November 2017).

The last three offences are traditionally considered as cybercrimes, but nowadays there are also online variations of 'old' offline crimes. These crimes include offences against reputation, money laundering offences, fraud and means of payment offences. For example, as Kerr et al. (2013) state, frauds committed online can also be similar to those that have traditionally been committed offline.[15]

Next, the relevant sections of the Criminal Code of Finland (39/1889)[16] are presented in order to understand better the sentencing practice. Penalty scales give the framework according to which the punishment for each offence should be sentenced in accordance with Finnish legislation. The sections are as follows:

Defamation (24:9 §, 879/2013)

A person who

(1) spreads false information or a false insinuation of another person so that the act is conducive to causing damage or suffering to that person, or subjecting that person to contempt, or

(2) disparages another in a manner other than referred to in paragraph (1) shall be sentenced for *defamation* to a fine.

Also a person who spreads false information or a false insinuation about a deceased person, so that the act is conducive to causing suffering to a person to whom the deceased was particularly close, shall be sentenced for defamation.

Criticism that is directed at a person's activities in politics, business, public office, public position, science, art or in comparable public activity and that does not obviously exceed the limits of propriety does not constitute defamation referred to in subsection 1(2).

Presentation of an expression in the consideration of a matter of general importance shall also not be considered defamation if its presentation, taking into consideration its contents, the rights of others and the other circumstances, does not clearly exceed what can be deemed acceptable.

Aggravated defamation (24:10 §, 879/2013)

If, in the defamation referred to in section 9(1), considerable suffering or particularly significant damage is caused and the defamation is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated defamation* to a fine or to imprisonment for at most two years.

Money laundering (32:6.1 §, 191/2011)

A person who

(1) receives, uses, converts, conveys, transfers or transmits or possesses property acquired through an offence, the proceeds of crime or property replacing such property in order to obtain benefit for himself or herself or for another or to conceal or oblit-

15 J. Kerr et al., 'Research on Sentencing Online Fraud Offences', Sentencing Council, June 2013, available online at https://www.sentencingcouncil.org.uk/wp-content/uploads/Research_on_sentencing_online_fraud_offences.pdf (visited 3 November 2017), at 26.

16 Ministry of Justice, Finland: 'The Criminal Code of Finland (39/1889, amendments up to 766/2015 included)', (Translation from Finnish. Legally binding only in Finnish and Swedish) available online at http://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf (visited 6 September 2017).

erate the illegal origin of such proceeds or property or in order to assist the offender in evading the legal consequences of the offence or
(2) conceals or obliterates the true nature, origin, location or disposition of, or rights to, property acquired through an offence, the proceeds of an offence or property replacing such property or assists another in such concealment or obliteration, shall be sentenced for *money laundering* to a fine or to imprisonment for at most two years.

Aggravated money laundering (32:7.1 §, 61/2003)

If in the money laundering
(1) the property acquired through the offence has been very valuable or
(2) the offence is committed in a particularly intentional manner,
and the money laundering is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated money laundering* to imprisonment for at least four months and at most six years.

Fraud (36:1.1-2 §, 769/1990)

A person who, in order to obtain unlawful financial benefit for himself or herself or another or
in order to harm another, deceives another or takes advantage of an error of another so as to have this person do something or refrain from doing something and in this way causes economic loss to the deceived person or to the person over whose benefits this person is able to dispose, shall be sentenced for *fraud* to a fine or to imprisonment for at most two years.

Also a person who, with the intention referred to in subsection 1, by entering, altering, destroying or deleting data or by otherwise interfering with the operation of a data system, falsifies the end result of data processing and in this way causes another person economic loss, shall be sentenced for fraud. (514/2003)

Aggravated fraud (36:2.1 §, 769/1990)

If the fraud
(1) involves the seeking of considerable benefit,
(2) causes considerable or particularly significant loss,
(3) is committed by taking advantage of special confidence based on a position of trust or
(4) is committed by taking advantage of a special weakness or other insecure position of another
and the fraud is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated fraud* to imprisonment for at least four months and at most four years.

An attempt is also punishable.

In the United Kingdom, Experimental Statistics from the CSEW estimated that there were 3.3 million incidents of fraud in the survey year ending June 2017, with over half of these (57 %) being cyber related, i.e. such as the internet or any type of online activity was related to any aspect of the offence.[17]

17 Office for National Statistics, 'Crime in England and Wales: year ending June 2017 – Crime against households and adults, also including data on crime experienced by children, and crimes against businesses and society', Statistical bulletin (2017), at 15.

Means of payment fraud (37:8 §, 769/1990)

A person who in order to obtain unlawful economic benefit for himself or herself or another

(1) uses a means of payment without the permission of the lawful holder, in excess of his or her right based on such permission, or otherwise without lawful right, or

(2) transfers a means of payment or means of payment form to another in order to have it used without lawful right

shall be sentenced for *means of payment fraud* to a fine or to imprisonment for at most two years. (602/1997)

Also a person who, by overdrawing his or her account or exceeding the agreed maximum credit limit, misuses a means of payment referred to in subsection 1 and in this way causes economic loss to another shall be sentenced for *means of payment fraud*, unless when using the means of payment he or she intended to compensate the loss without delay.

Aggravated means of payment fraud (37:9 §, 769/1990)

If in the means of payment fraud

(1) considerable or particularly significant loss is caused or

(2) the offender has, for the commission of the offence, made or had made means of payment forms from which the means of payment used in the offence was prepared, or if the offence is otherwise committed in a particularly methodical manner

and the means of payment fraud is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated means of payment fraud* to imprisonment for at least four months and at most four years.

Interference with communications (38:5.1 §, 578/1995)

A person who by tampering with the operation of a device used in postal, telecommunications or radio traffic, by maliciously transmitting interfering messages over radio or telecommunications channels or in another comparable manner unlawfully prevents or interferes with postal, telecommunications or radio traffic, shall be sentenced for *interference with communications* to a fine or to imprisonment for at most two years.

Interference in an information system (38:7a.1 §), 368/2015)

A person who in order to cause detriment or economic loss to another, by entering, transferring, damaging, altering or deleting data or in another comparable manner unlawfully prevents the operation of an information system or causes serious interference in it shall be sentenced for *interference in an information system* to a fine or to imprisonment for at most two years.

Computer break-in (38:8.1-2 §), 368/2015)

A person who by using an access code that does not belong to him or her or by otherwise breaking a protection unlawfully hacks into an information system where infor-

mation or data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a *computer break-in* to a fine or to imprisonment for at most two years. Also a person who, without hacking into the information system or a part thereof,

(1) by using a special technical device or

(2) otherwise by by-passing the system of protection in a technical manner, by using a vulnerability in the information system or otherwise by evidently fraudulent means unlawfully obtains information or data contained in an information system referred to in subsection 1

shall be sentenced for a computer break-in.

2.2 Sentencing

Sentencing is theoretically interesting and practically a really important subject. The passing of a sentence on an offender is the public stage of the criminal procedure.[18] Hough and Roberts (2012) state that sentencing represents the heart of the criminal procedure, and that it is the element of the criminal justice system that attracts most media and public interest. Sentencing is most likely to come into a person's mind when they think about criminal justice.[19]

Chapter 6 of the Criminal Code of Finland concerns sentencing. In Finland the general type of punishments are summary penal fine, fine[20], conditional imprisonment, community service, monitoring sentence and unconditional imprisonment (6:1.1 §). Community service and a monitoring sentence can be imposed instead of unconditional imprisonment under certain conditions.

When there is a need to select, the choice between conditional and unconditional imprisonment is made by the Criminal Code as follows: a sentence of imprisonment for a fixed period not exceeding two years may be conditional (conditional imprisonment), unless the seriousness of the offence, the guilt of the offender as manifested in the offence or the criminal history of the offender requires the imposition of an unconditional sentence of imprisonment (6:9.1 §).

In sentencing, all grounds according to law affecting the amount and type of punishment, as well as the uniformity of sentencing practice, are taken into account (6:3.1 §). The general principle in Finnish sentencing is that the sentence shall be determined so that it is in just proportion to the harmfulness and dangerousness of the offence, the motives for the act and the other culpability of the offender manifest in the offence (6:4 §).

---

18 A. Ashworth and J. Roberts, 'Sentencing: theory, principle, and practice', in M. Maguire, R. Morgan, and R. Reiner (eds.), *The Oxford Handbook of Criminology* (5th edn., Oxford: Oxford University Press, 2012) 866–894, at 866.

19 M. Hough and J. V. Roberts. 'Public Opinion, Crime, and Criminal Justice', in M. Maguire, R. Morgan, and R. Reiner (eds.), *The Oxford Handbook of Crminology*. (5th edn., Oxford: Oxford University Press, 2012) 279–297, at 285.

20 A fine is imposed as day-fines (or unit fines). For instance, 20 day-fines at EUR 10 each equal to EUR 200. The more blameworthy the act, the more day-fines are imposed. The statutory maximum number of day-fines is 120 or, if the fine is imposed for several offences, 240. There is no general, statutory minimum number of day-fines to be imposed, but for certain offences a minimum amount has been determined. The amount of one day-fine depends on the income of the convict. The amount of a day-fine is based on a person's net income. The minimum amount of a day-fine is EUR 6. See Oikeus.fi, Fine, available at: https://oikeus.fi/tuomioistuimet/karajaoikeudet/en/index/rikosasiat/seuraamukset/sakko.html (visited 3 November 2017).

3 Sentencing Practice of Cybercrimes

For several decades criminal sentencing has been an active research field.[21] There are so far very few studies that have examined cybercrime sentencing. Marcum et al. (2011) found that the female cybercrime offenders are more likely to receive longer sentences for their crimes compared to males. They also examined how the type of cybercrime affects the sentence length. Their results indicated that offenders who committed identity theft, cyber fraud or destruction of property were more likely to get lengthier sentences compared to other cybercrime offenders. The findings indicate that sentencing practices place strong emphasis on punishment of cybercrime offenders whose crimes involve violation of privacy and serious financial loss. From these results it is also possible to see that cybercrime offenders who commit offences that potentially effect multiple victims in very damaging ways (i.e. use of personal information to falsely obtain money and property, destruction of credit history) are being sentenced harshly.[22]

According to Marcum et al. (2012) gender was not shown to be a predictive factor in regard to type of sentence for cybercrime offenders. The findings of the study indicated that previous violent offence and public order offence convictions were more likely to receive a prison sentence.[23]

In regard to sentencing fraud offences, for example, there is really limited research literature at the international level. Levi (2010) states that fraud cases seldom attract severe sanctions.[24] Kerr et al. (2013) found that the offline or online nature of the method of fraud made no difference to the seriousness of the offence and how it should be viewed for sentencing purposes. It was felt that regardless of the method used, the crime is the same.[25]

Bo Williams (2016) reports that judges are struggling to determine the appropriate punishments for cybercrimes. Cybercrime is such a recent phenomenon that there are few guideposts for judges to use.[26]

There is so far no research on sentencing practice of cybercrime in Finland. No information is available at the individual level about what kind of factors influence the sentencing of cybercrime. We can only ask if cyber-related crimes are judged similarly or differently than traditional offline offences.

With the help of the statistics from Tilastokeskus[27] it is possible to get some information by using them as guidelines, based on the aggregate data, to find what kind of punishments have typically been given for cyber-related crimes. Here the sentencing practice is examined during the 2010s. Table 1 presents criminal offences, sum of people sentenced for the offences in the district courts in 2010–2016 and typical sentences imposed.

---

21 J. T. Ulmer, 'Recent Developments and New Directions in Sentencing Research', 29 *Justice Quarterly* (2012) 1–40, at 1.

22 C. D. Marcum et al., 'Doing Time for Cyber crime: An Examination the Correlates of Sentence Length in the United States', 5 *International Journal of Cyber Criminology* (2011) 825–835.

23 C. D. Marcum et al., 'Incarceration or community placement: examining the sentences of cybercriminals', 25 *Criminal Justice Studies* (2012) 33–40.

24 M. Levi, 'Hitting the suite spot: sentencing frauds', 17 *Journal of Financial Crime* (2010) 116–132.

25 Kerr et al., *supra* note 15, at 59.

26 K. Bo Williams, 'Judges struggle with cyber crime punishment', *The Hill*, September 2016, available at http://thehill.com/policy/cybersecurity/265285-judges-struggle-with-cyber-crime-punishment (visited 3 November 2017).

27 Statistics Finland, 'Prosecutions, sentences and punishments' (Official Statistics of Finland, Helsinki, 2017) available at http://www.stat.fi/til/syyttr/index_en.html (visited 27 October 2017).

According to Tilastokeskus' statistics different forms of fraud offences have been really common. In contrast, data and communications offences are still very rare in Finnish District Courts.

Except in regard to money laundering, the most typical punishment has been a fine for the basic forms of offence. In the case of an aggravated form of offence the most typical punishment has been conditional imprisonment.

Data and communications offences, i.e. the 'original' cybercrimes, have been judged rather similarly as other offences including cybercrimes. According to the statistics, the most severe sentencing practice has been in regard to aggravated money laundering offences. That is consistent with the theoretical penalty scales in law.

Table 1. Criminal offences, amount of people sentenced for the offences in the district courts in 2010–2016 and typical sentences imposed.

Offence	N (2010-2016)	Typical punishment
Defamation (24:9 §)	1213	Fine (95 %), 25 day-fines
Aggravated defamation (24:10 §)	94	Conditional imprisonment (43 %), 3 months
Money laundering (32:6.1 §)	236	Conditional imprisonment (43 %), 3 months
Aggravated money laundering (32:7.1 §)	133	Conditional imprisonment (79 %), 8 months
Fraud (36:1§1-2)	14104	Fine (59 %), 40 day-fines
Aggravated fraud (36:2§1)	2174	Conditional imprisonment (73 %), 7 months
Means of payment fraud (37:8 §)	2664	Fine (45 %), 40 day-fines
Aggravated means of payment fraud (37:9 §)	454	Conditional imprisonment (60 %), 7 months
Interference with communications (38:5.1 §)	44	Fine (52 %), 40 day-fines
Interference in an information system (38:7a.1 §)	4	Fine (75 %), 100 day-fines
Computer break-in (38:8.1-2 §)	19	Fine (95 %), 25 day-fines

4 Conclusion

This article has shortly examined the sentencing of cybercrimes. As Roberts (2014) has already found out, cybercrime sentencing is an issue that needs a lot more exploration than it has been given. Cybercrimes fail to be contained within traditional modes of sentencing, and often the sentences given seem to be too severe or too lenient to fit the crime. Although much attention has been given up to the subject of apprehending, detecting and prosecuting cybercriminals, more attention needs to be paid to what happens next.[28]

There are a limited number of cybercrime convictions compared to other crimes, so it will take time before there are enough cases on which one can confidently say something with authority about the sentencing of cybercrime. For Finland, this is a good start, and the official statistics are better than nothing. They give some background and provide understanding about the kind of cybercrime sentencing practices we have.

28 Roberts, *supra* note 14.

An increased focus on investigating and prosecuting cybercrimes has placed added pressure on the legal system to assess responsibility appropriately and to mete out punishments that act as a deterrent.[29] That is why, for example, it is really important to get more research and information about cybercrime sentencing in the future.

29 Bo Williams, *supra* note 26.

CYBER FRAUD AS CYBERCRIME*

Jussi Tapani

1 Introduction

There is extensive literature addressing such questions as what is meant by 'cybercrime', what the actual scope, scale and damage of such crimes is, who cybercriminals are and what the most effective measures to prevent cybercrime etc. would be.[2] This is because our understanding of these issues and problems depends both on our perception of the environment in which these crimes are committed *and* the social and political responses to those problems.[3] The non-legislative resolution approved by the European Parliament in October 2017 may serve as an illuminating example concerning the political commitment to combatting cybercrime. The Members of European Parliament (MEPs) were almost unanimous that 'The EU must invest more in cybersecurity to prevent attacks aimed at critical infrastructure and destabilising societies'.[4] Another relevant example is the statement of the City of London regarding the opening of a new state-of-the-art court to tackle cybercrime and fraud in the financial sector.[5]

Although there are good reasons to be cautious and not overestimate the effectiveness of this kind of high-level statement, the statistics show that cybercrime is becoming an ever-increasing problem. Thus, at the top of the most common United Kingdom (UK) online offences, one finds bank account fraud and non-investment fraud,[6] and in Finland, the amount of fraud in the Internet context is steadily increasing.[7]

However, it seems almost impossible to find solid enough ground for a concept of cybercrime that would capture the diversity of this criminological interesting phenomenon. Thus, it is not surprising that the only multilateral legally binding instrument, the Council of Europe Convention on Cybercrime (CETS No 185), is unable

---

* This article is partially based on my earlier article on this issue. See J. TAPANI, 'Three generations of cyber fraud. Some reflections from the Finnish perspective', in C. CRESPO SANCHIS (ed.), *Fraude electrónico su gestión penal y civil*, (Valencia: Tirant monografías 2015), at. 255–266.

2 M. YAR, *Cybercrime and Society*, (2nd edn., London: SAGE Publications, 2013), at. 4–6 and D. WALL, *Cybercrime, The Transformation of Crime in the Information Age*, (Cambridge: Polity Press, 2007), at. 8–29.

3 Y. JEWKES and M. YAR, 'Introduction: the Internet, cybercrime and the challenges of twenty-first century', in Y. JEWKES and M. YAR, (ed.), *Handbook of Internet Crime*, (London and New York: Routledge, 2012), 1–8, especially at. 3–5.

4 http://www.europarl.europa.eu/news/en/press-room/20171002IPR85128/step-up-measures-to-prevent-cyber-attacks-and-online-sexual-abuse-urge-meps (visited 4 October 2017).

5 http://www.telegraph.co.uk/news/2017/10/08/city-londoncyber-court-tackle-online-fraud-financial-sector/ (visited 9 October 2017).

6 http://www.telegraph.co.uk/news/2017/10/08/city-londoncyber-court-tackle-online-fraud-financial-sector/. More information will be found http://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables (visited 9 October 2017).

7 http://www.poliisi.fi/tietoa_poliisista/tiedotteet/1/1/poliisin_vuosi_2016_rikosten_maara_pysytteli_edellisen_vuoden_tasolla_-_nettipetokset_jatkoivat_kasvuaan_56212 (visited 8 October 2017).

to provide an agreed conception of cybercrime.[8] If this is the state of affairs, does this not justify the claim that there is no hope of reaching consensus on the use of the concept of *cyber fraud*?

One could seek to tackle this problem by arguing, like *Majid Yar*, that it is useless to try to grasp cybercrime as a single element. He believes that it would be better to view the term as describing a range of illegal activities that have a common denominator, namely the central role played by networks of ICT in their commission.[9]

Another possibility would be to argue that we do not necessarily need a conceptual consensus in jurisprudence. Thus, more important than conceptual clarity and consensus would be the *context*, as this forms our understanding of certain phenomena and the way we use certain concepts. Therefore, according to Federal Bureau of Investigation (FBI), Internet fraud is defined as follows:

> "Internet fraud is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them. Internet crime schemes steal millions of dollars each year from victims and continue to plague the Internet through various methods … Frequent instances of Internet fraud include business fraud, credit card fraud, internet auction fraud, investment schemes, Nigerian letter fraud, and non-delivery of merchandise."[10]

I see no reason to underestimate this description, because it is relatively informative and able to capture the key features and types of cyber fraud. Nevertheless, a closer look at the definition used by the FBI reveals a conceptual problem. Why are the diverse other methods such as business e-mail compromise (BEC), data breach, denial of service, e-mail account compromise (EAC), malware/scareware, phishing/spoofing and ransomware not included under the concept of Internet fraud – even though one can readily find a short and good description of each of these?[11]

Therefore, for the purpose of this article I would rather make use of *Susan W. Brenner´s* description of cybercrime.[12] She points out that lawyers and law enforcement officers use this term to refer to crimes the commission of which involves the use of computer technology.[13] This conceptual framework divides cybercrimes into three subcategories: a) a computer is the target of the crime, b) a computer is the tool used commit a traditional crime, such as theft and fraud, and c) a computer plays an incidental role in committing one or more crimes. As *Jonathan Clough* pinpoints, we see here a three-stage classification of computer crimes, computer-facilitated crimes and computer-supported crimes.[14]

My interest lies mainly in the second subcategory, that is, cases in which a computer is the tool used to commit a traditional crime. I argue that there are problems enough to tackle even in the context of traditional fraud when a fraudster uses

8 However, the Convention includes some key definitions, such as ´computer system´, ´computer data´, ´service provider´, and ´traffic data´ (Article 1). Furthermore, crime types, i.e. offences, have been divided into subcategories, which reflects the aim of systematization (see especially articles 7–10).

9 YAR, *supra* note 1, at. 9.

10 https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud (visited 4 October 2017).

11 See *supra* note 6. See also https://www.ic3.gov/crimeschemes.aspx, where a wide range of current and ongoing Internet trends and schemes identified by the Internet Crime Complaint Center are listed along with their descriptions.

12 S. W. BRENNER, *Cybercrime and Law, Challenges, Issues, and Outcomes,* (Boston: Northeastern University Press, 2012), at. 14.

13 It is worth mentioning that this categorization is too limited in the criminological sense because it focuses on the technology rather than the relationship between offenders and their targets or victims. This important point is made by YAR *supra* note 1, at. 10.

14 J. CLOUGH, *Principles of Cybercrime*, (Cambridge: Cambridge University Press, 2010), at. 10. See also WALL *supra* note 1, at. 99.

a computer as a tool to commit fraud. Therefore, my aim is to explore (1) whether we need to rethink our perception of fraud in the cyber context, and, if the answer is positive, (2) what would be those elements in our perception that need rethinking?

This article is structured as follows. First, I will briefly describe three courses of events that will then form a descriptive basis for further analysis. Two of these courses of events are real criminal cases – the first is somewhat old, the second is rather new. My third example concerns a hypothetical course of events which could be of possible relevance to criminal law. Secondly, I will discuss the normative implications of these courses of events, that is, some criminal law and criminal procedure law-related problems that are connected to these examples. However, I do not seek to examine these problems comprehensively.

2 Three Generations of Cyber Fraud[15]

2.1. Online Auction Fraud

Fraud belongs to the most complex socio-legal phenomena of human society, which is illuminated very well in *Sissela Bok´s* book on lying, for example.[16] There are numerous ways of cheating another person or institution and recent changes in actual practices involving changes in communication and its structures have increased the opportunities for deception. Thus, the Internet has become an excellent platform and tool for committing fraud.[17] It is not an overestimation of the current state of affairs to claim that it is a paradise for those who seek the gullible, the greedy or the vulnerable.[18] Therefore, we have to understand not only the mechanism of the most common types of cyber fraud and how they are legally constructed but perhaps more importantly we need to know how to prevent these crimes as well.[19]

My first example belongs to the *first generation* of cyber fraud in the Internet context. Although the example may be seen as an old-fashioned and traditional way of defrauding people, it is a surprisingly common and effective way of defrauding. Furthermore, it is an excellent and revealing version of the basic fraud dynamic – deceiving someone into handing over money or property.[20] Thus, this example presents the subcategory of purchase fraud, that is, *auction fraud* (an online auction scheme). On the Internet there are many different websites, such as eBay, where people are able to buy and sell items in an auction; some of these sites are in some sense universal due to the language they are in being widely used, for instance English, whilst others are more restricted for the opposite reason: one of these more nationally restricted sites is located in Finland and is named "Huuto.net".[21]

The distinctive feature of auction fraud is that it "involves fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction

15 The title of this article – and of this chapter – draws inspiration from David S. Wall´s analysis on a generational history of Internet as conduit for criminal activity. For more detail, see D. WALL, 'Criminalising cyberspace: the rise of the Internet as a ´crime problem´', in Y. JEWKES and M. YAR (ed.), *Handbook of Internet Crime*, (London and New York: Routledge, 2012), 88–103, especially at. 94–98.

16 S. BOK, Lying, Moral Choice in Public and Private Life, (New York: Vintage Books, 1999).

17 See http://www.ic3.gov/crimeschemes.aspx (visited 5 October 2017).

18 CLOUGH *supra* note 13, at. 183.

19 http://www.fraud.org (visited 6 October 2017). See also BRENNER *supra* note 11, at. 76–82.

20 BRENNER *supra* note 11, at. 76.

21 The abbreviation Huuto comes from the Finnish word 'huutokauppa', i.e. 'an auction' in English.

site or the non-delivery of products purchased through an Internet auction site".[22] Let us now suppose that a person starts an auction on a site with low price for certain item and that in this particular example it is a Nokia mobile phone. One bidder is particularly interested in this type of Nokia phone and offers the highest price, but what happens is that the fraudster accepts the payment from the auction winner, but never delivers the promised goods. Alternatively, the fraudster delivers an item that is less valuable than the one offered – for example, a counterfeit item or one that has been refurbished.

Both in a criminological and a conceptual sense, auction fraud can be understood as a subcategory of mass-marketing fraud, which is conducted through solicitation via the Internet "to induce multiple persons to (1) purchase goods or services; (2) participate in a contest, sweepstakes, or lottery; (3) invest for financial profit; or (4) otherwise pay advance fees or ´taxes´ for services that are promised but not delivered".[23] Depending on the auction system on the website, it is possible to sell the same item multiple times. Another typical feature of this mass-marketing fraud in Finland has been the high degree of *recidivism* of the offenders: the fraudsters have continued this method of defrauding even after they have been caught and punished.[24]

2.2 Quick Loan Companies and Fraudulent Behaviour

My second example concerns 'quick loan' companies. These financial institutions are similar to banks, but their ability to provide loans has been legislatively restricted in Finland.[25] These instant or quick loans are normally of 100 or 200 Euros, and the interest rate is restricted to a certain maximum: when the credit is under 2000 euros, the interest rate may be at maximum the reference rate according to the Interest Act (Section 12) with an additional 50 per cent (Consumer Protection Act, Chapter 7 Section 17a). It should be noted that before the latest legislative reform the interest rates were sky-high – Statistics Finland has provided information according to which the annual percentage rate of charge has been as high as 920 per cent.[26]

The legislative framework of the quick loan market also includes the system of electronic identification, which must be sufficiently secure. This system is based on the Act Amending the Act on Strong Electronic Identification and Electronic Signatures (533/2016). The concept of *strong electronic identification* refers "to the identification of a person and the verification of the authenticity and validity of the identification by an electronic method based on at least two of the following three alternatives: a) a password or similar that the identification device holder knows; b) a chip card or similar that the identification device holder has in his or her possession;

22 http://www.ic3.gov/crimeschemes.aspx (visited 5 October 2017). See even YAR *supra* note 1, at. 80–82 and CLOUGH *supra* note 13, at. 185–187.

23 http://www.ic3.gov/media/MassMarketFraud.pdf.

24 In Finland, one may have witnessed the record of cyber fraud offences when a relatively young male offender was convicted for 300 online frauds. It is worth mentioning that at the same time there was ongoing police investigation against this same person. See http://www.hs.fi/kotimaa/Nettipetosten+ennätysmies+tuomittiin+yli+300+uudesta+rikoksesta/a1411442228938 (visited 8 October 2017).

25 A brief summary concerning the problems of supervising quick loan companies will be found on the homepage of the Financial Supervision Authority http://www.finanssivalvonta.fi/en/Financial_customer/Financial_products/Loans/Consumer_credits/Pages/quick_loans.aspx#.VD9mXEuubQN (visited 8 October 2017).

26 See Government Bill 78/2012 concerning changes to the Consumer Protection Act, at. 12.

or c) a fingerprint or some other characteristic identifying the device holder"[27] (for more on these concepts, see Section 2 and 8a, Act on Strong Electronic Identification and Electronic Signatures).

Therefore, it is possible to apply for a quick loan by using either a) net bank access codes, that is, via a user ID and security password issued by one's own bank, or b) a mobile ID, that is, the Mobile Certificate in one's mobile phone. In addition, in both alternatives the applicant needs a mobile phone number for the verification carried out by a quick loan company. Also worth mentioning in this context is the possibility of using a prepaid phone number for verification.

Let us suppose that a person succeeds in acquiring someone's net bank access codes. This can be done by *phishing*, that is, acquiring sensitive information by masquerading as a trustworthy entity – in Finland, such entities include the police, customs and banks, for example. Naturally, a person can also steal net bank access codes in the traditional sense. The third option is that the person is entitled to have these codes but uses them unlawfully.[28] In order to acquire the biggest possible loot, he or she decides to apply for a loan from several companies. After the procedure of applying for a loan and subsequent verification of the applicant have been successful, the loan will be transferred to the applicant´s bank account. What happens follows is the transfer of this money to another bank account, which can be owned either by the applicant or another person. The last step will be the withdrawal of the money from this bank account. It should of course be recalled that the applicant has neither the intention nor the ability to pay back the loans.

2.3 Real Estate Fraud

The third case is a hypothetical one, but it has many similarities to cases that were very common in Finland at the end of 1980s and at the beginning of 1990s.[29] These 'older' cases were linked to the purchase of real estate. The starting point of the legislative structure is that there are specific requirements for a purchase involving the purchase or sale of real estate in Finland. One of these requirements is *public purchase witnessing*, which is needed in order to obtain title to the property (Chapter 2, Section 1 of the Code of Real Estate). The concept of a title refers to the procedure for registering ownership rights to a property, unseparated parcel or designated share in the title and mortgage register (Chapter 5, 7 and 10–13 of the Code of Real Estate).

Public purchase witnessing is related to the validity of the transaction as follows.[30]

1) "A sale of real estate shall be concluded in writing. The seller and the buyer or their attorneys shall sign the deed of sale. A notary i.e. a public purchase witness shall attest the sale in the presence of all the signatories of the deed

27 More information can be found at http://www.viestintavirasto.fi/en/cybersecurity/electronicidentificationandsignature.html (visited 8 October 2017).

28 The term 'unlawfully' refers here to a situation in which a person has the permission of the account holder to use these codes but exceeds his or her authority.

29 See also TAPANI, J., 'Financial Crisis and Criminal Law – Is Trust Everything that Matters?', in H. GUNNLAUGSSON, H. (ed.), *When the unforeseen is seen. NSfK Workshop in Reykjavik, Iceland*, 2012, available online at http://nsfk.org/Portals/0/Archive/1_When%20the%20unforeseen%20is%20seen.pdf, at 44–69.

30 Chapter 2, Section 1 of the Code of Real Estate. More information will be found in http://www.maanmittauslaitos.fi/en/real-property (visited 8 October 2017).

of sale. Only a public purchase witness can carry out the confirmation. Without public purchase witnessing, the conveyance is null and void, and the purchaser cannot get the title for the property.

2) The public purchase witness, or public notary, acts as a witness for the conveyance and, at the same time, checks the identity of the parties and the formal competence followed in the transfer process. The conveyance cannot be registered, if there is a good reason to suspect the competence of the transfer."[31]

However, since 1.11.2013 it has been possible to sell or buy real estate via an online service called the Property Transaction Service (Chapter 5 and 9a of the Code of Real Estate). The service is maintained by the National Land Survey of Finland.[32] What is relevant here is the exception made to the requirement to use a public purchase witness. The Property Transaction Service does not demand that the public purchase witness confirm the purchase (Chapter 9, Section 9 of the Code of Real Estate) because the online service uses the strong electronic identification system (see chapter 2.2.). This means that the seller and the buyer use a) net bank access codes, b) a Citizen Certificate issued by the Population Register Centre, or c) a mobile ID.

Let us suppose that two persons succeed in acquiring net bank access codes by phishing or stealing them, or they use the codes unlawfully in another way. It is possible to construct a hypothetical course of events whereby these persons fabricate a false purchase of real estate in order to apply for a loan from a bank with false information. According to the Code of Real Estate (Chapter 9a, Section 8), the right to draw up a draft contract on the online system belongs to the person who has title to the real estate. Therefore, it is possible for these persons to orchestrate the creation of a false document and manipulate a false purchase of real estate.[33] The Property Transaction Service would then allow them to register (fraudulent) title to the real estate (Chapter 9a, Section 12) and use this as collateral for a loan. As a result, it is obvious that in reality there would be a fundamental lack of collateral for granting this loan and that the bank would therefore become a victim of fraud.

3 Criminal Law Context

3.1 General Remarks

Fraud offences are included in Chapter 36 of the Finnish Criminal Code.[34] This chapter has the title "Fraud and other dishonesty". According to Chapter 36 Section 1 (760/1990):

> a person who, in order to obtain unlawful financial benefit for himself or herself or another or in order to harm another, deceives another or takes advantage of an error of another so as to have

31 According to the Code of Real Estate (Chapter 2, Section 1), the text shall include information as follows: 1) the intent to convey; 2) the real estate to be conveyed; 3) the seller and the buyer; and 4) the price or other consideration.

32 See https://www.kiinteistoasiat.fi/english_info (visited 8 October 2017).

33 It is worth noting that the state is liable to compensation for damages caused by unlawful identification to the online service system (Chapter 9a, Section 3 of the Code of Real Estate).

34 See J. TAPANI, 'Petos', in D. FRÄNDE ET AL., *Keskeiset rikokset*, (4rd edn., Helsinki: Edita Publishing, 2014), at. 586–610 and A. NUUTILA – M. MAJANEN, 'RL 36: Petos ja muu epärehellisyys', in T. LAPPI-SEPPÄLÄ ET AL., *Rikosoikeus*., (3rd edn., Helsinki: WSOY, 2009), at. 973–990.

> this person do something or refrain from doing something and in this way causes economic loss to the deceived person or to the person over whose benefits this person is able to dispose, shall be sentenced for fraud to a fine or to imprisonment for at most two years.[35]

In Subsection 2 (514/2003), criminal liability is extended to:

> any person who, with the intention referred to in subsection 1, by entering, altering, destroying or deleting data or by otherwise interfering with the operation of a data system, falsifies the end result of data processing and in this way causes another person economic loss.

From the conceptual point of view, the essential element of fraud is deception, referring to "the communication of a message with which the communicator, in communicating, intends to mislead – that is, the communication of a message that is intended to cause a person to believe something that is untrue".[36] In other words, the concept of deception refers to the defendants' conduct, that is, whether he or she has passed deliberately false, misleading or insufficient information to the victim.[37] Furthermore, it is axiomatic in fraud that deception must be the cause of the profit gained. This means theoretically and practically that deception must be an operative cause of victimhood, thus allowing the defendant/perpetrator to obtain property unlawfully. [38] In other words, the classic case is such that the perpetrator induces the victim into a financial transaction that then causes financial loss to the victim. Fraud is, thus, understood here paradigmatically as an intentional deception resulting in financial loss to another person. It is worth mentioning that the concept *intentional* deception means here that criminal liability is based only on intent (Chapter 3 Section 6 of the Finnish Criminal Code).

3.2 Typical Criminal-law- and Procedure-law-related Problems

I wish to claim that the Finnish fraud statue is rather well formulated, the wording of the statue is understandable in common sense, its scope of criminal liability is proper, and it bears critical scrutiny in those above presented three examples. It seems that there are no major problems if we look at, for example, the classic case of defrauding people via an online auction (Huuto.net case): the perpetrator can normally be identified without great effort[39] and the requisite criteria for fraud are fulfilled – both concerning deception and financial loss.

However, there remain different theoretical and pragmatic problems concerning the criminal justice system. The main problem is related to the question of how the criteria for deciding the number of offences should be interpreted. The legislative technique in the Finnish Criminal Code is based on a three-level-system, which

35 In Section 2, the criteria for aggravated fraud are set out, according to which the penalty is imprisonment for at least four months and at most four years. In Section 3, petty fraud is criminalised with the sanction being a fine.

36 S. P. GREEN, *Lying, Cheating, and Stealing, A Moral Theory of White-Collar Crime*, (New York: Oxford University Press, 2006), at. 76. See also S. P. GREEN, 'Cheating", *Law and Philosophy*, 23 (2), 2004, at. 137–185.

37 According to the Oxford English Dictionary, the word 'information' means 'knowledge communicated concerning some particular fact, subject, or event' or 'contrasted with *data*: that which is obtained by the processing of data'.

38 From the comparative perspective, see J. HUSA and J. TAPANI, 'Germanic and Nordic Fraud – A Comparative Look Under the Surface of Commonalities', 5 *Global Jurist Advances*.

39 Fraud is difficult to commit without leaving any electronic traces, and the perpetrator can normally be identified by their IP address (Internet Protocol address).

means that there are normally three different categories of offence: a) a basic offence (*fraud*, Chapter 36, Section 1), b) an aggravated form of offence (*aggravated fraud*, Chapter 36, Section 2) and c) a lenient form of offence (*petty fraud*, Chapter 36, Section 3). This three-level-system includes both the description of the offences and the scale of the penalty.

The typical feature of an online auction scheme is to dupe multiple persons, defrauding a great number of people who each suffer relatively small financial loss. This leads to an interesting question about the number of offences. Should the decisive element be the number of victims, that is, are there as many *petty frauds* (Chapter 36, Section 3) as there are victims or should the acts of the perpetrator be viewed as one offence, that is as one fraud (Chapter 36, Section 1)?

The same question occurs in cases in which the fraudster causes a financial loss big enough to fulfil the criteria of fraud. If he succeeds in defrauding a great number of people, we have to decide whether these acts are interpreted as only one offence, in other words as *aggravated fraud* (Chapter 36, Section 2). It is worth mentioning that the case law of the Finnish Supreme Court (hereinafter KKO), 2011:84[40] refers to the tendency of interpreting different single acts as one offence – contrary to theft[41] (Chapter 28, Section 1 of the Finnish Criminal Code).[42] This difference could be explained by the fact that courts tend to put emphasis on the fault element (mens rea) of the perpetrator. Furthermore, a difference can be seen in moral wrongfulness between theft and fraud. Both offences are attacks against another's rights of ownership;[43] however, when committing a theft the perpetrator takes the property without his or her consent, while committing a fraud means that the perpetrator uses deception to persuade the victim to surrender the property willingly.[44]

Concerning the case of quick loan companies, there are additional challenges – both from the point of view of criminal law and of criminal procedural law. Firstly, it seems that the theory of complicity can cause certain problems. Finland is among those countries where the type of participation is reflected in the conviction stage and where the different participation modes are evaluated differently (what is known as the differential participation model).[45] According to the Penal Code (Chapter 6, Section 8), the sentence must be determined in accordance with a mitigated penal latitude if the perpetrator is convicted as an abettor in an offence. This mitigation means that in determining the punishment at most three-fourths of the maximum sentence of imprisonment or fine and at least the minimum sentence provided for the offence may be imposed on the perpetrator. Taking aggravated fraud as example, it leads to the penal latitude of a minimum of 14 days imprisonment and a maximum 3 years instead of the minimum of 4 months and the maximum of 4 years.[46]

40 Furthermore, reference can be made to the case Supreme Court, Finland (hereinafter: KKO) 2014:7. However, this case dealt mostly with the criminal liability of a money collection offence (Chapter 17, Section 16 c) and the interpretation of the concept of pyramid scheme defined in the Money Collection Act (255/2006).

41 KKO 2002:33 and KKO 2011:66.

42 J. TAPANI, 'Rikosten yksiköinti – marginaalista ytimeen?', in T. HYTTINEN, T. (ed.), *Rikoksesta rangaistukseen, Juhlajulkaisu Pekka Viljanen 1952 – 26/8 – 2012*, (Turku: University of Turku, 2012), at. 221–239. See also M. ULVÄNG, *Brottslighetkonkurrens – Om relationer mellan regler och fall*, (Uppsala: Iustus Förlag, 2013).

43 Protection of property is guaranteed in Finland both in the Convention for the Protection of Human Rights and Fundamental Freedoms (Protocol 1 Article 1) and in the Constitution of Finland (Section 15). Concerning theft, see GREEN *supra* note 35, at. 89.

44 BRENNER *supra* note 11, at. 59.

45 J. TAPANI and M. TOLVANEN, *Rikosoikeuden yleinen osa – Vastuuoppi*, (2nd edn., Helsinki: Talentum, 2013), at. 413–415.

46 J. TAPANI and M. TOLVANEN, *Rikosoikeus – Rangaistuksen määrääminen ja täytäntöönpano*, (3rd edn., Helsinki: Talentum, 2016), at. 31–34.

As a consequence, it is of great importance to consider the degree to which it is blameworthy to give another person a permission to use your net bank access codes. What if the person then uses these access codes? Does it automatically mean that the owner of the bank account shares the guilt as a co-perpetrator or accomplice to fraud? What about a person who is asked to withdraw money from his own bank account? Does he act as a co-perpetrator or accomplice to fraud? Or should he be charged with money laundering? What kind of knowledge is needed in order to claim that the person did something intentionally?

In addition, there have been certain challenges concerning the pre-investigation of cases regarding quick loan companies. The system earlier described concerning the quick loan market enables the use of Internet café's or neighbours' unprotected WLAN connections when applying for a loan from quick loan companies. Therefore, it is not always easy to identify either the person or the real perpetrator behind the events. This is a very good example of the nature of the problems that occur in our modern communications environment and of the challenges that have to be dealt with in gathering and presenting evidence in criminal cases.[47]

It is worth emphasizing that the scope of the fraud offence seems to be a proper one, and there should be no major problems applying it to the cases of quick loan companies. In other words, one does not have to dwell upon the question of deceiving a machine and the structure of the fraud offence.[48] This is because the perpetrator has valid access codes in applying for the loan, but he is using these codes for an illegal purpose. The actual untrue representation made to the machine is not punishable because the access codes are real. Thus, the criminal liability is based on the provision of false information concerning the recipient's willingness and capacity to pay back the loan.

Regarding the third case, that is, the hypothetical case of real estate fraud, it is certainly too early to estimate whether – and to what degree – certain risks embedded in the system will be realised. However, I believe that the most vulnerable parts of this online system will be net bank access codes or other identification tools. If a person succeeds in gaining possession of these tools – either by stealing or unlawfully using them – the system appears to allow a fraudster to orchestrate a fictional transaction in order to apply for a loan from a bank. It seems impossible to construct a system that is 100% safe, and there will also always be people who are willing to, and capable of, testing the vulnerability of such systems.

3.3 The Rational Decision-Making of the Victim

I wish to highlight that not only the element of deception but also the conception of the victim's state of mind has been thoroughly discussed in many different legal systems.[49] It should come as no surprise to note that the concept of deception has not been analysed merely by focusing on the defendant's conduct, that is, has he or she passed deliberately false, misleading or insufficient information to the victim? Other elements looked into include the kind of conclusions that the victim is legally

47 For a more detailed analysis, see I. WALDEN, 'Computer forensics and the presentation of evidence in criminal cases', in Y. JEWKES and M. YAR (ed.), *Handbook of Internet Crime*, (London and New York: Routledge, 2012), at. 603–627.

48 CLOUGH *supra* note 13, at. 204–205.

49 J. HUSA and J. TAPANI *supra* note 37.

entitled to draw from the defendant's conduct and the legitimate expectations that inform the victim's decision-making.[50]

It is important that, according to this line of thinking, to a great extent the core of basic criminal fraud – as well as cyber fraud – is *communication between defendant and victim*. This interaction makes it possible for the fraudster to practise deceit with evil intent in order to profit unlawfully. According to this idea, we may continue by saying that one also has to pay attention to the victims' decision-making, but are there actually any minimum criteria for rational decision-making on the part of the victim? Is the defendant guilty of obtaining property by deception if the victim has added his or her own contributory negligence; for example, he or she suspected, or should have suspected, the content of the information? Even though the answers may somewhat differ, it is important to see that the question itself is, basically, the same: should the victim have known better?

In Finland, there is some case law from the Supreme Court that provides a normative background for ideas about the victim's own, normative responsibility in decision-making.[51] Furthermore, it can be argued that business actors must practise a certain minimum degree of caution in business relations. Potential victims have their own, normative responsibility for obtaining and processing information. This means that in legal decision-making one has to take into account the kind of information that the offender has passed on to the victim, the kind of expectations that the victim has had and whether the victim has been deceived from a strictly legal perspective.

When we seek to answer these questions in legal proceedings, it is possible to utilize the following criteria: a) *the principle of legal protection*, b) the *principle of proportionality* and 3) *the principle of concrete suspicion*.[52] The (Finnish) principle of legal protection means that firms and individuals alike must pay attention to risk management when they are doing business. The principle of proportionality helps judges to orientate toward facts such as the size of the financial loss, the probability of financial loss and the contracting parties' ability to avoid financial loss. The principle of concrete suspicion demands that judges, in practice that is, decide whether certain facts roused, or should have roused, concrete suspicions about the content of the information (e.g. defendants' statements may be inconsistent with other information). In other words, what can normally be expected from persons' decision-making in that kind of situation?

I claim that these normative criteria are useful for the police, the prosecutor and the judge, but I certainly admit that there is also a need for more factual-rooted criteria. By this, I mean facts that are simultaneously relevant concerning both the prevention of fraud and constructing the possible criminal liability of fraud. An outstanding list of these kinds of facts can be found, for example, on the homepage of Fraud.org, which is a project of the National Consumers League.[53]

Firstly, if someone claims that one can earn money with little or no work or make money via an investment with little or no risk, it is probably a fraud. Offers that seem too good to be true actually usually are too good to be true. Secondly, one should know the party with whom one is dealing. If the entity is unfamiliar, one should always call the number found on a website's contact information page or try to confirm the reality

50 M. PAWLIK, 'Betrügerische Täuschung durch die Versendung rechnungsähnlicher Angebotsschreiben?', *Strafverteidiger* 2003, at. 297–301, 298–299.

51 KKO 1995:23, KKO 1995:24, KKO 1995:25 and KKO 2011:84. See J. TAPANI, 'Miten asianomistajan selonottovelvollisuus määrittää petoksen rangaistavuuden alaa?', In Keskuskauppakamarin Liiketapalautakunta 80 vuotta, (Helsinki: Alma Talent, 2017), at. 309–318.

52 J. TAPANI, *Petos liikesuhteessa, Talousrikosoikeudellinen tutkimus,* (Helsinki: Suomalainen Lakimiesyhdistys, 2004), at. 195–196.

53 http://www.fraud.org/prevent_fraud (visited 11 October 2017).

of the entity from information found on the Internet. Furthermore, it is useful to read reviews or other consumer complaints.

Thirdly, the offer should be understood properly. A legitimate seller will provide a consumer with all the details about the products or services, the total price, the delivery time, the refund and cancellation policies, and the terms of any warranty. Therefore, one should contact the seller if any of these details are missing, and if they are unable to provide the details it may be a sign of fraud. Fourthly, one has to resist pressure. Legitimate companies and charities will be happy to grant a consumer time to consider the offer. It may be fraud if they demand that a consumer act immediately or refuse to take "No" for an answer. Some scammers may also demand that the consumer pay off a loan immediately or damaging consequences may occur. The consumer should always take time to look into who is requesting the money before they pay up. Fifthly, one should be cautious about unsolicited emails. They are often fraudulent. Responding to unknown senders may simply verify that it is a working email address and result in even more unwanted messages from strangers.

4 Conclusions

I have analysed three different courses of events, each of which represents one of the categories of the three generations of cyber fraud. As can be easily noted, these cases are not *pure* in the sense that they represent only one certain generation of cyber fraud. Instead, we could call all of these cases *hybrid cyber frauds*[54] because committing this fraud demands both the context of cyber space and a computer as a tool. This is true even for the third case, the real estate fraud, which is wholly mediated by technology. In this case, a fraudster uses the technology, but this is combined with the traditional method of fraud as the fraudster applies for a loan using a false document and a fabricated purchase of real estate.

What then are my answers to those questions that I aimed to explore? Firstly, we certainly are in the process of rethinking our perception of fraud in the cyber context. However, my answer to the question of the need to rethink our perception is both yes and no. This needs a brief clarification. I take for granted that cyber space as a context alters our practices of communication, but the practices are still *communication* between human beings, and every time we discuss communication we tend to find the risk of lying or cheating lurking around the corner.

Secondly, it seems that those elements of our perception that need rethinking mostly concern the development of ICT technology. However, the more fundamental changes seem to link to the practices of *where*, *when* and *how* we communicate with each other, and these changes may also have effects on the "essence"[55] of defrauding people.

What might be the future forms of fraud, for example, in Finland? According to information provided by police statistics, around half of the total number of registered cases of fraud can be categorized as cyber fraud.[56] This statement does not

54 WALL *supra* note 14, at. 96–97.

55 Here, I use the term 'essence' in the ontological sense because I find it reasonable to argue that modern technology alters both our understanding of reality as a social reality *and* the content of this social reality.

56 http://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/polisenaxwwwstructure/56207_Poliisin_tilastot_vuosi_2016.pdf?05d5de4b8a46d488 and http://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/polisenaxwwwstructure/56209_Poliisin_tilastot_vuosi_2016_nettipetokset.pdf?19fce54b8a46d488 (visited 11 October 2017).

reveal exactly what kinds of offences these cases are, but it seems probable that they are both traditional, first generation fraud, involving many cases of online auction fraud, and also more sophisticated cases of fraud in which a perpetrator makes use of modern technology. Therefore, criminal-law- and procedural-law-related problems are certainly becoming more challenging.

TRADEMARK INFRINGEMENTS AS CYBER FRAUDS IN THE NORDIC COUNTRIES

Laura Tammenlehto

1 Introduction

The sale of counterfeited products forms a large part of cybercrime in the EU.[1] Online marketplaces have become the key distribution channel for these products due to the possibilities of easy and effective international marketing.[2] The counterfeiters sell fake products on major, widely available and trusted platforms.[3] Counterfeiting has damaging consequences not only for the development of markets and the financial position of the right owner but also for consumers. Counterfeited products are often more expensive than what consumers would be prepared to pay for copies, although they may still be cheaper than the original ones.[4]

Trademark includes an assumption of certain content and quality, which counterfeited products often fail to fulfil. This is due to the lack of quality checks imposed by public standards authorities and by the brand proprietor. The deficiencies in content and quality create a consequent risk to the health and safety of the consumers. There is also no after sales service or effective recourse available for the consumers in the event of damage or injury.[5]

Criminal organizations often attempt to fund their activities by counterfeiting. Counterfeiters tend to take advantage of the differences in national jurisdictions by locating and targeting their activities based on the possibility of the most lenient consequences for their conducts.[6] In the Nordic countries, the right-owner has possibilities to react to counterfeiting through trademark crime provisions. These provisions do not cover the consequences caused by counterfeited products to the consumer. The sale of counterfeit goods often parallels fraud[7] due to its strong deceptive elements. For the requirement of misleading the victim, the sale of counterfeited goods fulfils the essential elements of the fraud provisions. However, fulfilling the requirement of causing direct financial damage to the victim is not always clear.

This chapter analyses and compares the Nordic fraud provisions from the point of view of the consumer's position in the online sale of counterfeited goods. The

1 A joint project between Europol and the European Union Intellectual Property Office, *2017 Situation report on counterfeiting and piracy in the European Union* (hereinafter: EUIPO 2017), at 11. Available at: https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union, visited 31 January 2018.

2 Europol, *EU serious and organised crime threat assessment 2017* (hereinafter: SOCTA 2017), at 46. Available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 , visited 31 January 2018.

3 EUIPO 2017, at 36.

4 M. Blakeney, *Guidebook on enforcement of intellectual property rights*, London 2010, at 13. Available at: http://trade.ec.europa.eu/doclib/html/122641.htm, visited 31 January 2018.

5 Ibid., at 13.

6 SOCTA 2017, at 46.

7 The preparatory works of the Finnish fraud provision actually define the sale of fake or defective goods as originals as one form of fraud. HE 66/1988 vp. (Finnish Government Bill on changing the Criminal Code and certain other Acts in the first phase of the total reform of the criminal legislation), at 131.

chapter handles the background of the sale of counterfeited goods via the Internet, after which it concentrates on the national fraud provisions and their ability to answer the threats of the phenomenon. This chapter approaches the matter with two example groups of goods that are recognized as potentially creating severe health and safety risks, food and spare parts. Both of these groups are usually sold under protected trademarks and are increasingly popular in the counterfeiting industry.

This chapter handles the above described problems from a criminal law point of view. The chapter does not handle problems relating to the investigation of international crimes nor the questions regarding jurisdiction. In addition, regulations relating to civil remedies, unfair competition and consumer protection have been left out of the chapter.

2 Trademark Infringement and Health and Safety Risk – Food and Spare Parts

The function of trademark is to distinguish the goods of the right–owner trader from those of another. It not only indicates the origin of the goods but also guarantees a certain quality for them on which the consumers can rely. Well–known trademarks are of significant financial value to their owner.[8] A trademark creates a certain idea and expectation of the product. The consumers assume to get products of a certain origin and the same quality as those of the same mark, which they have purchased earlier. With food products, a certain mark may also create the presumption of following a predefined and safety regulated manufacturing and supply chain. With spare parts, similar expectations target the production material and resistance to abrasion. Counterfeited products that do not reach the required and expected standards pose significant health and safety issues.[9]

Trademark confers on the right–owner to enjoin unauthorized use of his mark in the course of trade. Specifically, it confers the use of: 1) identical marks for identical goods or services; 2) identical or similar marks for identical or similar goods, if this entails the likelihood of confusion;[10] and 3) identical or similar marks for goods or services, which are not similar to those for which the trademark is protected if the trademark has a reputation and if the use made of it a) takes unfair advantage of the reputation or the distinctive character of the trademark or b) is detrimental to them. In addition to this, for a trademark infringement to be at hand, the alleged infringer must have actively used the sign. The use of the sign must have occurred in the course of trade and in relation to goods or services. The use must also have been such

8 C. Waelde et al., *Contemporary intellectual property. Law and policy*. Oxford University Press 2011, at 547-552.

9 R. M. Hilty, *Economic, legal and social impacts of counterfeiting*, in book C. Geiger (ed.), *Criminal enforcement of intellectual property rights. A handbook of contemporary research.* Edward Elgar 2012, at 9; *EUIPO 2017*, at 11-12.

10 Defining the likelihood of confusion requires an assessment of the level of similarity of the marks and the goods and services. Crucial is the overall impression that is created on the relevant public. A. Kur and T. Dreier, *European intellectual property law*, Edward Elgar 2013, at 208-211. See also, e.g. ECJ cases: C-251/95, *Sabèl* v. *Puma*, [1997] ECR I-6191, judgment of 11 November 1997; C-39/97, *Canon Kabushiki Kaisha* v. *MGM*, [1998] ECR 1-5507, judgment of 29 September 1998; C342/97, *Lloyd Schuhfabrik Meyer* v. *Klijsen Handel*, [1999], ECR I-3819, judgment of 22 June 1999.

that it jeopardized the protected trademark functions, and in particular the essential function of guaranteeing commercial origin.[11]

Counterfeiting, basically, means stealing the intellectual property, that is the market force of the trademark, from the legitimate trader.[12] Counterfeiting is done in order to benefit financially from the already existing trademarks without having to use time and resources to gain the position in the market and create a well-known and powerful brand.[13] Counterfeiting of trademark protected goods can be harmful not only to the right owner, but also to consumers. The effects of counterfeiting on the right owner may be direct economic losses, which appear as a decrease in the sale of goods sold on the market. The effects may also transpire as counterfeited products harming the reputation and the presumption of quality related to the trademark, which may lead to a more permanent decrease in the market position.

The sale of counterfeited goods may affect the consumers' interests in different ways. First, the counterfeited products may mislead the consumers either because the whole product including the trademark protected sign is copied or because the external appearance of the imitation[14] is similar to the original product. This affects the consumer's trust in market transparency and delivery of truthful information.[15]

Second, counterfeit goods may cause health and safety risks to consumers.[16] The health and safety risks are evident in the fields of food products and spare parts. Counterfeited foods may, for instance, contain toxic substances, contain allergens that are not included in the ingredients or be outdated and therefore rotten. Counterfeited spare parts may be manufactured from cheaper and not as strong materials as the original parts, which may lead to unexpected breakage of the parts causing serious accidents or even death.

Third, the low quality of the counterfeited goods may lead to consumers' expectations not being met when the product does not function as expected. All three effects are usually the result of deception.[17] The most important effect from the criminal law point of view is, naturally, the risk to health and safety.

Counterfeiting is criminalized in the Nordic countries under the trademark crime provisions.[18] All countries have enacted punishable intentional infringement of trademark (both registered and established by use) with the threat of penalty of imprisonment. The object of protection in these provisions is the exclusive right to exploit trademark, which means that only acts directly infringing the said exclusive right may be punishable with criminal sanctions based on the trademark crime provisions. Therefore, even though trademark infringements can cause harm to other people than the right-holder, for instance, to consumers when they buy counterfeited goods via the Internet, the trademark crime provisions only enable the actions of

11 Ibid., at 195-201.

12 D. Matthews, *Counterfeiting and public health,* in book C. Geiger (ed.), *Criminal enforcement of intellectual property rights. A handbook of contemporary research.* Edward Elgar 2012, at 42-44. Here it should be noted that the right owner is also able to continue the use of the trademark himself. So any actual transition of property is not done, but the stolen 'item' is the brand of the trademark, which is illegally exploited.

13 OECD (2008), *The economic impact of counterfeiting and piracy (*hereinafter*: OECD (2008))*, OECD Publishing 2008, at 48-49.

14 Imitation is allowed in certain situations under specific conditions. See more, e.g. R. M. Hilty 2012, at 16-17, A. Kur – T. Dreier 2013, at 195-234. This chapter only handles illegal imitation.

15 A. Ohly, *Counterfeiting and Consumer protection*, in C. Geiger (ed.), *Criminal enforcement of intellectual property rights. A handbook of contemporary research.* Edward Elgar 2012, at 25.

16 Ibid., at 25.

17 Ibid., at 26.

18 See Trademark Acts of each country: Finland: Section 56a and Chapter 49 Section 2 of the Criminal Code; Sweden: Chapter 8 Section 1; Norway: Section 61; and Denmark: Section 42: In Sweden and Denmark, also gross negligent acts are criminalized.

the right–owner against the infringers. They do not cover the consequences that are caused to the end user of the counterfeited product.

The first example of the class of goods creating a significant health risk, which has caught the interest of the counterfeiters, is food products.[19] All deliberate and intentional actions to fraudulently modify or represent food, its ingredients or packaging for economic gain are gathered under a collective term 'food fraud'.[20] Food fraud[21] has been divided into seven categories in regard to the economic and public health threats.[22]

19 This presentation applies also to beverages.

20 J. Spinck – D. C. Moyer, *Defining the public health threat of food fraud*, Journal of Food Science, Vol. 76, Nr. 9, 2011,at R158. Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1750-3841.2011.02417.x/epdf, visited 31 January 2018.

21 The concepts of 'fraud' and 'food fraud' must be separated from one another. 'Fraud' means the criminally punishable act defined in the criminal legislation. 'Food fraud', as pointed out, is a more general concept to describe fraudulent actions related to the food industry, without any guarantees of the act actually fulfilling the essential elements of 'fraud'.

22 Ibid., at R162.

Table 1. Food fraud incident types[23]

Term	Definition	Example	Potential public health threat that may lead to illness or death
Adulterate	A component of the finished product is fraudulent	Melamine added to milk	Fraudulent component
Tamper	Legitimate product and packaging are used in a fraudulent way	Changed expiry information, product up-labelling etc.	Fraudulent packaging information
Over–run	Legitimate product is made in excess of production agreements	Under–reporting of production	Fraudulent product is distributed outside of regulated or controlled supply chain
Theft	Legitimate product is stolen and passed off as legitimately procured	Stolen products are co-mingled with legitimate products.	Fraudulent product is distributed outside of regulated or controlled supply chain
Diversion	The sale or distribution of legitimate products outside of intended markets	Relief food redirected to markets where aid is not required	Shortages or delays of relief food to needy populations
Simulation	Illegitimate product is designed to look like but not exactly copy the legitimate product	'Knock-offs' of popular foods not produced with same food safety assurances	Fraudulent product of lesser quality
Counterfeit	All aspects of the fraudulent product and packaging are fully replicated	Copies of popular foods not produced with same food safety assurances	Fraudulent product

Food fraud covers many different acts, but from the point of view of public health the most relevant are adulteration, tampering, simulation and counterfeiting. In situations of over-run, theft and diversion the food product itself is legal, but the distribution of it is not. This could be seen to have more economic than health impacts. In situations of tampering, the food product is also legal, but the health risk comes

23 Ibid., at R162.

from the manipulation of, e.g. the expiry date, which potentially leads to the product becoming unsuitable for human consumption.

From the point of view of trademark infringements, counterfeiting is the most important form of food fraud. Simulation of goods infringes trademark, unless it is performed within the rather narrow acceptable limits. In tampering, over-run, theft and diversion of the product itself is yet again practically legal. In theft, trademark infringement may occur if the perpetrator, for instance, releases the stolen products onto a new market. If tampering, over-run or diversion are done by someone else than the right-owner, trademark infringement may occur. There might also be some level of theft involved. If the perpetrator in these is the right–owner himself, then naturally he cannot be infringing his own trademark. Other illegalities than trademark infringement may, of course, be in question. Adulterate goods are infringing if they are 1) sold under a protected trademark and 2) manufactured by someone else than the right–owner. If these two requirements are not fulfilled, then trademark infringement is not at hand. For instance, if milk is sold merely as milk and not under the, e.g. Valio or Ingman trademark, then the conduct is not infringing a trademark, but the product may still be a counterfeit in relation to what the consumers expect milk to be.

The public health risks that may result from food fraud can be divided into direct, indirect and technical food fraud risks. Direct food fraud risk means that there is an imminent risk to the health of the consumer. For instance, an acutely toxic or lethal contaminant has been included in the product. Indirect food fraud risk means that the consumer is at risk through long–term exposure to low doses of a chronically toxic contaminant, which build up in the body. This includes also the omission of beneficial ingredients such as vitamins. Technical food fraud risk means non–material modification of the product, for instance, by misrepresenting product content or the information about the country of origin.[24]

Another example of a high-risk class of goods is spare parts, for instance, of a car. In spare parts, the health and safety risk may actualize in low-quality products, deficiencies or unexpected breakage that may affect the main product's safety.[25] These products can be for instance dysfunctional brake pads or airbag mechanisms, or low-quality electrical components that give electric shocks to users.[26] The field is rather different in comparison to food products; however, the potential risks to health and safety are equitable in both of them.

The situations in which the consumers buy counterfeited products vary. First, consumers may be willing to acquire legitimate products, which means they are deceived into purchasing counterfeits. Second, consumers may willingly and knowingly be purchasing counterfeited products and are motivated by, for instance, the price of the product. Third, consumers may merely be uninterested in the origin of the product and whether or not it is a counterfeit.[27] The starting point from which the consumer has acquired the counterfeit product affects the evaluation of the fulfillment of fraud.

24 Spinck – Moyer 2011, at R159.
25 OECD/EUIPO (2016), *Trade in counterfeit and pirated goods: Mapping the economic impact* (hereinafter: OECD/EUIPO (2016)), OECD Publishing, Paris 2016, at 15.
26 OECD (2008), at 148.
27 OECD (2008), at 42.

3 Nordic Fraud Provisions and Their Applicability in the Sale of Counterfeit Goods

Computer-related frauds are not a new phenomenon, although ongoing technological development multiplies the opportunities for committing them. These types of frauds relate most commonly to, for instance, means of payment, selling non-existent goods, non-delivery of sold goods, data tampering etc. These conducts are criminalized across the EU if they produce a direct economic or possessory loss to the property of another and the perpetrator has acted with the intent of obtaining unlawful economic gain for himself or for another person.[28] Often the problem is that existing criminal provisions fail to cover the conduct that is performed in the cyber environment.[29]

The Nordic Criminal Codes include specific criminalizations related to online frauds, such as means of payment fraud and data tampering,[30] but there are no general clauses criminalizing all fraudulent online activities. Mostly, the case-specific evaluation is conducted by interpreting the existing crime provisions in the online environment. Therefore, the sale of illegal goods via the Internet must fulfil the essential elements of the traditional fraud provisions in order for it to constitute a cyber fraud.

28 Council of Europe, Explanatory report to the convention on cybercrime hereinafter: CE report 2001), European Treaty Series - No. 185 at 14-15. Available at: https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwigoszqm4LZAhWFECwKHQZeAgUQFggmMAA&url=https%3A%2F%2Frm.coe.int%2F16800cce5b&usg=AOvVaw1CJJ_q_4Tb05UJ_X0jfUXN, visited 31 January 2018.
According to the Convention, the term 'loss of property' includes loss of money, tangibles and intangibles with an economic value. CE report 2001, at 15. Available at: https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwigoszqm4LZAhWFECwKHQZeAgUQFggmMAA&url=https%3A%2F%2Frm.coe.int%2F16800cce5b&usg=AOvVaw1CJJ_q_4Tb05UJ_X0jfUXN, visited 31 January 2018.

29 Q. Wang (ed.), *A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe*, Wolf Legal Publishers 2017, at 16.

30 Ot.prp. nr. 22 (2008-2009) (Proposal of the Ministry of Justice and Police on changing the Criminal Code of Norway), at 57-58; HE 66/1988 vp, at 130; Statens Offentliga Utredningar (Government Bill on increasing the criminal law protection of property, hereinafter SOU) SOU 2013:85, at 66.

The essential elements of the Finnish fraud provision[31] consists of five elements. First, the perpetrator must either actively mislead the victim or take advantage of the victim's error. Second, the victim must actually err.[32] Third, the erring of the victim must lead to actions or inactions that, fourth, cause financial damage or the danger of it to the victim or another person whose benefits are under the victim's authority. The final element is the aim of the crime; the perpetrator must have the aim to benefit from the act himself or gain benefit for someone else or harm the victim.[33] Here it must be pointed out that the 'harm the victim' requirement specifically means financial harm.[34]

As a very simple example of buying counterfeited goods online, this would mean that the perpetrator either lies to the victim about the origin of the goods or does not correct the victim's erroneous perception. The perpetrator can do this, for instance, by adding a trademark to the product and thus claiming that the product is manufactured under the said trademark. Naturally, the victim must have a false impression of the situation, which he believes to be true; that is he believes the goods to be original. This false impression must lead to actions or inactions, for instance, the ordering of the counterfeited product of low quality instead of trying to find a legitimate high-quality product to order. The action or inaction causes the victim financial damage when the low-quality counterfeit instantly breaks and the victim loses the purchase price. The perpetrator has the aim to make money by selling the counterfeited goods.[35]

---

31 The fraud provisions in Finnish Criminal Code (hereinafter FCC) Chapter 36: '1 § Petos
Joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä, on tuomittava *petoksesta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
Petoksesta tuomitaan myös se, joka l momentissa mainitussa tarkoituksessa dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaan tietojenkäsittelyn lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa. (13.6.2003/514)
Yritys on rangaistava.
2 § Törkeä petos
Jos petoksessa 1) tavoitellaan huomattavaa hyötyä, 2) aiheutetaan huomattavaa tai erityisen tuntuvaa vahinkoa, 3) rikos tehdään käyttämällä hyväksi vastuulliseen asemaan perustuvaa erityistä luottamusta tai 4) rikos tehdään käyttämällä hyväksi toisen erityistä heikkoutta tai muuta turvatonta tilaa ja petos on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä petoksesta* vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.
Yritys on rangaistava.
3 § Lievä petos
Jos petos, huomioon ottaen tavoitellun hyödyn tai aiheutetun vahingon määrä taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava *lievästä petoksesta* sakkoon.' The wordings of the law cannot be interpreted from a translated section. Also, none of the translations of Nordic laws are official, and not all of the countries provide even an unofficial translation. For these reasons, the author has chosen to provide the sections in the original languages. The author provides links to the unofficial translation of the law in question, if such a translation exists. The unofficial translation of the FCC is available at: http://finlex.fi/en/laki/kaannokset/1889/18890039.

32 For instance in case Korkein oikeus (the Supreme Court of Finland) (hereinafter: KKO) KKO 2004:109, judgment of 3 November 2004, the perpetrator had neglected the duty to inform the fee collecting organization about manufacturing copies of videocassettes with the result that the organization did not collect fees from him and therefore suffered from financial loss. This neglect, however, was not considered as active erring. Neither was it considered taking advantage of the victim's erring because mere unawareness cannot be interpreted as erring.

33 A-M. Nuutila – M. Majanen, *RL 36: Petos ja muu epärehellisyys*, in T. Lappi-Seppälä et al., *Rikosoikeus*, Alma Talent 2008, at Petos. Erehdyttämisen muotoja. Perustunnusmerkit; HE 66/1988 vp, at 132-133.

34 HE 66/1988 vp, at 131.

35 The perpetrator might also have the aim of harming the buyers with his products. More likely, however, is that the perpetrator simply does not care whether the product is harming the health and safety of the buyer. OECD (2008), at 148.

In Finland, only intentional frauds are punishable. The criminalized behaviour may be divided into three levels based on the severity and harmfulness of the act. The threat of penalty varies from fines for petty fraud, to the maximum of two years imprisonment for the basic form of the act and up to the maximum of four years imprisonment for aggravated fraud.

Other Nordic countries have executed their fraud provisions in a similar way to Finland. The Swedish description of the act[36] also consists of five elements with the exception that only active misleading of the victim is punishable. Therefore, taking advantage of the victim's error does not fulfil the essential elements of the crime. For the Swedish fraud provision to be fulfilled, the perpetrator must benefit from the incident. However, the wordings of the law do not cover acts with the purpose of merely harming the victim. The criminal conduct may be divided into three grades with of the threat of penalty varying from fines to the maximum of six months imprisonment for a petty offence, to a maximum of two years imprisonment for the basic form of the act and up to the maximum of six years imprisonment for the aggravated form of the act. Only intentional acts are punishable.

Norway[37] technically executes fraud provisions in the same way as the other countries. In Norway, both active erring and more passive taking advantage of the victim's error are punishable. The victim must err, and the erring must lead to either

36 According to Swedish Criminal Code (hereinafter: SCC) Chapter 9 of Fraud and other dishonesty: '1 § Den som medelst vilseledande förmår någon till handling eller underlåtenhet, som innebär vinning för gärningsmannen och skada för den vilseledde eller någon i vars ställe denne är, dömes för bedrägeri till fängelse i högst två år.
För bedrägeri döms också den som genom att lämna oriktig eller ofullständig uppgift, genom att ändra i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehandling eller någon annan liknande automatisk process, så att det innebär vinning för gärningsmannen och skada för någon annan. *Lag (1986:123)*.
2 § Är brott som avses i 1 § med hänsyn till skadans omfattning och övriga omständigheter vid brottet att anse som ringa, döms för ringa bedrägeri till böter eller fängelse i högst sex månader.
För ringa bedrägeri döms också den som utan att göra rätt för sig tillgodogör sig husrum, förtäring, transport, tillträde till föreställning eller annat sådant som tillhandahålls under förutsättning av kontant betalning, oavsett om han eller hon vilseleder någon eller inte. Det gäller dock inte om gärningen avser värde som inte är ringa och om den i övrigt är sådan som avses i 1 §. *Lag (2017:442)*.
3 § Är brott som avses i 1 § att anse som grovt, döms för grovt bedrägeri till fängelse i lägst sex månader och högst sex år.
Vid bedömningen av om brottet är grovt ska det särskilt beaktas om gärningsmannen har missbrukat allmänt förtroende eller använt urkund eller annat vars brukande är straffbart enligt 14 eller 15 kap. eller vilseledande bokföring eller om gärningen annars varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada. *Lag (2017:442)*.' The unofficial translation of the SCC is available at: http://www.government.se/government-policy/judicial-system/the-swedish-penal-code/

37 The Norwegian Criminal Code (hereinafter: NCC) enacts that: '§ 371. Bedrageri
Med bot eller fengsel inntil 2 år straffes den som med forsett om å skaffe seg eller andre en uberettiget vinning a) fremkaller, styrker eller utnytter en villfarelse og derved rettsstridig forleder noen til å gjøre eller unnlate noe som volder tap eller fare for tap for noen, eller b) bruker uriktig eller ufullstendig opplysning, endrer data eller datasystem, dispon-erer over et kredittkort eller debetkort som tilhører en annen, eller på annen måte uberettiget påvirker resultatet av en automatisert databehandling, og derved volder tap eller fare for tap for noen.
§ 372. Grovt bedrageri
Grovt bedrageri straffes med fengsel inntil 6 år. Ved avgjørelsen av om bedrageriet er grovt skal det særlig legges vekt på om a) det har hatt til følge en betydelig økonomisk skade, b) det er voldt velferdstap eller fare for liv eller helse, c) det er begått ved flere anledninger eller over lengre tid, d) det er begått av flere i fellesskap eller har et systematisk eller organisert preg, e) lovbryteren har foregitt eller misbrukt stilling, verv eller oppdrag, f) det er ført eller utarbeidet uriktige regnskaper eller uriktig regnskapsdokumentas-jon, eller g) lovbryteren har forledet allmennheten eller en større krets av personer.
§ 373. Mindre bedrageri
Bedrageri straffes med bot når straffskylden er liten fordi det gjaldt en ubetydelig verdi og forholdene for øvrig tilsier det.
§ 374. Grovt uaktsomt bedrageri
Grovt uaktsomt bedrageri straffes med bot eller fengsel inntil 1 år. Dersom et grovt uaktsomt bedrageri må anses som grovt, jf. § 372 annet punktum, kan fengsel inntil 2 år anvendes.' The unofficial translation of the NCC is available at: http://app.uio.no/ub/ujur/oversatte-lover/cgi-bin/sok.cgi?dato=&nummer=&tittel=penal&type=LOV&S%F8k=Search

action or inaction that causes financial damage or the danger of it to the victim or someone else. The perpetrator must have the purpose to gain unjustified financial profit for himself or someone else. The noticeable difference in the Norwegian fraud provisions in comparison to other Nordic provisions is that they criminalize also gross negligent forms of the act, while in all other countries only intentional acts are punishable. Penalties vary quite a lot in Norway. For gross negligent fraud[38], the threat of penalty is from fines to one year imprisonment or, if the form of the act is aggravated in a way that is defined in the provision concerning aggravated fraud, to two years imprisonment. The petty form of intentional fraud is punishable with fines, and the basic form of the act with the maximum of two years imprisonment. In the aggravated form of intentional fraud, the maximum penalty rises to six years imprisonment.

Danish fraud provisions[39] are nearly equitable to the Norwegian provisions with the exception that only intentional acts are punishable. The wordings of the Danish fraud provision also suggest that the person who suffers from financial damage should be more closely related to the situation at hand than is the case according to the Norwegian fraud provision, which requires simply that 'someone' suffers damage. The threat of penalty is the most severe in Denmark, with the maximum of eight years imprisonment for aggravated fraud. Petty fraud is punishable with fines, and the basic form of the act with the maximum penalty of one year and six months imprisonment.

The elements regarding erring of the victim and the erring leading to action or inaction are common to all the countries. The element of misleading the victim in the Swedish provision differs from that of other countries by not including the mere exploitation of the victim's erring. This may rule out some situations from the sphere of punishability if the perpetrator's active measures to mislead the victim

---

38 Gross negligent fraud can be either a basic form of the act or an aggravated form of the act. The evaluations of grading is done based on the descriptions of the act in the intentional fraud provisions. Ot.prp. nr. 22 (2008-2009), at 326-327.

39 Danish Criminal Code (hereinafter: DCC) Chapter 28 of Property crimes:'§ 279. For bedrageri straffes den, som, for derigennem at skaffe sig eller andre uberettiget vinding, ved retsstridigt at fremkalde, bestyrke eller udnytte en vildfarelse bestemmer en anden til en handling eller undladelse, hvorved der påføres denne eller nogen, for hvem handlingen eller undladelsen bliver afgørende, et formuetab.
§ 279 a. For databedrageri straffes den, som for derigennem at skaffe sig eller andre uberettiget vinding retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer til elektronisk databehandling eller i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling..
…
§ 285. De i §§ 276 og 278-283 nævnte forbrydelser straffes med fængsel indtil 1 år og 6 måneder. I de i § 283, stk. 2, nævnte tilfælde kan straffen såvel for skyldneren som for den begunstigede fordringshaver gå ned til bøde.
Stk. 2. Ulovlig omgang med hittegods straffes med bøde eller fængsel indtil 1 år og 6 måneder.
§ 286. Straffen kan stige til fængsel indtil 6 år, når de i §§ 276, 281 og 282 nævnte forbrydelser er af særligt grov beskaffenhed navnlig på grund af udførelsesmåden, eller fordi forbrydelsen er udført af flere i forening eller under medtagelse af våben eller andet farligt redskab eller middel, eller på grund af de stjålne genstandes betydelige værdi eller de forhold, under hvilke de befandt sig, eller fordi der er tale om tyveri begået som led i organiseret indbrudskriminalitet, eller fordi der er tale om systematisk eller organiseret afpresning, eller når et større antal forbrydelser er begået.
Stk. 2. Straffen kan stige til fængsel indtil 8 år, når de i §§ 278-280 og 283 nævnte forbrydelser er af særligt grov beskaffenhed navnlig på grund af udførelsesmåden, eller fordi forbrydelsen er udført af flere i forening, eller som følge af omfanget af den opnåede eller tilsigtede vinding, eller når et større antal forbrydelser er begået.
§ 287. Er nogen af de forbrydelser, der er nævnt i §§ 276-283, af mindre strafværdighed på grund af de omstændigheder, hvorunder handlingen er begået, de tilvendte genstandes eller det lidte formuetabs ringe betydning eller af andre grunde, er straffen bøde. Under i øvrigt formildende omstændigheder kan straffen bortfalde.
Stk. 2. Forsøg på forbrydelse, der er omfattet af stk. 1, er strafbart.'

cannot be proven. Based on the wordings of the laws, Finland is the only country in which fraud with the purpose of harming the victim is enacted as punishable. This widens the scope of the application of the Finnish fraud provision compared to the other countries. The harm here is considered to be financial in nature.[40] Norway, on the other hand, is the only country in which also gross negligent acts are punishable. This in a way, too, widens the scope of criminalization. However, it does not provide any new forms of the act under the crime provision but only lowers the level of fulfillment of the subjective guilt in the existing descriptions of the act. In Finland and Sweden, the person, to whom the action or inaction performed under the erring must cause financial damage or the danger of it, must be the victim or someone for whom the victim is acting. In Norway and Denmark the party suffering the damage is not as accurately defined as in Finland and Sweden.

The fulfillment of all Nordic fraud provisions requires formation of direct financial damage.[41] The financial damage may occur as a result of a direct decrease of assets or as unreceived financial profit, the danger of which is also enough to fulfil the requirement of direct financial damage in Finland and Norway. There must be a direct causality between the erring, the action or inaction resulting from it and the damage originating from them.[42]

Causality defines what is required from the relation of the conduct and the consequence for criminal liability to actualize.[43] Causality exists if the conduct has been necessary to the formation of the result.[44] The starting point is that if several separate contributions exist to endeavour the same result they do not exclude each other, but all of them individually are seen as adequate to have caused it.[45] If a single act is considered to be inadequate in order to cause the consequence it is evaluated in relation to other factors affecting the actualization of the consequence. This single act needs to be a necessary part of these other factors. Together these factors are adequate to cause the consequence.[46] Physical causality means that a certain act primarily leads to the same result in every situation. Mental causality is in question when a person gives a reason to decide in a certain way to another, and this decision leads to the result. Judicial causality is at hand when the connection between the act and the result is formed with the help of the crime provision.[47]

Regarding the online sale of counterfeited goods, situations in which a consumer has known about the counterfeit nature of a product are irrelevant from the point of view of the fraud provisions because of the lack of erring in the situation.

---

40 HE 66/1988 vp, at 131-132.

41 In case Högsta domstolen (The Supreme Court of Sweden) NJA 2016:4, judgment of 24 February 2016 (fraudulent bid) the requirement of direct financial damage was seen to be fulfilled by the perpetrator's fraudulent bid causing the buyers to pay a higher price for the right of residence than they would have without the false bid. NJA 2016:4, paragraphs 19 and 20. In case KKO 2003:88, judgment of 3 October 2003, judgment of direct financial damage has been at hand when the companies in question did not in reality receive the additional rights to use a computer program due to the modifications done by the perpetrator to the original product.

42 S. Schjølberg, *Cyberkriminalitet*, Universitetsforlaget 2017, at 91; HE 66/1988 vp, p. 132.

43 K. Nuotio, *Teko, vaara, seuraus. Rikosvastuun filosofisista, kriminaalipoliittisista ja lainopillisista perusteista,* Suomalainen Lakimiesyhdistys 1998, p. 273.

44 L. B. Langsted et al., *Criminal law in Denmark*, Kluwer Law International 2014, at 49.

45 J. Tapani and M. Tolvanen, *Rikosoikeuden ylenen osa. Vastuuoppi*, Talentum 2013, at 164-169.

46 P. Asp et al., *Kriminalrättens grunder*, Iustus Förlag 2013, at 78-89; J. Tapani and M. Tolvanen 2013, at 168.

47 D. Frände, *Yleinen rikosoikeus*, Edita 2012, at 71-77; J. Tapani and M. Tolvanen 2013, at 170-173; N. Jareborg, *Allmän kriminalrätt,* Iustus Förlag 2001, at 161 and 235-236. For more about the specific content of the doctrine in different Nordic countries see, e.g. K. Nuotio 1998, at 272-282; J. Tapani and M. Tolvanen 2013, at 163-173; P. Asp et al. 2013, at 78-89; J. Andenæs, *Allminnelig strafferett,* Universitetsforlaget 2016, at 125-137; L. B. Langsted et al. 2014, at 49-50.

If a consumer has simply been uninterested in the originality of the product, it is likely that the requirements of erring and acting or not acting under the erring will not be fulfilled. If the counterfeit nature of the product is irrelevant to the consumer, he most likely would not have acted any differently, even if the nature of the product had been verified. Therefore, the consumer would not have erred and the erring would not have affected his action or inaction, and the essential elements of fraud will not be fulfilled. However, depending on the perpetrator's efforts, the attempt of fraud might be in question.

The clearest situation of fulfilling the fraud provision in this field is when the consumer without knowing purchases online what he thinks to be original goods and the purchase of the counterfeited product itself causes the financial damage. More challenging by interpretation are incidents in which the counterfeited products mostly cause harm to health or safety. For instance, if a consumer unwittingly buys counterfeited brake pads or other engine parts of a car that break in the middle of driving and cause an accident by making the driver lose control of the car. Which of the resulting damages if any are a direct financial consequence of the fraudulent activity that is the sale of the counterfeited component? Other elements of fraud are fulfilled in the situation because the consumer has erred in regard to the originality of the product, and due to this erring he has decided to buy the counterfeited product. By adding the infringing trademark, the perpetrator has actively erred the victim into believing that the sold product is an original one. He has also had the aim to gain unjustifiable financial profit for himself from the sale because he has not given the products to the buyer free of charge and has not been entitled to the profits for the use of the trademark.

The damages that the example situation could for instance cause are damage to the car itself, damage of property into which the car runs, injury to the driver, who here is assumed to be the same person who purchased the counterfeited goods, and injury to a third person. The damage required in the fraud provision is direct financial damage, which may occur as a direct decrease in the economic value of property, unreceived financial gain or the danger of them. This definition of direct financial damage rules out personal injuries. The damage that the car causes to property into which it runs is a direct consequence of the driver losing control of the car but an indirect consequence of the counterfeited engine part breaking. The only direct consequence of the counterfeited engine part breaking is the damage to the car itself, which could be considered as a decrease in the economic value of the property. But, the question still remains: can this decrease be considered a direct consequence of the erring of the victim on the origin of the product and the purchase of the product based on this erroneous conception? This could be the case as there is a danger of the decrease at hand taking place immediately after the counterfeited engine part has been installed in its place, and also the mere danger of the financial damage is enough to fulfil the essential elements.[48] However, counterfeited engine parts do not always break. It is impossible to say for sure what is the probability of counterfeited engine parts breaking in comparison to original engine parts and through that make certain that an actual risk of financial damage is present.

The evaluation becomes slightly different regarding the other example group of goods. If a consumer buys a counterfeited food product online which causes an allergic reaction or intoxication, for instance, due to an allergen or some other legal substance left unmentioned in the ingredients and forces the victim to seek medical care, does the conduct of the counterfeiter fulfil the essential element of fraud? As

48 See, e.g. KKO 2003:88, judgment of 3 October 2003.

above, the active erring element is fulfilled by adding the protected trademark on the counterfeited product, and the erring has lead to the consumer to err and act based on this erring by purchasing the counterfeited product as an original one. The counterfeiter has yet again profited from the sale of the illegitimate product, which indicates the aim to gain unjustified financial benefits. The requirement of direct financial damage seems to stay unfulfilled. There is no decrease in the financial value of property or loss of financial gain nor is there danger of them at hand. The only damage caused to the victim is the personal injury and the costs of medical care related to it. It can, of course, be pondered whether or not the hospital costs could be considered as a decrease in the victim's assets and therefore, as financial damage, but it seems a little far-fetched. The situation becomes even more difficult in some countries if the person consuming the food product is not the same person who purchased it.

In light of these examples it appears that the Nordic fraud provisions do not optimally answer the threats of the online sale of counterfeited products and should, therefore, be developed to fit better into the changing operational environment. Fraud is, traditionally, an economic crime, and the sale of counterfeited goods is an economic activity with health and safety dimensions. In light of the developments in crime, I would suggest reconsidering the limitation of damage caused by fraud that fulfils the essential elements of the crime. Currently, only direct financial damage or the danger of it can fulfil the fraud provisions. Instead, the requirement of damage should be widened to include also direct damage to property and injury to a person (and the danger of them).

4 Conclusions

The chapter studied the online sale of counterfeited goods from the point of view of criminal law. It compared the Nordic fraud provisions and studied their applicability in the situation with the examples regarding food and spare parts. In all, it seems safe to say that the applicability of the Nordic fraud provisions in the example situations is, at the least, questionable. The problem seems to be in fulfilling the fraud provisions' requirement of direct financial damage.

The sale of counterfeited food and spare parts cause serious threat to health and safety. The trademark crime provisions are designed to enable right–owners to combat the wrongdoings that target their trademarks, and therefore consumers' interests are not acknowledged in them. Widening the scope of trademark crime provisions to cover wrongdoings to third parties would not fit into the purpose of trademark legislation.

Fraud provisions could serve as an answer to the existing inconsistency. However, they need to be developed further to be fully applicable to the field in question. One way of executing this could be by modifying the requirement of the actions or inaction causing direct financial damage or the danger of it into the requirement of causing direct damage or the danger of it, including both direct damage to property and direct damage to a person. This would not hinder the spirit of fraud provisions, for it would still remain economic activity being the cause of the damage. It is justifiable that perpetrators, who cause personal injuries by trying to gain unjustified financial benefit at the expense of others, are punished also for the consequences of their actions.

From the point of view of the perpetrator, the Nordic systems do not vary enough in regard to their threats of penalty in general and descriptions of the act to say that it would be easier or more tempting to commit a crime in one Nordic country over another. The descriptions of the act are rather similar, with few variations. In Sweden, the erring part of the fraud provision is not as easily fulfilled as in other countries because the passive taking advantage of the victim's erring is not included in the criminalization. In Norway and Denmark, the circle of people to whom the conduct must cause financial damage is wider than in Finland and Sweden, which simplifies the fulfillment of the element. The description of the act is the widest in Finland with the element of the purpose of harming in addition to the purpose of gaining financial benefit fulfilling the fraud provision. The problems regarding the element of direct financial damage are similar in every country.

However, the highest maximum penalties, that is the maximum penalties for aggravated fraud, vary a great deal. From that point of view, Finland is the most intriguing option for perpetrators, with the threat of a maximum penalty of four years of imprisonment, whereas in Denmark the threat of a maximum penalty rises to eight years of imprisonment for the same act. It is, though, interesting that the Danish basic form of act is punishable with a lower maximum sentence (one year and six months of imprisonment) than basic frauds in other countries (two years of imprisonment), while the highest maximum sentence of all is still in Denmark. Another interesting observation regarding threats of penalty relates to the Norwegian gross negligent fraud provision. The application of it leads to the unusual situation where the maximum penalty is higher for f a gross negligent act than for an intentional act. This is odd, because intentional acts should be considered more reprehensible than gross negligent acts, which is usually shown in the penal scale.

LOCAL AND GLOBAL CHALLENGES IN THE FIGHT AGAINST CYBERCRIME

Global and European Responses to Cybercrime

Peter Sund

1 Introduction

1.1 Setting the Frame

Professor Jarno Limnéll stated in his address at the Tallinn Digital Summit[1] for the EU heads of state that the future of European digital era, inseparable from digital security, is constructed from the elements of *trust, cooperation* and *responsibility*. Cyber security,[2] or more plainly *digital security*, has quickly become one of the most challenging domains of security.[3] Security is understood here as the absence of those things which are intentionally caused and can harm us, e.g. crime in particular. Digitalization as a whole, including digital networks, the Internet and all that is related to it is sweeping through developed societies and surreptitiously under the surface of developing countries as well. 'Everything that can be digitalized will be digitalized.'[4] The pace is overwhelming. If the former holds true, it means that in addition to societies and nations being digitalized, crime is being digitalized as well. As is stated in the EU information security Directive:

1 Organized by the Estonian Presidency of the Council of the European Union in cooperation with the President of the European Council and the European Commission on 29 September 2017.

2 Cyber-security commonly refers to the 'safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein'. See Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace* (2013). JOIN(2013) 1 Final.

3 For instance a UN panel of governmental experts conclusions, noting: '– – existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century – – Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole.' See Report of the *Group of Governmental Experts on Development in the Field of Information & Telecommunication in the Context of International Security*, 65th Session. UN Doc. A/65/201 (July 30, 2010); Also, A/68/98 (24 June 2013) of the same: 'Information and Communication Technologies (ICTs) have reshaped the international security environment. These technologies bring immense economic and social benefits. ICTs can also be used for purposes that are inconsistent with international peace and security, producing a noticeable increase in risk in recent years as they are used for crime and other disruptive activities.' Also, A/70/174 (22 July 2015) of the same: '*An open, secure, stable, accessible and peaceful ICT (Information and Communications Technology) environment is essential for all, and requires effective cooperation among States to reduce risks to international peace and security.*'

4 Professor of J. Limnéll (Cyber Security, Aalto University). Lecture on *Cyber Security* (at European Security and Defence College High Level Course, Tampere, 7 March 2017).

> *The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user-confidence and cause major damage to the economy.*[5]

> *The borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation. While the private sector should continue to play a leading role in the construction and day-to-day management of the Internet, the need for requirements for transparency, accountability and security is becoming more and more prominent.*[6]

There are certain elements (here called *cyber laws-of-nature*) in cyberspace that are fundamentally different from the physical space of atoms: the absence of time, distance and identity as well as the asymmetric and highly effective nature of the digital environment in comparison to the physical space. The success of *digitalization*, here understood as a digitally interconnected world, lies ultimately on something as simple as *trust*. Or to put it in other words: the lack of trust has the potential to critically disrupt the use of digital services, applications and data and the reliance on them. The trust is generated by individual human beings outside the digital world but realized inside cyberspace. If the projections of the digitalization, or the third industrial revolution as some call it, remain valid, then what are the consequences in terms of trust and confidence if and when even any meaningful digital content (in cyberspace) is suddenly jeopardized, i.e. inaccessible, corrupted/altered, repudiated or its confidentiality breached? What happens for example to the economic human activity in cyberspace?

Furthermore, as widely accepted and strongly argued by Daron Acemoğlu and James Robinson, states' prosperity (including economic prosperity) lies strongly in their ability to maintain inclusive institutions that uphold rules that thus create trust, i.e. confidential relationships, which results in economic growth.[7] Antti Lamberg argues the same from the other end. First, economic activity decreases, there is less tax revenue and then the institutions and rules start to get bogged down.[8] One can only imagine the consequences for digitalized nations when the prevailing digital environment for economic activity becomes unstable. Just think of the potential consequences of major contemporary cyber threat trends, such as the increase of ransomware, exploitation of digital vulnerabilities, corporate inner circle attacks, attacks endangering business continuity, theft of personal data, (targeted) phishing, online fraud, denial of service attacks and so on.[9] Limnéll argues that:

---

5 See for instance Directive (EU) 2016/1148 of The European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, preamble (2), at 1.

6 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (2013). JOIN(2013) 1 Final, at 3.

7 See, e.g. J. Kramer, *Inclusive Institutions Key for Economic Growth, by St. Gallen Symposium* (Huffington Post 20 March 2016). Available at: https://www.huffingtonpost.com/st-gallen-symposium/inclusive-institutions-ke_b_9510688.html

8 N. Vartiainen, *Suomalaistutkija varoittaa: Rooman tuhon kaltainen katastrofi voi toistua, kun väestönkasvu lakkaa* (Helsingin Sanomat [newspaper], Economic news 9 July 2017).

9 M. Lehto, J. Limnéll, E. Innola, J. Pöyhönen, T. Rusi and M. Salminen, *Finland's cyber security: the present state, vision and the actions needed to achieve the vision* (Prime Minister´s Office: Publications of the Government´s analysis, assessment and research activities 30/2017) at 12.

> *Analysis in recent years demonstrates that government responses to cyber attacks vary widely. Although there has been significant political pressure to "do something," past experiences illustrate that most policy responses are ad hoc. – – This indicates that cyber domain is a relatively new arena of conflict—especially for the policymakers—and, therefore, special attention should be directed towards it, and more research is needed to understand how nation-states could best respond to cyber hostilities – –.*[10]

The UNODC[11] has raised the same issue, although from the developing countries' point-of-view: 'considering *weaponization* of cyberspace and the impact that it could have, especially on developing countries, could be enormous. A significant cyber attack on a country that had no real capability to respond to a threat to its critical national infrastructure could cause immediate and long-standing impact.' [12]

The law is said to be slow to change.[13] Hence, international law may be even slower in that regard. In comparison to cyberspace's staggering speed of change, the development of regulation can be seen as the *tortoise* in the race against the *rabbit* (i.e. cyberspace). In the story, the rabbit was overconfident in its running speed, and while being distracted from the race itself, he failed to notice the slow but constant pace of the tortoise. He lost the race. We can read this story in two ways: either we may rely on the assumption that cyberspace will eventually 'collapse' as a result of reaching the breaking point of *distrust* (due to anarchy, impunity and lack of control), and only by rebuilding it will the necessary regulation catch up and take a final 'win' over it. If it does not, then we can admit that the regulation will not be able to catch up. In the case of the latter, the way to gain control – to arrive at the goal, even if in second place – is to assume that there is an *ending* to the race. Will there be a saturation point in the evolution of cyberspace? That shall remain an open question for now.

Whatever the case may be, there is no way around the fact that the race is already on-going.[14] For States, the critical success factor seems to be to develop adequate regulatory and control responses to internalize and adapt to the cyber laws-of-nature. However, as distances do not matter in cyberspace, the threat may, or should, be expected to arise as cross-border or *cross-jurisdictional* by default. Thus, the true and critical success factor really is to develop *joint international* regulatory and control responses to adapt to the ever-so-different cyber laws-of-nature. This article focuses on the global and European responses to cybercrime, and in particular as a part of cyber security from regulatory, institutional and procedural perspectives. Thus, also institutions such as structures or mechanisms of social order governing the behaviour of people are discussed. Institutions are a central concern for law, which is the formal mechanism for political rulemaking and enforcement. In essence, this article targets the elements of *cooperation* and *responsibility*[15] in cybercrime.

---

10 J. Limnéll, *Proportional Response to Cyberattacks* (Cyber, Intelligence, and Security, Volume 1, No. 2, June 2017) at 37.

11 United Nations Office on Drugs and Crime.

12 *In wake of 'WannaCry' attacks: UN cybersecurity expert discusses Internet safety* (UN News Centre 19 May 2017). Available at http://www.un.org/apps/news/story.asp?NewsID=56796#.WbscUa1IYVw

13 For instance R. Bravo, *Legal Initiatives to Fight Cybercrime and Cyber Threats* (7th EIN International Symposium, Military Academy, 29 May 2013); H. Tiesmaa. Kyberrikollisuutta on voitava torjua tehokkaasti (Akkusatoori 2/2016) at 34.

14 For instance Cybercrime Programme Office of the Council of Europe (C-PROC), *How Will New Cybersecurity Norms Develop?* (Cybercrime Digest, 1-15 March 2018) at 2.

15 In the meaning of responsibilities of States and Government structures.

1.2 Definitions and Specificities

There are no common definitions of cybercrime, digital crime and computer crime or internet crime. Often cybercrime, or simply computer crime, is referred to any illegal action that involves a network or computer. In this sense, the network or computer may be used to commit a crime or may be the target of a crime. Other, narrower, definitions include Roscini's: 'offences against the confidentiality, integrity and availability of computer data and systems committed by individuals or private entities for personal gain.'[16] From a practical law enforcement perspective, it may not be the most important issue to deal with, as long as everyone knows what is meant by somewhat equivocal or interchangeable terms. Practically speaking, in determining what is cybercrime, the first step is to evaluate whether an illegal action was committed. The second step is then to determine whether the action was committed through the use of or against a computer or network. Other constituent elements still remain somewhat debatable.

However, from legal, especially from the application of international law, and research perspectives the issue seems to have a clear significance. For instance, even the fact that national law enforcement authorities, such as the police in Finland or elsewhere, might apply differing definitions and categorizations, or for instance Europol at the multinational level, may cause challenges in dealing with the issue at least on a statistical, research and policy-setting level. Furthermore, 'a multitude of definitions will inescapably lead to diverging views on both the application and the progressive development of [policy and] law, causing also uncertainty as to what (currently or ideally) would constitute for instance unlawful behaviour, be it by individual or by even a State, such as cyber attacks.'[17] For this reason, it can hardly be surprise that the disagreement amongst experts at the definitional level is equally present at the operational level.

However, from an operational perspective and within the framework of criminal law it may well be enough to ascertain that those definitions of crime's constitutive elements included in the penal code would suffice current and near future needs for the law enforcement and judicial authorities to effectively seek to deal with the phenomenon. Conversely, in terms of international law enforcement cooperation, the caveat may still exist if and when there are inconstancies between the statutory stipulations of various cybercrimes in different jurisdictions.

In order to be able to formulate a situational awareness on cybercrime, the police in Finland have been classifying cybercrime as either crime directly targeting the digital environment formed by various interdependent computer systems or as crimes where these systems have been used as a means to commit other types of crimes.[18] The Finnish prosecution service classifies cybercrime as crimes committed in computer networks and in which the evidence is based on digital records.[19] As noted earlier, the intrusion of the digital environment into virtually all human activities may cause difficulty in the future to maintain these classifications: more and more different crimes may be committed in, via or against the digital environment. Consequently, it seems that an additional classification filter has been introduced, noting

16 C. Vossen, *Cyber Attacks Under the United Nations Charter* (Critical Reflections on Consequentialist Reasoning, 2014) at 13. Available at SSRN: https://ssrn.com/abstract=2594675 or http://dx.doi.org/10.2139/ssrn.2594675

17 C. Vossen, *supra* note at 18. Available at SSRN: https://ssrn.com/abstract=2594675 or http://dx.doi.org/10.2139/ssrn.2594675

18 Ministry of the Interior [Finland]. *Inquiry on the Fight Against Cybercrime* (Internal Security Publication Series, 14/2017).

19 H. Tiesmaa. *Kyberrikollisuutta on voitava torjua tehokkaasti* (Akkusaattori 2/2016) at 34.

that an offence is considered as a cybercrime *only* when the offence is committed within cyber space.[20]

Other classifications, such as the one used by Europol, are based mainly on legal limitations in terms of the jurisdiction provided for the Agency by the Treaties of the European Union[21] and Regulation on Europol[22] as well as the EU Council framework of the EU Policy Cycle for organized and serious international crime.[23] At the level of operations, the Europol focuses on cybercrimes that: 1) are committed by organized crime groups, particularly those generating large criminal profits, such as online fraud; 2) seriously harm victims, such as online child sexual exploitation; and 3) impact critical infrastructure and information systems in the EU, including cyber attacks.[24]

Furthermore, Europol seems to view the definition of cybercrime as existent 'only when the offence is committed within cyber space' as just one category of cybercrime. Europol defines this kind of crime as 'cyber-dependent crime', meaning any crime that can only be committed using computers, computer networks or other forms of information and communication technology (ICT).[25]

On the other hand, cyber security classifications may include lists of cyber threats such as hacking/hactivism, cybercrime, cyber espionage, cyber terrorism, cyber warfare etc.[26] The challenge of these classifications is that from legal and law enforcement perspectives virtually *all* of the threats and related behaviours fall into the scope of criminal law, which are thus defined as (cyber)crimes, regulated and addressed under the Penal Code of the State (see section Regulatory Framework). Consequently, they are also controlled by the criminal policy of a particular State. To avoid any misconception, various common or joint criminal policy formulations have taken place on a supra-national level as well. These are, however, usually part of *soft law* and thus binding only at the political level. This is discussed later.

Despite well-formulated declarations and criminal policies it seems that neither national nor international law enforcement and judicial mechanisms have been able to address cybercrime effectively in the meaning of stopping crimes, dismantling criminal organizations and bringing the culprits to justice.[27] The analysis done by Europol further shows that 'there is a progressive convergence of cyber and serious and organised crime, supported by a professional underground service economy.'[28]

---

20 A. Leppänen, K. Linderborg and J. Saarimäki, *Tietoverkkorikollisuuden tilannekuva* [Situational Awareness of Cybercrime] (Publications of the Government´s analysis, assessment and research activities 17/2016) at 8.

21 Treaty on the European Union (2010) articles 3–5; Treaty on the Functioning of the European Union (2010) articles 67, 83, 87 and 88; Charter of Fundamental Rights of the European Union (2010), art. 49.

22 Regulation (EU) 2016/794 of the European Parliament and of The Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, art. 3 (1) and related Annex I.

23 Council (EU) Conclusions on the creation and implementation of an EU policy cycle for organized and serious international crime, doc. 15358/10.

24 Europol, European Cybercrime Centre. Available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Accessed 29 September 2017).

25 See European Union Agency for Law Enforcement Cooperation (Europol), Internet Organised Crime Threat Assessment IOCTA 2017), at 18.

26 See for instance J. Limnéll, K. Majewski, M. Salminen, *Cyber Security for Decision Makers* (Helsinki Docendo, 2015); R. Bravo, *From the Spectrum of Conflict within Information Networks: towards a Conceptual Reconstruction* (Polícia Judiciária, 2010).

27 See, e.g. Europol IOCTA 2015: '– – While many aspects of cybercrime are firmly established, other areas of cybercrime have witnessed a striking upsurge in activity, including (computer network) attacks on an unprecedented scale, as cybercrime continues to take new forms and new directions – –'.

28 *Ibid*. p. 10.

Actually, it rather seems that the focus has quite substantively turned towards a more defence-oriented security focus. This change in focus and policy setting may also be the reason for why the responsive strategies have also turned towards the development of *resilience* instead of fighting against cyber crime (investigating, prosecuting and preventing criminal acts). Mikko Hyppönen, the Research Director of F-Secure, a Finnish cyber security company, stated in a lecture in Helsinki already in 2006 that fighting cyber crime effectively would require the establishment of some sort of 'joint European cyber police.'[29] Seemingly, the development of such capacity has taken more time and effort than the evolution of cyber criminal environment would have allowed. On the other hand, the control responses are not running idle but are advancing on all fronts: the regulatory, the institutional capacity and procedural practices.

1.3 Persistent Challenges in Cyberspace

The presence of cyber crimes relies heavily on the Internet and online activity, and as a result regulations and oversight of this type of activity has been expressed in the spectrum of cyber law, which is a fairly expansive legal field that consists of a variety of avenues and jurisdictions, including the ethical and moral use of the Internet for lawful purposes. Cyber law is considered to be one of the most recently developed legal fields as a result of the on-going advent of computer-based technology.

In terms of the development of the regulatory framework there has been limited success on addressing those issues constituting the challenges of cyber security. Those challenges could be divided into two domains: static and variable challenges.

Static challenges may be seen in relation to the permanent qualities of the digital environment (cyber laws-of-nature): the absence of time, distance and identity as well as the asymmetric and highly effective action in the digital environment when compared to the physical space. Asymmetric in this context means that the build-up of an attack may be undetectable, and once occurred it may be impossible to determine its origin. The term effective refers to the low-cost/high-impact nature of illegal cyber activities, such as computer network attacks, the release of confidential information or online frauds, as there is no need for a lot of financial capital, manufacturing power or other forms of physical material or equipment.[30] At its simplest, only a rather inexpensive computer, Internet connection and some time and patience to learn about software, hardware and network vulnerabilities would suffice. A lot of the intellectual capital is already in cyber space for anyone to utilize freely.

The important issue here is to note that the static challenges are those where little development has taken place in terms of mitigation. Naturally, as ICT technology is purposefully used to overcome time and distance, those attributes are inherent qualities of cyber space, and thus it makes very little sense in trying to slow down the data in cyber space. The response developed so far has been to retain some data (data retention or expedited preservation of stored computer data) for possible later access. Similarly, options to work around the challenges of distance in cyber space have been to bolster cross-border law enforcement and judicial cooperation, cyber intelligence and remote extraterritorial searches. Some rather extreme policy suggestions may have taken place to isolate for instance complete States from external connections. Cross-border law enforcement is discussed latter in more detail.

29 At Haaga-Helia University of Applied Sciences.
30 See, e.g. M. Lehto *et al*., *supra* note at 13.

In terms of identity in cyberspace there have been efforts to create more effective ways to identify cyber actors. Nevertheless, the issue seems to remain as equally challenging as before. There are two main issues to identity in cyber space: firstly, a digital identity (such as IP address or other individual ID of a particular device) and, secondly, the physical identity of the natural person using the device or network. There are a multitude of ways for trying to stay anonymous and hiding a person's digital identity. Methods used in web browsing include proxy servers, shared IP addresses by carrier-grade network address translation (NAT), virtual private networks (VPN) or The Onion Router (TOR). Anonymity is also related to activities in the darknet.[31] For email and communication there are ways such as using an alias and/or disposable email accounts, VPN and/or HTTPS Web-based email clients, Pretty Good Privacy (PGP) software, TOR chat or Cryptocat chat clients etc.

Without going into technical details or to issues on the ever-ongoing competition between state security actors and white hat hackers against malicious actors, the point is that anonymity has so far been, and probably also will be, a significant issue for political debate. Regulatory efforts have not really taken place in an effort to ban anonymity in cyber space. Thus, anonymity technologies are most likely not going away in the foreseeable future. The issue of anonymity may also become even more challenging due to new European regulation concerning EU data protection, which is without any doubt intended to improve security in cyber space generally but may in some cases actually decrease it. The EU General Data Protection Regulation (GDPR)[32] seems to conflict with the Internet Corporation for Assigned Names and Numbers (ICANN) *Whois* database service, also called the phone book of the Internet. The GDPR, which is set to take effect in the European Union on May 25, 2018 could make revealing personal information about website owners in Whois illegal in the EU jurisdiction.[33] This would naturally hinder any law enforcement efforts in Europe.

The second major issue, the physical identity of a user of a network device or piece of technology (connecting the two identities) will certainly remain a significant challenge despite any possible regulation on digital identity. Law enforcement community is ever more challenged by the issue. It can be expected that new investigative methodologies will face legal limitations, and thus there will be a call for new regulations to establish jurisdiction and to allow the utilization of these methodologies and technologies in the fight against crime.

Variable challenges on the other hand are challenges prone to change over time due to active mitigating efforts and development, as well as to overall evolution of cyberspace. These challenges include for instance: 1) a lack of international approximation of applicable penal and procedural regulation;[34] 2) intellectual property rights (IPR) and the attribution of information ownership;[35] 3) internet governance;

---

31 The darknet consists of content in overlay networks, which use the Internet but require specific software, configurations or authorization to access. The darknet forms a small part of the deep web, the part of the Web not indexed by search engines. See Joint Communication to the European Parliament and The Council. *Resilience, Deterrence and Defence: Building strong cyber security for the EU* (JOIN(2017) 450 final, 13 September 2017).

32 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).

33 Cybercrime Programme Office of the Council of Europe (C-PROC), *Cybercrime Diges*t (1-15 March 2018) at 2.

34 UN Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2014) at 52.

35 *Ibid*.

4) complex multi-stakeholder security environment; and 5) debates and approaches between risk or control-based management strategies.[36]

2 Institutional Framework

2.1 Global Institutions

The institutional framework is an effort to illustrate the relevant international structures and institutions and their main, somewhat permanent, processes that address or contribute to cybercrime. The presentation is by no means comprehensive and may have, in addition to deficits in recognizing certain institutions, excluded institutions which may only have a secondary or indirect relation to the fight against cybercrime. Hence, these institutions are not considered to be at the core of tackling cybercrime.

The United Nations (UN) System

The term UN System refers to the United Nations' main structure (principal organs) as well as to all its funds and programmes, research and training institute. In addition, it refers to other bodies, such as United Nations Office on Drugs and Crime (UNODC), United Nations Development Programme (UNDP) and the United Nations Interregional Crime and Justice Research Institute (UNICRI) as well as to the specialized agencies, such as International Telecommunication Union (ITU) and World Intellectual Property Organization (WIPO).

The UN System has the potential to operate on many fronts in regard to cyber security and cybercrime, which have been discussed earlier in this article. However, as the UN System has essentially, aside from the efforts of ITU (HLEG and GCI) discussed earlier, not been able to provide significant advances in relation to regulatory aspects of cybercrime, only the roles of the following will be discussed in more detail: ITU; UNODC; Chief Executives Board for Coordination (CEB); UN Conference on Trade and Development; Commission on Crime Prevention and Criminal Justice; and the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

International Telecommunications Union (ITU)

ITU is the United Nations' specialized agency for information and communication technologies – ICTs. It allocates global radio spectrum and satellite orbits, develops the technical standards that ensure networks and technologies seamlessly interconnect and strives to improve access to ICTs to underserved communities worldwide. ITU maintains the Global Cybersecurity Index (GCI), which is a survey that measures the commitment of Member States to cyber security in order to raise awareness. The GCI is included under Resolution 130 (Rev. Busan, 2014) on strengthening the role of ITU in building confidence and security in the use of ICT. The GCI revolves around the ITU Global Cybersecurity Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building and cooperation). ITU, together with international partners from the private-public and the private sector as well as

36 *Ibid*. at 55.

academia, established the GCI with the key objective of building capacity at the national, regional and international level. This was to be done through assessing the engagement level of countries on cybersecurity and using the gathered data to produce a list of good practices that can be used by countries in need.

Chief Executives Board for Coordination (CEB)

Under the chairmanship of the Secretary General, the CEB provides coordination and strategic direction for the system as a whole in areas under the responsibility of executive heads. Focus is placed on inter-agency priorities and initiatives, while at the same time ensuring that organizations' independent mandates are maintained. The CEB database[37] provides a documentary reference search for cybercrime related issues in the UN System.

In recognition of the increasing concern among the agencies of the United Nations system regarding cyber security and cybercrime, CEB, through its High-level Committee on Programmes, endorsed a United Nations-wide framework on cyber security and cybercrime in November 2013. The framework establishes principles for programme development activities related to cybercrime and cyber security as well as for better coordination among United Nations entities on this issue in support of Member States. When it reviewed the information security landscape during its second regular session in November 2013, CEB focused its deliberations on:

> *The role that United Nations system organizations can play, both individually and collectively, to support intergovernmental deliberations relating to cyber security, cybercrime and information policies. To further these efforts, CEB agreed that United Nations system organizations would work together to develop a system-wide comprehensive and coherent strategy to support agencies as they address the challenges of cyber security, cybercrime and policies on information.*[38]

UN Conference on Trade and Development (UNCTAD)

UNCTAD is a permanent intergovernmental body established by the United Nations General Assembly in 1964. UNCTAD is part of the UN Secretariat and reports to the UN General Assembly and the Economic and Social Council, but it has its own membership, leadership and budget. UNCTAD maintains a reference database on Cybercrime Legislation Worldwide.[39]

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[40]

The Group's mandate is to study, with a view to promoting common understandings, the following: existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures; the issues of the use of information and communications technologies in conflicts and how international law applies to the use of information and communications technologies by

37 Available at http://www.unsystem.org/ (Accessed 29 September 2017).

38 Chief Executives Board for Coordination (CEB). *Report on Addressing cybercrime and cybersecurity*. Available at: http://www.unsystem.org/content/addressing-cybercrime-and-cybersecurity (Accessed 29 September 2017).

39 UNCTAD, *Organization*. Available at http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx (Accessed 29 September 2017).

40 The Group was established pursuant to paragraph 4 of General Assembly resolution 68/243 (2014).

States; and the international concepts aimed at strengthening the security of global information and telecommunications systems.

The Group has concluded that international law, and especially the UN Charter, applies to state activity cyberspace and agreed to four peacetime norms: States should not interfere with each other's critical infrastructure; they should not target each other's computer emergency response teams; they should assist other nations investigating cyberattacks; and they are responsible for actions that originate from their territory.[41] However, the progress of the Group seem to have reached a dead-end in 2017 seemingly due to major States such as China and Russia taken clear back-steps from earlier agreements.[42]

Commission on Crime Prevention and Criminal Justice (CCPJ)

CCPCJ was established by the Economic and Social Council (ECOSOC) resolution 1992/1, upon request of General Assembly (GA) resolution 46/152, as one of its functional commissions. The Commission acts as the principal policymaking body of the United Nations in the field of crime prevention and criminal justice. ECOSOC provides for the CCPCJ's mandates and priorities in resolution 1992/22, which include improving international action to combat national and transnational crime and the efficiency and fairness of criminal justice administration systems. The CCPCJ also offers Member States a forum for exchanging expertise, experience and information in order to develop national and international strategies and to identify priorities for combating crime. The CCPCJ functions also as a governing body of the United Nations Office on Drugs and Crime (UNODC) and approves the budget of the United Nations Crime Prevention and Criminal Justice Fund, which in turn provides resources for technical assistance in the field of crime prevention and criminal justice worldwide.

In recent years the CCPJ has issued the following declarations: 1) Resolutions 26/4 (2017)[43] and 27/7 (2013)[44] on Strengthening international cooperation to combat cybercrime; 2) Resolution 22/8 (2013)[45] on Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime; and 3) Resolution 20/7 (2011)[46] on Promotion of activities relating to combating cybercrime, including technical assistance and capacity building.

United Nations Office on Drugs and Crime (UNODC)

The UNODC is mandated to assist Member States in their struggle against illicit drugs, crime and terrorism. In the Millennium Declaration, Member States also

41 UN General Assembly, doc. A/70/174, 22 July 2015, Seventieth session, item 93 of the provisional agenda. *Developments in the field of information and telecommunications in the context of international security*.

42 Council on Foreign Relations. *The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?* (29 June 2017). Available at https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what (Accessed 28 September 2017).

43 CCPJ declarations. Available at: http://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_26/CCCPJ_Res_Dec/CCPCJ-RES-26-4.pdf

44 CCPJ declarations. Available at: http://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-7.pdf (Accessed 29 September 2017).

45 CCPJ declarations. Available at: http://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-8.pdf (Accessed 29 September 2017).

46 CCPJ declarations. Available at: http://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2011/CCPCJ/Resolution_20-7.pdf (Accessed 29 September 2017).

resolved to intensify efforts to fight transnational crime in all its dimensions, to redouble the efforts to implement the commitment to counter the world drug problem and to take concerted action against international terrorism. The three pillars of the UNODC work programme are: field-based technical cooperation projects to enhance the capacity of Member States to counteract illicit drugs, crime and terrorism; research and analytical work to increase knowledge and understanding of drugs and crime issues and expand the evidence base for policy and operational decisions; and normative work to assist States in the ratification and implementation of the relevant international treaties, the development of domestic legislation on drugs, crime and terrorism and the provision of secretariat and substantive services to the treaty-based and governing bodies.[47]

UNODC maintains a repository of cybercrime containing a listing of lead institutions of UN Member States as well as good practice and lessons learned that are relevant to the application of criminal justice.[48] UNODC has also released Comprehensive Study on Cybercrime in 2014 pursuant to the request made by the General Assembly already in 2010.[49]

The International Criminal Police Organization (ICPO-Interpol)[50]

In the history of police investigations of computer crime and cybercrime, Interpol has since the 1980s been the leading international police agency in this field. Interpol has established *Regional Working Parties* for regions in Africa, Asia, Latin America and Europe. These working parties consist of the heads or experienced members of national computer crime units. Interpol has established a rapid information exchange system for cybercrimes. This is an international 24/7-response system including National Central Reference Points (NCRPs) in more than 120 countries for a global cooperation on cybercrime investigation that also has been endorsed by the G8 High Tech Crime Sub-Group. The 24/7-system enables police in one country to immediately identify experts in other countries and obtain assistance in cybercrime investigations and evidence collection. Interpol has also established the Global Complex (IGC), based in Singapore. The IGC is an integral part of Interpol's efforts to reinforce its operational platform and is mandated to focus on developing innovative and state-of-the-art policing tools to help law enforcement around the world, especially in enhancing preparedness to effectively counter cybercrime. The IGC should also operate a 24-hour Command and Co-ordination Centre (CCC).[51]

Council of Europe (CoE)

The Council of Europe is 'an international organisation mandated to uphold human rights, democracy, and rule of law.'[52] The Council of Europe does not make binding

47 UNODC website. Available at https://www.unodc.org/unodc/en/about-unodc/index.html?ref=menutop (Accessed 29 September 2017).

48 UNODC Repository on Cybercrime Lessons Learned. Available at https://www.unodc.org/cld/search-sherloc-les.jspx?f=en%23lessonsLearned.country_s%3aFinland&&tmpl=cyb (Accessed 29 September 2017).

49 Available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/unodc-comprehensive-study-cybercrime (Accessed 29 September 2017).

50 The Constitution of the ICPO-INTERPOL adopted by the General Assembly at its 25th session (Vienna, 1956).

51 Schjolberg, S. and Ghernaouti-Helie, S. *A Global Treaty on Cybersecurity and Cybercrime* (2011) at 58; See also Interpol at www.interpol.org (Accessed 29 September 2017).

52 Council of Europe. *Home*. Available at: http://www.coe.int/en/web/portal/home (Accessed 30 September 2017).

laws, but it promotes these values through international conventions, such as the Convention on Cybercrime. It monitors member states' progress in these areas and makes recommendations through independent expert monitoring bodies and has the power to enforce select international agreements reached by States on various topics.

The best-known body of the Council of Europe is the European Court of Human Rights, which enforces the European Convention on Human Rights. The CoE was established in 1949 and has 47 member states covering approximately 820 million people. The Council's two statutory bodies are the Committee of Ministers, comprising the foreign ministers of each member state, and the Parliamentary Assembly, comprising members of the national parliaments of each member state. The Commissioner for Human Rights is an independent institution within the Council of Europe and is mandated to promote awareness of and respect for human rights in the member states.

Organisation for Economic Co-operation and Development (OECD)

The OECD's mission is to promote policies that will improve the economic and social well being of people around the world. The OECD provides a forum in which governments can work together to share experiences and seek solutions to common problems and set international standards on a wide range of issues, such as digital security.

2.2 European Union Structures and Processes

European Union's (EU) institutional set-up may be argued to be somewhat complicated, but with some clarification the roles and responsibilities as well as the systematics of the various institutions become more understandable. Firstly, the EU institutions can be divided into EU Institutions, Bodies and Agencies. There are seven institutions, where the European Council sets the EU's overall political direction – but has no powers to pass laws.

The legislative bodies are the European Commission, the European Parliament and the Council of the European Union (also *the Council*). There are several relevant substructures operating, especially under the Council, that are mandated to support the political and regulatory processes. These are for instance CATS,[53] COSI[54] and LEWP.[55] The EU's Court of Justice upholds the rule of European law. Other institutions are not relevant in the scope of this article. Relevant bodies to understand the EU regulatory framework discussed later are for instance the European External Action Service (EEAS) and the European Data Protection Supervisor. Additionally, a host of specialized agencies handle a range of technical, scientific and management tasks of the Union, such as Europol, Eurojust, CEPOL and ENISA.

European Union Agency for Law Enforcement Cooperation (Europol)[56]

The legal frameworks of the Justice and Home Affairs' (JHA) agencies have been one of the focus areas of revision during recent years. One of them is Europol:

53 Committee provided for by Article 36.
54 Standing Committee on Operational Cooperation on Internal Security.
55 Law Enforcement Working Party.
56 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

> *The aim of the new Regulation on European Union Agency for Law Enforcement Cooperation (Europol) was to replace Council Decision 2009/371/JHA establishing Europol by a new Regulation based on Article 88 of the Treaty on the Functioning of the European Union introduced by the Lisbon Treaty and make Europol more efficient, more accountable and its data protection regime more robust, so that it can offer the best possible support to the Member States in their efforts of combating crime.*[57]

Europol Regulation entered into force in May 2016. The purpose of Europol is to support and strengthen action taken by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime that affects two or more Member States, terrorism and forms of crime that affect a common interest covered by the Union policy. The policy covering the crimes under Europol's mandate is subject to amendment by the Union. In essence, Europol is an information exchange and analysis hub, which provides various services (analytical, coordination, facilitation, development and capacity building) for the EU Member States' law enforcement community as well as Union structures. It does not have an executive mandate for coercive measures.

One major development is that Europol will be able to perform analysis across its information system, and therefore it can now potentially identify, for example, links between organized crime and terrorism. This was not possible before. The significance of this change is not only the potential benefit for more enhanced law enforcement in Europe but also the emergence of a paradigm shift towards more integrated crime prevention and security. This, in turn, may be a clear advantage in the field of cybercrime. The issue will come under examination later in this article. As is widely known, Europe has been bound to its history of separating state security threats from other forms of crime (including serious and organized crime) due to the unfortunate events during World War II when the International Criminal Police Commission (ICPC), nowadays known as Interpol, was overtaken by the Nazi regime. This resulted in the improper and illegal utilization of its sensitive data (political policing). It now seems that it took the terrorist incidents in Paris and other locations in 2015 to push the change in law enforcement policy.

In 2013 the European Cybercrime Centre (EC^3) was set up in Europol to bolster the response of law enforcement to cybercrime in the EU and to help protect European citizens, businesses and governments:

> *EC3 acts as the focal point in the fight against cybercrime in the Union, pooling European cybercrime expertise to support Member States' cybercrime investigations and providing a collective voice of European cybercrime investigators across law enforcement and the judiciary. Its operations focus on cybercrime forensics for operational support, crime prevention and capacity building as well as strategic analysis and advice.*[58]

The EC3 also hosts the Joint Cybercrime Action Taskforce (J-CAT), which brings also the law enforcement authorities of for example the United States, Canada and Australia on board: 'Its mission is to drive intelligence-led, coordinated action

57 Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. SN 1365/1/16 REV 1, Brussels 9 February 2016.

58 Europol: *Crime Areas & Trends, Cybercrime*. Available at: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime (Accessed 20 August 2017).

against key cybercrime threats through cross-border investigations and operations by its partners'.[59]

Each year the EC3 issues the Internet Organised Crime Threat Assessment (IOCTA[60]). The 2017 IOCTA reports how cybercrime continues to grow and evolve. The IOCTA provides a predominantly law enforcement focused assessment of the key developments, changes and emerging threats in the field of cybercrime over the last year. It relies on the contributions of the EU Member States and partners in private industry, the financial sector and academia. The report also describes some of the key challenges faced by law enforcement in terms of investigation and prosecution of cybercrime.[61] It also informs the setting of priorities and helps streamline resources within the EU and internationally to respond to cybercrime in an effective and concerted manner.[62]

In January 2016 Europol established the European Counter Terrorism Centre (ECTC), which is an operations centre and hub of expertise that reflects the growing need for the EU to strengthen its response to terror. The ECTC focuses on: 1) tackling foreign fighters; 2) sharing intelligence and expertise on the financing of terrorism (through the Terrorist Finance Tracking Programme and the Financial Intelligence Unit); 3) online terrorist propaganda and extremism (through the EU Internet Referral Unit); 4) illegal arms trafficking; and 5) international cooperation among counter terrorism authorities.

Europol and the European Union Intellectual Property Office (EUIPO) have also launched the Intellectual Property Crime Coordinated Coalition (IPC3), which focuses on fighting intellectual property crime and in particular online marketplaces that offer a wide range of counterfeit goods as well as phishing and online fraud.

The European Union's Judicial Cooperation Unit (Eurojust)

> *Eurojust stimulates and improves the coordination of investigations and prosecutions between the competent authorities in the Member States and improves the cooperation between the competent authorities of the Member States, in particular by facilitating the execution of international mutual legal assistance and the implementation of extradition requests. Eurojust supports in any way possible the competent authorities of the Member States to render their investigations and prosecutions more effective when dealing with cross-border crime. Eurojust's competence covers the same types of crime and offences for which Europol has competence, such as terrorism, drug trafficking, trafficking in human beings, counterfeiting, money laundering, computer crime, crime against property or public goods including fraud and corruption, criminal offences affecting the European Community's financial interests, environmental crime and participation in a criminal organization.*[63]

Its regulatory framework has been under revision several times since its establishment in 2002. The Council Decision 2002/187/JHA of 28 February 2002 that set up Eurojust with a view to reinforcing the fight against serious crime established it

59 Europol: *Crime Areas & Trends, Cybercrime*. Available at: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime (Accessed 20 August 2017).

60 Europol, *Internet Organised Crime Threat Assessment IOCTA* (2017). Available at: https://www.europol.europa.eu/iocta/2017/FOREWORD.html (Accessed 29 September 2017).

61 See the end of this section.

62 Europol, *Internet Organised Crime Threat Assessment IOCTA* (2017). Available at: https://www.europol.europa.eu/iocta/2017/FOREWORD.html (Accessed 29 September 2017).

63 Eurojust, *Background*. Available at: http://www.eurojust.europa.eu/about/background/Pages/mission-tasks.aspx (Accessed 30 September 2017).

as an EU body.[64] The legal framework was amended already in 2003[65] and 2008.[66] However, the *lisbonization*[67] process is still underway due to the Proposal for a Regulation on the establishment of the European Public Prosecutor's Office (EPPO),[68] which will become the next step of institutional evolution. The Proposal for EPPO is interconnected with the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust):[69]

> *In terms of cybercrime, Eurojust's annual reports confirm that there is an on-going need for EU and international coordination and support in the area of cross-border serious crime. The past decade has seen an explosion of organised crime, such as drug trafficking, trafficking in human beings, terrorism and cybercrime, including child pornography. A new criminal landscape is emerging, marked increasingly by highly mobile and flexible groups operating in multiple jurisdictions and criminal sectors, and aided, in particular, by widespread, illicit use of the Internet. Member States cannot effectively combat these at national level, so coordination and assistance become paramount. Eurojust is the only EU agency that supports national judicial authorities to appropriately investigate and prosecute these cases.*[70]

European Agency for Law Enforcement Training (*CEPOL)*

> *CEPOL is an agency of the European Union dedicated to develop, implement and coordinate training for law enforcement officials. CEPOL contributes to a safer Europe by facilitating cooperation and knowledge sharing among law enforcement officials of the EU Member States and to some extent, from third countries, on issues stemming from EU priorities in the field of security; in particular, from the EU Policy Cycle on serious and organised crime.*[71]

The new Regulation on CEPOL presents significant innovations when compared to the old Council Decision 2005/681/JHA. The magnitude of these changes is only observable when considering the wider policy context as defined in a series of key EU documents issued between 2013 and 2015, which de facto constitute a new European law enforcement training policy framework.[72] These documents are notably the European Law Enforcement Training Scheme (LETS), the European Agendas on Security and Migration respectively, the European Union Counter-Terrorism Strategy,

64 Eurojust, *Legal framework*. Available at http://eurojust.europa.eu/about/legal-framework/Pages/eurojust-legal-framework.aspx (Accessed 30 September 2017).

65 Council Decision 2003/659/JHA of 18 June 2003, amending Decision 2002/187/JHA.

66 Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA.

67 The latest chapter in the development of Eurojust is contained in the Lisbon Treaty, namely in Chapter 4, Articles 85 and 86. Article 85 mentions Eurojust and defines its mission as being 'to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States […]'. Article 86 states that 'in order to combat crimes affecting the financial interests of the Union, the Council, by means of regulations adopted in accordance with a special legislative procedure, may establish a European Public Prosecutor's Office from Eurojust'. Available at http://eurojust.europa.eu/about/background/Pages/History.aspx (Accessed 30 September 2017).

68 EU Doc. 13467/15 EPPO 41 EUROJUST 186 CATS 103 FIN 722 COPEN 288 GAF 46

69 The proposal has not been approved so far, thus the Council Decision 2002/187/JHA on Eurojust remains in force.

70 Proposal for a Regulation of the European Parliament and of the Council, 17 July 2013 on the European Union Agency for Criminal Justice Cooperation (Eurojust).

71 CEPOL, *About*. Available at: https://www.cepol.europa.eu/who-we-are/european-union-agency-law-enforcement-training/about-us. (Accessed 30 September 2017).

72 CEPOL, *New Legal Framework - Overall Impact Assessment* (34th Governing Board documents 6.1 b).

and the Cyber-security strategy.[73] In terms of cybercrime, the Agency implements training and competency development programmes in the fields of online card fraud, child sexual exploitation, cyber forensics and cyber security.[74]

The European Network and Information Security Agency (ENISA)

The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. It is involved in supporting exchanges of good practices between EU States. Currently, ENISA's approach to cyber security focuses on activities in three areas: recommendations; activities that support policy making and implementation; and 'Hands On' work, where ENISA collaborates directly with operational teams throughout the EU.

In accordance with the new Proposal on ENISA, the 'EU Cybersecurity Agency' in September 2017,[75] it is proposed that the current role of ENISA should be strengthened in the many areas where the Agency is already providing added value (see above), and new areas where support is needed would be added, in particular in implementing the so called NIS Directive,[76],[77] the review of the EU Cybersecurity Strategy, the upcoming EU Cybersecurity Blueprint for cyber crisis cooperation and ICT security certification. Two of the new key areas where the Agency would play an important role are 1) cyber security crisis management and cyber security certification and 2) standardization of ICT products and services:

> *The agency will also serve as a focal point for information and knowledge in the cybersecurity community. ENISA, in cooperation with the relevant bodies at Member State and EU level, notably the network of Computer security incident response teams, CERT-EU, Europol and the EU Intelligence and Situation Centre (INTCEN), will also contribute to EU-level situational awareness. In addition, for the Agency to perform the tasks and achieve the objectives set in the proposal it should have a permanent mandate which would allow for a more strategic and longer-term planning and thus enabling for a better preparedness to tackle the future challenges.*[78]

---

73 Communication from the Commission to the European parliament, The Council, the European Economic and Social Committee and the Committee of the Regions '*The European Agenda on Security*' (COM(2015) 185 final of 28 April 2015);
Communication from the Commission to the European parliament, The Council, the European Economic and Social Committee and the Committee of the Regions '*The European Agenda on Migration*' (COM92015) 240 final of 13 May 2015);
Joint Communication to the European parliament, The Council, the European Economic and Social Committee and the Committee of the Regions '*Cybersecurity Strategy of the European Union: An Open, safe and Secure Cyberspace*' (JOIN/2013/01 final 14469/4/05 REV4, Brussels, 30 November 2005).

74 CEPOL, *Single programming document: years 2017-2019 - Work Programme 2017*.

75 Proposal for a Regulation of the European Parliament and of the Council 13 September 2017, on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification, ['Referred to as the Cybersecurity Act'] (doc. COM(2017) 477).

76 Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 *concerning measures for a high common level of security of network and information systems across the Union* [Referred as the EU Cybersecurity Act].

77 See European Union Agency for Law Enforcement Cooperation (Europol) (2017) *Internet Organised Crime Threat Assessment* IOCTA (2017), at 31: The Network Information Security (NIS) directive that calls for cybersecure solutions in critical sectors will require identified operators in these sectors to take appropriate and proportion- ate measures to manage the risks posed to the security of their networks and information systems, including the need to notify significant incidents. As such, the NIS directive is expected to have a strong and positive impact on the cybersecurity of European critical infrastructure.

78 Joint Communication to the European Parliament and The Council, *Resilience, Deterrence and Defence: Building strong cyber security for the EU* (13 September 2017 JOIN(2017) 450 final).

In terms of cybercrime, ENISA's role could be seen as a kind of a European *cyber locksmith* to deter and fight against *cyber burglars*.

EU Policy Cycle[79]

The main driving force in the EU in terms of a coherent and coordinated response to cybercrime is the Policy Cycle. It is a multi-annual policy cycle with regard to serious international and organized crime in order to tackle the most important criminal threats in a coherent and methodological manner through optimum cooperation between the relevant services of the Member States, EU Institutions and EU Agencies as well as relevant third countries and organizations.

The policy cycle for serious international and organized crime consists of four steps: 1) policy development on the basis of a European Union Serious and Organised Crime Threat Assessment (EU SOCTA) that must provide for a complete and thorough picture of criminal threats impacting the European Union; 2) policy setting and decision-making through the identification by the Council of a limited number of priorities, both regional and pan-European. For each of the priorities a Multi-Annual Strategic Plan (MASP) needs to be developed in order to achieve a multidisciplinary, integrated and integral (covering preventive as well repressive measures) approach to effectively address the prioritised threats; 3) implementation and monitoring of annual Operational Action Plans (OAP) that will be aligned to the strategic goals, which have been determined in the MASP as the multilateral cooperation platform to address the prioritised threats, and 4) at the end of the policy cycle a thorough evaluation will be conducted and will serve as an input for the next policy cycle.

The Policy Cycle connects the operational knowledge (situational awareness of crime) of the law enforcement community and other stakeholders to the policy setting process. The purpose of it is to utilize the intelligence-led principle of policing at the European level. Thus, the process takes the political realities also into consideration as would be the case in terms of criminal policy of any independent State. The process has produced the following priorities, including cybercrime, for the period of 2014–2017:[80] facilitation of illegal immigration; trafficking in human beings; counterfeit goods (health & safety); synthetic drugs (and cocaine); Excise & Missing Trader Intra Community (MTIC) fraud; cybercrime (payment card fraud, child Sexual Exploitation and cyber-attacks; illegal firearms trade; and organized property crime by mobile organized criminal groups.

3 International Regulatory Framework

3.1 Soft Law and Policy

States are sovereign. On the international arena there is no legal hierarchy between States such as within a State where 'someone always has the last say'. However, States can for example via various treaties transfer or give away parts of their sovereignty, legal competency and power and thus bind themselves to certain obligations.

79 EU Council conclusions on the creation and implementation of a EU policy cycle for organized and serious international crime (25 October 2010, doc. 15358/10).

80 Draft Council conclusions 17 April 2013 on setting the EU's priorities for the fight against serious and organized crime between 2014/2017, doc. 8450/1/13 REV 1.

The EU is an example of a treaty-based organization with borrowed sovereignty from its Member States. Even so, the basis and foundation of the EU and its functions lay in international law. Hence, *mutual recognition*[81] is the way in which states communicate legally with each other.[82] In order to portray a broader understanding on the development of cybercrime regulation the domain of international law, including EU law, needs to be examined.

In this article the scope of international law is limited to statutory public international and EU law, including so-called *soft law*. The term *international law* is being used to describe *international public law* (treaties) and *supranational EU law* together due to systemic differences of these domains, especially due to the *sui generis* nature of EU law. The term chosen is only for the purpose of simplicity in discussing statutory law above a State's sovereignty and jurisdiction. Customary, private and case law is not discussed unless directly connected to any statutory provisions. The policy developments are discussed under the headline Policy and Soft Law, and some of the institutional aspects are discussed under the headline Institutional Framework.

For the purpose of this article the term *soft law* is understood as normative provisions contained in non-binding texts,[83] such as protocols, recommendations, resolutions and Memorandums of Understanding. Many law enforcement and criminal justice related international legal instruments exist only as soft law. They are usually based on strategy-policy ambitions and provide incentives to States to improve or consolidate such cooperation. Despite the non-binding legal nature of these instruments, they should nevertheless be considered as part of formal law enforcement and criminal justice cooperation. Below, some relevant instruments are introduced in summary. *Policy* is understood as a high-level overall plan encompassing the general goals and acceptable procedures for a definite course of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions.

The United Nations (UN)

The UN has been active, especially in the last two years, in addressing cybercrime and cyber security, but as far as the law is concerned there has not been development of an international statutory law on cybercrime or cyber security outside of the remits of the *jus ad bellum / jus in bello*, i.e. laws of war. The UN has, on the other hand, engaged in global political discussions on the possibility of a global treaty on cyber security and cybercrime. United Nations Congress on Crime Prevention and Criminal Justice in Salvador, Brazil, in April 2010, made a recommendation in the Salvador Declaration, and The Commission on Crime Prevention and Criminal Justice made a follow-up at its 19th Session in Vienna in May 2010 on the issue,[84]

81 Treaty on the Functioning of the European Union (2010), art. 82(1): 'Judicial cooperation in criminal matters in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions and shall include the approximation of the laws and regulations of the Member States – –.'

82 P. Sund, P. and B. Wennström, *European Internal Security – Challenges and Developments. Police's operating environment' review* (Police University College (Finland), 2016).

83 T. Fajardo, *Soft Law*. (Oxford Bibliografies, 2014). Available at: http://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0040.xml (Accessed 11 September 2017). See further in the same: Soft law covers a wide range of instruments of a different nature and functions that make it very difficult to contain it within a single formula. Its only common feature is that it is in written form, but the other characteristics are variable and negotiable and they constitute an *infinite variety*. So the term encompasses soft rules that are included in treaties, nonbinding or voluntary resolutions, recommendations, codes of conduct, and standards.

84 Schjolberg, S. and Ghernaouti-Helie *supra* note, at ii.

The Commission recommended to the United Nations Economic and Social Council the adoption of a Draft Resolution in response to the call for the development of an international instrument on Cybercrime, 'to undertake a comprehensive study of the problem of cybercrime and responses to it'. The Resolution was adopted by the General Assembly (December 2010 session). With Resolution 65/230, the General Assembly called for a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector,[85] which was conducted by UNODC.

Propelled by the momentum at the global level, and in conjunction with the work of the High-Level Experts' Group (HLEG) on cyber security under the International Telecommunications Union (UN specialized agency for information and communication technologies), Stein Schjolberg (chair of the HLEG) and Solange Ghernaouti-Helie even proposed a Draft Code on Peace, Justice And Security In Cyberspace – A Global Treaty on Cybersecurity and Cybercrime.[86] However, it seems that the pace of reaching a global treaty under the UN system has wound down. Instead, it seems that the Convention on cybercrime of the Council of Europe has proven to be quite successful, despite criticism on European orientation, in reaching global coverage.

Organization for Economic Co-operation and Development (OECD)

The OECD has produced a few international standards on digital security. Some recent cybercrime related instruments released by the OECD[87] include: C(2015)115 Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity; C(2011)155 Recommendation of the Council on the Protection of Children Online; C(2011)154 Recommendation of the Council on Principles for Internet Policy Making; C(2008)35 Recommendation of the Council on the Protection of Critical Information Infrastructures; C(2007)67 Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy; and C(2006)57 Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws against Spam.

Governmental Advisory Committee (GAC) for the Internet Corporation for Assigned Names and Numbers (ICANN)[88]

The GAC examines and advices a range of issues related to the functions and responsibilities of ICANN. It has dealt for instance as an international law enforcement community initiative to recommend amendments to the Registrar Accreditation Agreement (RAA) and due diligence recommendations for ICANN to adopt in accrediting registrars and registries as a way to combat online crime. The amendments

85 Exact wording: ' – – requests the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, an open-ended intergovernmental expert group, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.'

86 Schjolberg, S. and Ghernaouti-Helie, *supra* note.

87 OECD, *Acts*. Available at: http://webnet.oecd.org/oecdacts/ (Accessed 11 September 2017).

88 Law Enforcement Recommended RAA Amendments and ICANN Due Diligence. *Final Drafting Team Report on Improvements to the RAA* (18 October 2010). Available at https://publicintelligence.net/icann-lea-recommendations/ (Accessed 28 September 2017).

have been considered important in order to aid the prevention and disruption of efforts to exploit domain registration procedures by criminal groups for criminal purposes.[89] The GAC has also continued working on the EU General Data Protection Regulation (GDPR) and its impact to the Whois service.

Council of Europe (CoE)

Council of Europe Committee of Ministers have adopted the following Recommendations (soft law instruments) under the scope of criminal law (both substantive and procedural law) relevant to cybercrime: No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications; No. R (88) 2 on piracy in the field of copyright and neighbouring rights; No. R (87) 15 regulating the use of personal data in the police sector; No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes; No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services; No. R (95) 13 concerning problems of criminal procedural law connected with information technology; No. R (96) 8 on Europe in a time of change: crime policy and criminal law; and No. R (2001) 8 on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services).

The Global Alliance Against Child Sexual Abuse Online

The Global Alliance Against Child Sexual Abuse Online was launched on 5 December 2012 by the European Commission and the United States, and it aimed to raise standards worldwide and unite efforts around the world to more effectively combat online sexual crimes against children. It gathered 54 countries, which committed to pursue concrete actions to enhance victim protection, identify and prosecute offenders, raise awareness and reduce the availability of child pornography online and the re-victimization of children. Annexes to the Declaration set out concrete operational goals and examples of potential actions that participants could undertake to reach these goals.[90]

G8 Group of States

> *The Group of Eight States (G8) established in 1997 the Subgroup of High-Tech Crime (the Lyon Group). At the meeting in Washington in 1997 Ten Principles was adopted in the combat against computer crime, including a 24/7 network for the assistance in global cybercrime investigations. This network consists of more than 40 countries around the world, and work also in cooperation with Interpol's 24/7 network. The goal was to ensure that no criminal receives safe havens anywhere in the world.*[91]

89 ICANN, *Law Enforcement Recommendations for Domain Registration and WHOIS Data Collection Revisions*. Available at https://publicintelligence.net/icann-lea-recommendations/ (Accessed 28 September 2017).

90 European Commission, *Migration and Home Affairs*. Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse_en (Accessed 26 September 2017).

91 Schjolberg, S. and Ghernaouti-Helie, *supra* note at 58.

Since then, several statements have been adopted at the G8 Meetings under combating against cybercrime and terrorist use of the Internet. In the 2000 Okinawa Meeting one of the G8 adopted goals was: 'We must take a concerted approach to high-tech crime, such as cyber-crime, which could seriously threaten security and confidence in the global information society. Our approach is set out in the Okinawa Charter on Global Information Society.'[92] In the 2004 Meeting one of the G8 adopted goals was: 'to ensure that law enforcement agencies can quickly respond to serious cyber-threats and incidents [cursive removed].'[93] In 2006 for the G8 Justice and Home Affairs Ministers a further statement was made: 'We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work.'[94] It was also stated that: 'Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists.'[95] The group went on and at the 2008 Hokkaido-Toyako Meeting even more detailed statement was made: 'We will strengthen our cooperation, including experience-sharing, to fight against transnational organized crime, including trafficking in persons, smuggling of migrants, illicit manufacturing of and trafficking in firearms, illicit traffic in narcotic drugs and psychotropic substances, cybercrime and money laundering.'[96]

The 2009 Meeting statement exemplifies the growing interest and precision of the political statements of the group: 'Criminal misuse of social networks, encryption services, VoIP services, the Domain Name System, and other new and evolving criminal attacks on information systems, pose increased challenges to law enforcement and are spreading.'[97] At the 2010 Muskoka Meeting the following statement brought cybercrime and terrorism more connected*:* 'We are also concerned about cybercrime as a growing threat. We will deepen our work together to weaken terrorist and criminal networks and have adopted a robust plan of action for this purpose.'[98] At the 2011 Meeting a full section on the Internet was released.[99] In 2012 the statements were related to countering violent extremism, including improving anti-money laundering and terrorist financing frameworks worldwide. This was the case also in 2015, 2016 and 2017. However, in 2016 the group released also G7 Principles and Actions on Cyber.[100]

EU Global Strategy

The EU Global Strategy[101] sets out the EU's core interests and principles for engaging in the wider world and gives the Union a collective sense of direction. Its

92 G8 Communiqué, *Toward a 21st Century of Deeper Peace of Mind: Crime and Drugs* (21–23 July 2000). Available at: http://www.g8.utoronto.ca (Accessed 26 September 2017).
93 Schjolberg, S. and Ghernaouti-Helie, S. *supra* note at 58.
94 *Ibid*.
95 G8 Summit Declaration on *Counter-Terrorism* (St. Petersburg, 16 July 2006). Available at: http://www.g8.utoronto.ca/summit/2006stpetersburg/counterterrorism.html (Accessed 1 October 2017).
96 G8 Communiqué, *Transnational Organized Crime* (7-9 July 2008). Available at: http://www.g8.utoronto.ca (Accessed 26 September 2017).
97 Schjolberg, S. and Ghernaouti-Helie, S *supra* note at 58.
98 G8 Communiqué, *International Peace and Security* (25-26 June 2010). Available at: http://www.g8.utoronto.ca (Accessed 26 September 2017).
99 Deauville Declaration, *Internet* (Deauville, 26 May 2011). Available at: http://www.g8.utoronto.ca/summit/2011deauville/2011-internet-en.html.
100 University of Toronto. *G7/8*. See more on http://www.g8.utoronto.ca/summit/2016shima/cyber.html (Accessed 26 September 2017).
101 European Commission, *Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy* (June 2016).

ambition is to keep citizens safe, preserve its interests and uphold values. The Strategy helps making the EU more effective in confronting energy security, migration, climate change, violent extremism and hybrid warfare.

The means to achieve the goals in terms of cyber security are to equip the EU and assist Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace by: strengthening the technological capabilities aimed at mitigating threats and the resilience of critical infrastructure, networks and services, and reducing cybercrime; fostering innovative information and communication technology (ICT) systems which guarantee the availability and integrity of data, while ensuring security within the European digital space through appropriate policies on the location of data storage and the certification of digital products and services; weaving cyber issues across all policy areas, reinforcing the cyber elements in Common Security and Defence Policy missions and operations; further developing platforms for cooperation; strengthening the voluntary framework for cyber crisis management; engaging in cyber diplomacy and capacity building with our partners and seeking agreements on responsible state behaviour in cyberspace based on existing international law; and supporting multilateral digital governance and a global cooperation framework on cyber security.

European Agenda on Security

The European Agenda on Security[102] sets out how the Union can bring added value to support the Member States in ensuring security. The European Agenda on Security aims to strengthen the tools that the EU provides to national law enforcement authorities to fight terrorism and cross-border crime. In particular, the Agenda focuses on improving information exchanges and operational cooperation between law enforcement authorities. It also mobilises a number of EU instruments to support actions through training, funding and research and innovation. The Agenda prioritizes terrorism, organized crime and cybercrime as interlinked areas with a strong cross-border dimension, where the EU action can make a real difference. All actors work together based on five key principles: 1) to ensure full compliance with fundamental rights; 2) to guarantee more transparency, accountability and democratic control; 3) to ensure better application and implementation of existing EU legal instruments; 4) to provide a more joined-up inter-agency and a cross-sectorial approach; and 5) to bring together all internal and external dimensions of security.

In summary, fighting cybercrime is a recognized priority under the Agenda, and the existing obstacles to cybercrime investigations are being addressed in the process of its implementation. Some practical initiatives are for instance common rules for data protection (EU Directive for police and criminal justice authorities), re-evaluation and amendment of the EU Data Retention Directive, further development of European databases (e.g. EU Passenger Name Record System, European Criminal Records Information System, European Police Record Index System), establishment of Internet Referral Unit, European Cybercrime Centre (EC^3) and a decentralized computer network supporting Financial Intelligence Units at Europol.

102 Communication from the Commission to the European parliament, The Council, the European Economic and Social Committee and the Committee of the Regions '*The European Agenda on Security*' (COM(2015) 185 final of 28 April 2015).

The EU Justice Agenda for 2020 - Strengthening Trust, Mobility and Growth within the Union

The EU Justice Agenda[103] sets out the political priorities that should be pursued in order to make further progress towards a fully functioning common European area of justice oriented towards trust, mobility and growth by 2020. In terms of cybercrime, the Agenda prioritizes the consolidation of operational cooperation between various practitioners by making sure that instruments agreed at the EU level are transposed, effectively implemented and used by Member States. It also suggests examining the improvement in the codification of EU criminal law in terms of criminal procedural rights.

Cybersecurity Strategy of the European Union

The EU Cybersecurity Strategy[104] clarifies the principles that should guide cyber security policy in the EU and internationally. These are: the EU's core values apply as much in the digital as in the physical world; protecting fundamental rights, freedom of expression, personal data and privacy; access to the Internet for all; democratic and efficient multi-stakeholder governance; and a shared responsibility to ensure security.

In addressing the challenges highlighted above, it introduces five strategic priorities: 1) achieving cyber resilience; 2) drastically reducing cybercrime; 3) developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP); 4) developing the industrial and technological resources for cyber security; and 5) establishing a coherent international cyberspace policy for the European Union and promoting core EU values (cyber diplomacy).

Furthermore, the strategy introduces a coordination mechanism between Network and Information Security (NIS) competent authorities, law enforcement and defence:

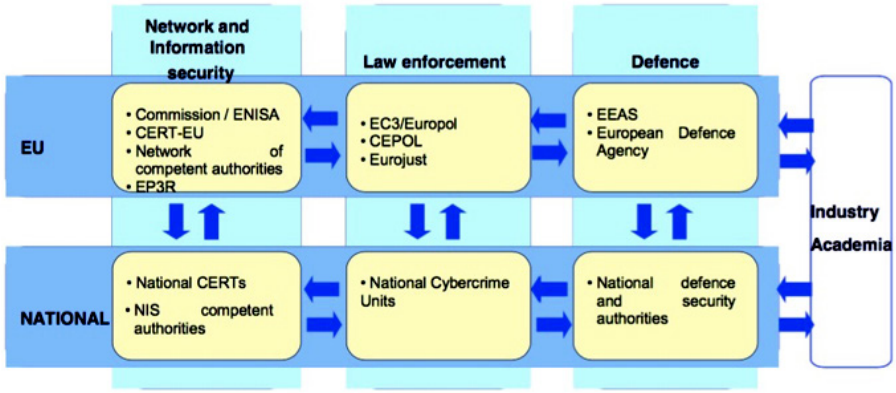

Figure 1. EU cyber security coordination mechanism.

103 Communication From the Commission to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions, *The EU Justice Agenda for 2020 - Strengthening Trust, Mobility and Growth within the Union* (11 September 2014, doc. COM(2014) 144 final).

104 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN(2013) 1 Final).

Resilience, Deterrence and Defence: Building strong cybersecurity for the EU [105]

> *EU cyber preparedness is central to both the EU Digital Single Market and the Security and Defence Union. Enhancing European cyber security and addressing threats to both civilian and military targets is deemed necessary. The communication is a proposal of a wide range of concrete measures that will further strengthen the EU's cyber security structures and capabilities with more cooperation between the Member States and the different EU structures concerned.*[106]

These measures would ensure that the EU is better prepared to face the ever-increasing cyber security challenges (in particular computer network attacks), namely in three key areas: 1) building EU resilience to cyber-attacks and stepping up the EU's cyber security capacity; 2) creating an effective criminal law response; and 3) strengthening global stability through international cooperation.

The challenges of cyber-attacks would be achieved by: establishing a stronger European Union Cybersecurity Agency built on the Agency for Network and Information Security (ENISA), to assist Member States in dealing with cyber-attacks; creating an EU-wide cyber security certification scheme that will increase the cyber security of products and services in the digital world; making a blueprint for how to respond quickly, operationally and in unison when a large scale cyber-attack strikes; forming a network of competence centres in the Member States and a European Cybersecurity Research and Competence Centre that will help develop and roll out the tools and technology needed to keep up with an ever-changing threat and make sure our defence is as strong as possible; writing a new Directive on the combating of fraud and counterfeiting of non-cash means of payment to provide for a more efficient criminal law response to cyber crime; building a framework for a Joint EU Diplomatic Response to Malicious Cyber Activities and measures to strengthen international cooperation on cyber security, including deepening of the cooperation between the EU and NATO; and driving high-end skills development for civilian and military professionals through providing solutions for national efforts and the set-up of a cyber defence training and education platform.[107]

Joint statement of Ministers of Justice and Home Affairs and representatives of the EU institutions[108]

After the shock of the attacks in Brussels on 22 March 2016, the EU declared as a matter of priority finding ways to secure and obtain electronic evidence (*e-evidence*) more quickly and effectively. This was to be done by intensifying cooperation with third countries and with service providers that are active on European territory in order to enhance compliance with EU and Member States' legislation as well as to foster contacts with law enforcement authorities and to identify concrete measures to address this complex matter:

> *An important element in implementing the Strategy will be the swift adoption of the proposal for a Directive on network and information security. The implementation of this Directive would not only promote better cooperation between law enforcement and cyber security authorities, but*

105 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Resilience, Deterrence and Defence: Building Strong Cyber Security for the EU* (13 September 2017 JOIN(2017) 450 final).

106 *Ibid*.

107 *Ibid*.

108 On 24 March 2016 doc. 7371/16.

also provide for cyber-security capacity building of competent Member States' authorities and cross-border incident notification.[109]

Council conclusions on improving criminal justice in cyberspace[110]

The conclusions on improving criminal justice in cyberspace set out concrete measures for future follow-up and action in three main areas of work: 1) in the streamlining of mutual legal assistance (MLA) proceedings and, where applicable, mutual recognition related to cyberspace, through the use of standardized electronic forms and tools; 2) in the improving of cooperation with service providers through the development of a common framework (e.g. use of aligned forms and tools) with them to request specific categories of data; and 3) in launching a reflective process on possible connecting factors for enforcement jurisdiction in cyberspace.

Council Conclusions on the European Judicial Cybercrime Network[111]

The European Judicial Cybercrime Network shall provide a centre of specialized expertise supporting judicial authorities, i.e. prosecutors and judges dealing with cybercrime, cyber-enabled crime and investigations in cyberspace. To this end, the Network shall facilitate and enhance cooperation between the competent judicial authorities dealing with cybercrime, cyber-enabled crime and investigations in cyberspace, respecting the structure and the competence within Eurojust and the European Justice Network (EJN).

As a summary of various other EU security policies, it may be noted that 8 out of 16 (50%) explicitly address cyber security and cybercrime. It is also possible to observe that the trend of inclusion of cyber issues in EU policies began around 2005 with the release of the EU Counter-Terrorism Strategy in response to the explosion of terrorist attacks in Europe and elsewhere. In 2004 alone, the following terrorist attacks took place: the major Moscow Metro terrorist bombings, the Beslan school hostage crisis, the Paris Indonesian Embassy bombing, the murder of Theo van Gogh in the Netherlands, the Madrid train bombing and several other minor bombings in Spain. In addition, the London terrorist bombings occurred in 2005.

109 Joint statement of Ministers of Justice and Home Affairs and representatives of the EU institutions (On 24 March 2016 doc. 7371/16) .

110 EU Council Conclusions, *Improving Criminal Justice in Cyberspace* (doc. 10007/16, ST 10007 2016 INIT 9 June 2016).

111 EU Council Conclusions, *The European Judicial Cybercrime Network*, doc. 10025/16, ST 10025 2016 INIT 6 June 2016).

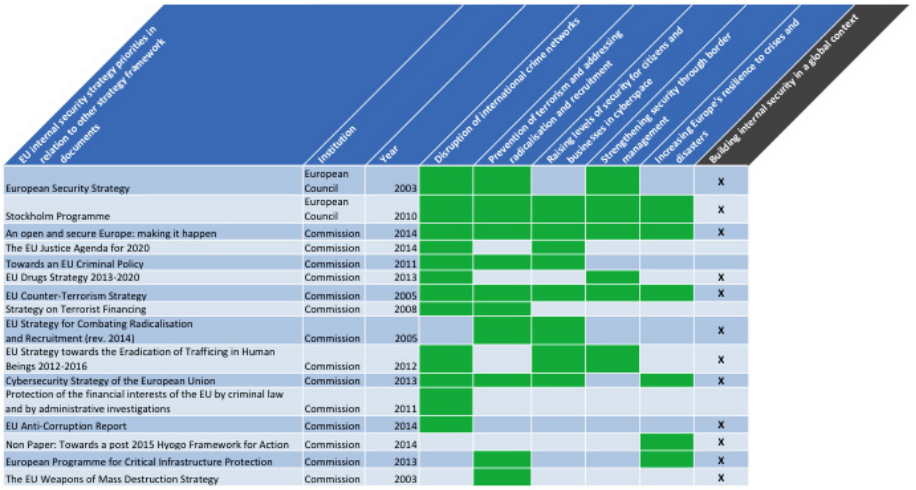

Figure 2. EU internal security strategy priorities in relation to framework documents[112]

In conclusion, some notions may be highlighted in relation to the various policy formulations falling into the scope of cybercrime: 1) cooperation between law enforcement and judicial authorities needs to be intensified and rationalized, both intra-EU and extra-EU. This includes also procedures concerning international mutual legal assistance; 2) the same approach should be implemented with (private) service providers; 3) and the underlying and more fundamental question about how jurisdiction in cyberspace should be established needs to be addressed in keeping with the principle of territoriality. Applying a business link connecting factor for jurisdiction may ensure a broader impact of Article 18 of the Budapest Convention, which sets out rules enabling the competent authorities to obtain data from a person or a service provider found to be present on its territory by the services it provides on the basis of a domestic production order. Also, in the absence of any possibilities for cooperation, such as in the loss (of knowledge) of location, the issue should be addressed similarly as in fact many countries already conduct extraterritorial searches:[113] 1) international cooperation in criminal investigations and judicial proceedings has so far been undertaken within different frameworks, corresponding to different courses of action, such as: (i) *MLA*, usually based on a mutual legal assistance treaty (MLAT); (ii) mutual *supranational data sharing*, often in an institutionalised setting, including multilateral databases (Shengen Information System), matching of national databases (Prüm) and bodies to facilitate information exchange between countries, such as Interpol, Europol and Eurojust; (iii) *extraterritorial investigation*, in which officials from state A perform or assist in investigative activities in state B, such as (short term) cross border hot pursuit or police and judicial liaison officers; and (iv) *joint supranational investigations*, such as EU Joint Investigation Teams;[114] 2) the borderless nature of cyberspace poses special challenges for law enforcement

112 Ministry of the Interior [Finland], *EU:n sisäisen turvallisuus strategia - kansalliset jatkotoimet* (Internal Security Publication Series, 22/2014).

113 More in-depth discussion can be found from the *Report of the EU Conference on jurisdiction in cyberspace* (held in Amsterdam on the 7 and 8 March 2016, doc. 7323/16).

114 *Report of the EU Conference on jurisdiction in cyberspace* (held in Amsterdam on the 7 and 8 March 2016, doc. 7323/16).

and judicial authorities, which often leads to impunity and thus calls for urgent improvement of law enforcement and judicial action in cyberspace; and 3) any use of investigative measures should be guided by the protection of fundamental rights and freedoms and the principles of necessity and proportionality.

In summary, the conclusions are rather clearly leading to consolidate the call made by Europol on some key challenges faced by law enforcement in terms of the investigation and prosecution of cybercrime: the need to address the issues of e-evidence challenges and the need for adequate and harmonized legislation to address the specificities of cybercrime. For instance, a combination of legislative and technical factors, which deny law enforcement access to timely and accurate electronic communications data and digital forensic opportunities, such as a lack of data retention, the implementation of Carrier-Grade Network Address Translation (CGN) and criminal abuse of encryption, are leading to a loss of both investigative leads and the ability to effectively attribute and prosecute online criminal activity.[115]

3.2 International Public Law (Treaties)

The most prominent example in respect to statutory international law is the Convention on cybercrime of the Council of Europe, which regulates the harmonization of domestic laws and lays down rules for State cooperation.[116] As a side note to the scope of the convention, it is noteworthy that this treaty does not contain rules on cyber activities attributable to States. In the words of the Explanatory Report, the Convention 'leaves unaffected conduct undertaken pursuant to lawful government authority'.[117] Therefore, it does not address the full extent of cybercrime, such as covert state-originated cyber attacks, that certainly are an object of the discussion in this article (see headline *Regulatory Framework, Applicable Offences Related to Warfare* above). In terms of the substantive criminal law, the Convention stipulates the areas of cybercrime to be established as criminal offences, which are: offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; offences related to infringements of copyright and related rights; and ancillary liability and sanctions (i.e. attempt and aiding or abetting as well as Corporate Liability).

The Convention also contains provision in the field of procedural law and international cooperation (including extradition and criminal intelligence). The value of the Convention is its geographical coverage. Since the inception of the Convention in 2001, 66 States have ratified/acceded it or are in the process of doing so. Additionally, more than 65 States are aligning its national laws or drawing from it in doing so. Essentially it means that more than 130 States are more or less in line with the Convention in terms of their criminal law and the number is still growing. Furthermore, for the future development of the issue of cybercrime, the Convention suggests that there is a need for globalization of (cyber)justice since effective fighting against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters. The notion basically refers to a need for broader competency rules for law enforcement and prosecution authorities. In consequence mutual legal assistance (MLA) requests should be more effectively (more quickly

115 Europol, *Internet Organised Crime Threat Assessment IOCTA* (2017).

116 Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004, CETS 185). The treaty is also known as the *Budapest Convention*.

117 *Explanatory Report to the Convention on Cybercrim*e. Available at: http://conventions.coe.int/treaty/en/reports/html/185.htm> (Accessed 27 September 2017).

and with very limited scope of refusal) executed, and the principle of territoriality may require a review in the future.

To date, cybercrime has primarily been addressed through national legislation and various regional frameworks (binding and non-binding), such as Arab League Model Cyber Law, Commonwealth Model Law on Computer and Computer-related Crime and the ECOWAS Directive.

3.3 European (Union) Criminal Law

Civil law has gone through a process of legal approximation, harmonization and integration in in European Union (EU). Step by step, laws that have an impact on especially the common market have been a subject of change through the EU, by for example various EU Regulations, Directives and court decisions (Case Law):

> *Although there is no overarching criminal policy for the EU, would the next strategic step be to integrate criminal law in the EU? A common European criminal law would definitely be a big step forward for law enforcement cooperation in Europe. There are steps towards the construction of such a system, for example the European Arrest Warrant,[118] Joint Investigation Teams[119] and other instruments that simplify cooperation between member states. However, there are significant issues with unifying criminal laws in the EU.*[120]

Firstly, there is a major difference in traditions that exists between continental law and common law systems, especially when it comes to criminal law. It is for example hard to see Germany giving up the tradition of stipulating the general part of its criminal code in some other unfamiliar construction as a major legal transplant that would reform the whole system of criminal law.[121] Secondly, is the basic question of what a crime is. Today, there are basically as many definitions as there are member states, and thus it would require significant harmonization efforts. Thirdly, addressing the question of relationship between law and morality. Criminalization is not just a technical question. When it comes to sexuality, abortion, family and other questions it is obvious that harmonization of European criminal codes is not a simple matter. One can find many more challenging questions when it comes to forming a common European criminal law. According to some, a way forward could be to focus on common minimum standards, but even from this point, the road to a common European criminal code seems still to be a long and bumpy ride. Further, as long as there is no single and common European criminal law system the principle of mutual recognition will be the basis for also law enforcement cooperation in the EU.[122]

Although, it must be noted that some significant efforts have been conducted in order to approximate substantive criminal law between EU member states. The

---

118 Council Framework Decision 2002/584/JHA on the European Arrest Warrant and the surrender procedures between Member States.

119 Framework Decision on Joint Investigation Teams (2002/465 of 13 June 2002, OJ 2002, L 162/1).

120 Sund, P. and Wennström B. European Internal Security – Challenges and Developments (2016) Police's operating environment' review Police University College (Finland).

121 See, e.g. Treaty on the Functioning of the European Union (2010), art 82(3): 'Where a member of the Council considers that a draft directive as referred to in paragraph 2 would affect fundamental aspects of its criminal justice system, it may request that the draft directive be referred to the European Council. In that case, the ordinary legislative procedure shall be suspended. After discussion, and in case of a consensus, the European Council shall, within four months of this suspension, refer the draft back to the Council, which shall terminate the suspension of the ordinary legislative procedure.'

122 P. Sund and B. Wennström, *European Internal Security – Challenges and Developments* (Police's operating environment review, Police University College (Finland), 2016).

Treaties of the EU[123] provide for three objectives in terms of providing European definitions and sanctions of crimes: 1) more efficient fight against serious cross-border crime, Art. 67(3) and 83(1) TFEU; 2) support for the implementation of other EU policies (economic and financial crimes), Art. 83(2) TFEU; and 3) facilitation of the application of mutual recognition instruments: Art. 82(2) TFEU.

Article 83(1) of the TFEU stipulates:

> *'The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.*
>
> *These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.*
>
> *On the basis of developments in crime, the Council may adopt a decision identifying other areas of crime that meet the criteria specified in this paragraph. It shall act unanimously after obtaining the consent of the European Parliament.'*

These areas of crime are commonly referred to as *Eurocrimes* and could be said to set the pathway towards a common European criminal law,[124] although other views may be expressed as well. Nevertheless, the fact is that article 83(1) provides legal competency for the EU to regulate the definitions of constitutive elements of crimes as well as definitions of sanctions for crime *areas* stipulated in the article. It is important to note that the article deals with crime areas, not just particular offences, such as money laundering and is hence to be understood as covering potentially several different offences related to the crime area in question. Furthermore, as one easily notices, Eurocrimes fall to large extent under the scope of cybercrime.

Another aspect in relation to cyberspace more generally is the EU priority on development of the *Digital single market* connecting to the following EU policy areas: better access for consumers and business to online goods, helping to make the EU's digital world a seamless and level marketplace to buy and sell; the right environment for digital networks and services, designing rules that match the pace of technology and support infrastructure development; and economy and society, ensuring that Europe's economy, industry and employment take full advantage of what digitalisation offers.[125]

The notion of other EU policy areas is relevant due to article 83(2) TFEU,[126] which affirms the need of approximation in substantive criminal law in crime areas

123 Treaty on the European Union, TEU (2010); Treaty on the Functioning of the European Union, TFEU (2010).

124 See art. 67(3) TFEU: Objectives of judicial and police cooperation.
'The Union shall endeavour to ensure a high level of security through measures to prevent and combat crime, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters, and, if necessary, through the approximation of criminal laws.'

125 European Commission, *Priorities*. Available at https://ec.europa.eu/commission/priorities/digital-single-market_en (Accessed 11 September 2017).

126 'If the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures, directives may establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned. Such directives shall be adopted by the same ordinary or special legislative procedure as was followed for the adoption of the harmonisation measures in question, without prejudice to Article 76.'

other than the listing above in 83(1) TFEU. In terms of cybercrime, the stipulation could mean even rather expansive actions in the future.

One particular issue to be highlighted is the framing of the EU's competence in criminal matters; this is to say that it falls under *shared competence*, meaning that in accordance with art. 2(2) of the TFEU Member States continue to 'exercise their competence to the extent that the Union has not exercised its competence'. This means in practice that EU Member States may not initiate any national regulatory efforts after the related common action.

3.4 European Union Cybercrime Regulatory Framework

The following presentation of substantive EU criminal legislation targeting cybercrime is limited to and contrary to, the definition of for instance Europol, legal instruments within the scope of those cyber offences committed *only* within cyber space. This restriction is made due to the limited possibility of dealing with all crime threats having a dimension in cyberspace, as discussed earlier in this article. Furthermore, also any legislation on data protection, cyber security (resilience) or the procedural framework of criminal law is excluded, unless focussing exclusively on cyberspace. It is also important to note that there have been several legal instruments provided for since the early 2000s, which have since been amended and repealed with a newer legislation. The following section summarizes the approximation of legislation in the field of criminal law so far.

Proposal for a Directive on Combating Fraud and Counterfeiting of Non-cash Means of Payment[127]

On 13 September 2017, the Commission proposed a new Directive aiming to ensure that a clear, robust and technology neutral policy/legal framework is in place that would eliminate operational obstacles that hamper investigation and prosecution and enhance prevention of these types of crime. The proposal corresponds to provisions of the Council of Europe Budapest Convention on Cybercrime. As the Directive is only a proposal at the moment, the current EU legislation that provides common minimum rules to criminalize non-cash payment fraud is Council Framework Decision 2001/413/JHA[128] on combating fraud and the counterfeiting of non-cash means of payment.

Directive 2017/541/EU on combating terrorism[129]

The Directive is the cornerstone of the Member States' criminal justice response to counter terrorism. In terms of cybercrime it covers provisions for conduct related to, in particular, foreign terrorist fighters and terrorist financing, including forms of conduct committed through the Internet such as using social media as well as measures against public provocation content online (including radicalisation online). It also aims to reduce the overall amount of funds obtained from non-cash payment fraud,

127 Proposal for a Directive of The European Parliament and of The Council of 13 September 2017, on Combating Fraud and Counterfeiting of Non-cash Means of Payment and Replacing Council Framework Decision 2001/413/JHA.

128 Official Journal of the European Union L 149, 2 June 2001.

129 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA.

most of which go to organized crime groups to commit serious crimes, including terrorism.

Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the fourth Anti-Money Laundering Directive)[130]

The Directive covers the situation where criminals abuse non-cash payment instruments with a view to concealing their activities. This proposal complements it by addressing the situation where the non-cash payment instruments have been, for instance, unlawfully appropriated, counterfeited or falsified by the criminals.

Proposal for a Directive amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[131]

Directive (EU) 2015/849 of the European Parliament and the Council constitutes the main legal instrument in the prevention of the use of the Union's financial system for the purposes of money laundering and terrorist financing:

> *The amended Directive, which is to be transposed by 26 June 2017, sets out a comprehensive framework to address the collection of money or property for terrorist purposes by requiring Member States to identify, understand and mitigate risks related to money laundering and terrorist financing. The proposal of the Directive introduces the definition and inclusion of virtual currencies to the framework. Providers of exchange services between virtual currencies and fiat currencies (that is to say currencies declared to be legal tender) as well as custodian wallet providers for virtual currencies are under no obligation to identify suspicious activity. Terrorist groups are thus able to transfer money into the Union's financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity on those platforms. It is therefore essential to extend the scope of Directive (EU) 2015/849 so as to include virtual currency exchange platforms and custodian wallet providers. Counter-terrorism investigations in Europe have shown that the use of the Internet is an integral component in any terrorist plot.*[132]

Directive 2013/40/EU on Attacks Against Information Systems[133]

The Directive aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cybercrime laws and introduce tougher criminal sanctions. It establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities. The proposal corresponds to provisions of the Council of Europe Budapest Convention on Cybercrime.

---

130 Directive 2015/849/EU of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

131 Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, at 21.

132 Europol, *Internet Organised Crime Threat Assessment IOCTA* (2017) at 52.

133 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.

Directive 2011/92/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography[134]

The Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children, child pornography and solicitation of children for sexual purposes. It also introduces provisions to strengthen the prevention of those crimes and the protection of the victims thereof:

> *The Directive obliges EU Member States to provide for criminal penalties in their national legislation in respect of the provisions of Union law on combating sexual abuse, sexual exploitation of children and child pornography. In terms of cybercrime, the directive targets both: child pornography, constituted by making, distributing or downloading child sexual abuse images, and solicitation of children for sexual purposes with specific characteristics in the context of the Internet. Member States must also ensure that child pornography web pages hosted within their territory are promptly removed and must strive to remove those hosted abroad. It also allows the removal of or, where appropriate, block websites containing child pornography could be based on various types of public action, such as legislative, non-legislative, judicial or other.*[135]

3.5 European Procedural Criminal Law

Even though this article is not focussing on the aspects of procedural criminal law, for the sake of awareness and clarity, a short summary list on pan-European cooperation mechanisms in criminal matters that facilitate coordination of investigation and prosecution of cybercrime (not exclusive to cybercrime) are listed:[136] Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust);[137] Regulation (EU) 2016/794 on Europol;[138] Directive 2014/41/EU regarding the European Investigation Order in criminal matters; Council Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings; Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders; Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union; Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence; Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams; Council Decision 2002/187/JHA setting up Eurojust;[139] and Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union.

While for instance one of the most recent legal instruments, the European Investigation Order (EIO) is expected to simplify cooperation between judicial

134 Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011, on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA.

135 *Ibid*.

136 See also European Justice Network, *Home*. Available at: https://www.ejn-crimjust.europa.eu/ejn/EJN_Home.aspx

137 The proposal has not been approved so far, thus the Council Decision 2002/187/JHA on Eurojust remains in force.

138 Europol Regulation is discussed in more detail under the headline Institutional Framework.

139 Eurojust is discussed in more detail under the section Institutional Framework.

authorities and expediting investigations, existing legal frameworks and operational processes would still need to be further harmonized and streamlined for dealing with cross-border e-evidence. Such measures, as well as any development efforts on data encryption, data retention and Internet governance should thoroughly consider the specific law enforcement needs and strive for practical and proportionate solutions.[140]

4 The Scope of National Criminal Law in Cyber Security

This section examines the case of Finland as an example of State actions in relation to cybercrime and more widely cyber security. This example should not be read as a showcase or best practice and instead as a mere sample of any developed State having a strong interconnection with the instruments of international law. Although States may not exercise sovereignty over cyberspace *per se*, States may exercise their jurisdiction with regard to cybercrimes and other cyber activities pursuant to the bases of *sovereignty*[141] and subsequent jurisdiction recognized in international law.[142],[143] In accordance with the Finnish Penal Code,[144] Chapter 1, Sections 3, 5 and 7 as well as Section 10 jointly provide for jurisdiction of cybercrime in the forms of: *subjective territorial* (incident initiated within its territory but completed elsewhere); *objective territorial* (where a particular incident has effects even though the act was initiated outside its territory); *active personality* (nationality of the perpetrator); *passive personality* (nationality of the victim); *protective principle* (national security threat to the State); and *universal jurisdiction* (violation of a universal norm of international law, such as war crimes).

These elements of jurisdiction are by no means new. However, some of them are repeatedly mentioned in various declarations, reports, studies recommendations and other soft law instruments as well as hard law instruments, such as the European Convention on Cybercrime. The issue of jurisdiction is of concern in the global context, as cybercrime postulates efficient law enforcement and judicial cooperation, hence any caveats in jurisdiction hinder, if not impede, such efforts. More such caveats may even create safe havens for cyber criminals. Thus, the purpose of multi-dimensional regulation on criminal jurisdiction is to secure the State's legal right to intervene, in essence, with any offences linked to the State either on a territorial or personality basis.

As discussed earlier, basically all cyber threats (e.g. hacking/hactivism, computer network attacks, cyber espionage, cyber terrorism, cyber warfare) and related behaviours fall into the scope of criminal law in addition to other cybercrime offences such as (online) fraud, sexual crimes (e.g. child pornography) etc. that are not discussed in detail here. There are several provisions in the Penal Code covering the aforementioned criminal behaviours; some being stipulated (usually by way of amendment) to cover old, non-digital and the digital environment such as a Message interception offence and some by the way of introducing a completely new offence

140 Europol, *Internet Organised Crime Threat Assessment IOCTA* (2017).
141 Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).
142 M. Schmitt, *Tallinn Manual On The International Law Applicable To Cyber Warfare* (Cambridge University Press, 2013) at 26.
143 See, e.g. Council of Europe, Convention on Cybercrime, Section 3 art. 22. (Nov. 23, 2001, Eur. T.S. No. 185).
144 The Criminal Code of Finland, 39/1889 (amendments up to 766/2015 included).

such as an Interference in an information system offence. The Finnish Penal Code is constructed by first depicting the so-called basic form (typology) of a particular offence, followed by an aggravated form and then a petty form of the same when applicable. Many types of offences do not include aggravated or petty forms of a particular crime at all. Below only the basic forms of such offences are included.

Applicable offences related to Hacking are as follows: Chapter 38 Section 3 – Message interception (578/1995), which refers to criminal behaviour where information is obtained on the contents of basically any message protected from outsiders;[145] and Chapter 38 Section 8(b) – an offence involving a system for accessing protected services (919/2014):

> *A person who, in violation of the prohibition laid down in section 269, subsection 2 of the Information Society Code (917/2014), for commercial purposes or so that the act is conducive to causing considerable detriment or loss to a provider of protected services, produces, imports, offers for sale, rents out or distributes a system for accessing protected services, or advertises, installs or maintains the same, shall, unless a more severe or equally severe penalty is provided elsewhere in law for the act, be sentenced for an offence involving a system for accessing protected services to a fine or to imprisonment for at most one year.*

Applicable offences related to Computer network attack are as follows: Chapter 38 Section 5 – Interference with communications (578/1995), which refers to criminal behaviour of malicious transmittal of interfering messages over radio or telecommunications channels;[146] and Chapter 38 Section 7(a) – Interference in an information system (368/2015), which refers to criminal behaviour of entering, transferring, damaging, altering or deleting data that unlawfully prevents the operation of an information system.[147]

Applicable offences related to Espionage are as follows:[148] Chapter 38 Section 8 – Computer break-in (368/2015), which refers to the criminal behaviour of unlawfully hacking into an information system where information or data is processed, stored or transmitted electronically;[149] and Chapter 38 Section 9(a) – Identity theft (368/2015), which refers to the criminal behaviour of unlawfully using personal information, access codes or other corresponding identifying information of another to deceive a third party.[150]

Applicable offences related to Terrorism are as follows:[151] Chapter 34 Section 1 – Criminal mischief *[Sabotage] (578/1995)* (2) '– – Also a person who damages or

145 See details on the exact provision: M. Tolvanen, *Cyber Crimes in Finnish Criminal Law* (2017) at 2.
146 *Ibid* at 4-5.
147 *Ibid* at 6.
148 International law does not outlaw cyber espionage. Espionage is covered only in national criminal law. See C. Vossen, *supra* note.
149 See details on the exact provision: M. Tolvanen, *Cyber Crimes In Finnish Criminal Law* (2017) at 10
150 *Ibid* at 14.
151 Finnish Penal Code, Chapter 34 Section 6 – Definitions:
'(1) An offender has a terrorist intent if it is his or her intent to:
(1) cause serious fear among the population,
(2) unlawfully force the government of a state or another authority or an international organization to perform, allow or abstain from performing any act,
(3) unlawfully overturn or amend the constitution of a state or seriously destabilize the legal order of a state or cause particularly harm to the state economy or the fundamental social structures of the state, or
(4) cause particularly extensive harm to the finances or other fundamental structures of an international organization.'
(2) A *terrorist group* refers to a structured group of a least three persons established over a period of time and acting in concert in order to commit offences referred to in section 1.

destroys property or unlawfully interferes in the operation of production, supply or communications channels, so that serious danger is caused to power supply, public health care, defence, administration of the law or another corresponding important societal function shall be sentenced for criminal mischief. – –'; Chapter 34 Section 9(a) – Endangerment of data processing (368/2015), which refers to the criminal behaviour of possessing/using a technical tool designed to endanger or damage data processing or to break the technical security of an information system;[152] and Chapter 34 Section 9(b) – Possession of a data system offence device (540/2007), which refers to criminal behaviour of possessing/using a technical tool designed to cause impediment or damage to data processing of an information system.[153]

Furthermore, some offences may fall into the scope of terroristic activity only when combining the constitutive elements from two or more Sections, such as: Chapter 17 Section 1 – Public incitement to an offence (563/1998):

> *(1) A person who through the mass media or publicly in a crowd or in a generally published writing or other presentation exhorts or incites anyone into the com- mission of an offence, so that the exhortation or incitement*
> *(1) causes a danger of the offence or a punishable attempt being committed, or*
> *(2) otherwise clearly endangers public order or security, shall be sentenced for public incitement to an offence to a fine or to imprisonment for at most two years.*
> *(2) If the exhortation or incitement causes the commission of an offence or a punishable attempt, the provisions in Chapter 5 on participation apply.*

Combined with:

Chapter 34(a) Section 1 – Offences made with terrorist intent (17/2003)

> *(1) A person who, with terrorist intent and in a manner that is conducive to causing serious harm to a State or an international organisation*
> > *(1) – –*
> > *(2) intentionally commits the offence of imperilment, an intentional explosives offence, a violation of the provisions on dangerous objects, or the public incitement to an offence referred to in Chapter 17, section 1 [emphasis added], shall be sentenced to imprisonment for at least four months and at most four years,*
> > *(3) commits an aggravated theft or an aggravated theft for temporary use directed against a motor vehicle suitable for public transport or the transport of goods, sabotage [emphasis added], traffic sabotage, endangerment of health, aggravated damage to property ... shall be sentenced to imprisonment for at least four months and at most six years, – –*

Furthermore, in accordance with Sections 2–5 also the preparation, directing, promotion, provision of training, training, recruitment and financing of the aforementioned offences are punishable. Financing is punishable both in support of terrorism within the scope of the constituting offences as well as by only financing a known terrorist group in accordance of the definition in Section 6 (2). All the aforementioned may be conducted in cyberspace.

It may be important to also note that in the application of International Law, other States have the same or similar statutes covering the jurisdiction on cross-border criminality:

---

152 See details on the exact provision: M. Tolvanen, *Cyber Crimes In Finnish Criminal Law* (2017) at 14.
153 *Ibid*.

This, in turn means that the variety of jurisdictional bases, two or more States often enjoy jurisdiction over the same person or object in respect of the same event. Considering a case of a terrorist group that launches a cyber attack from the territory of State "A" designed to cause physical damage to State "B's" electricity-generation plants triggering an accident that injures workers. Members of the terrorist group are from various States. State "A" may claim jurisdiction on the basis that the operation occurred there. State "B" enjoys jurisdiction based on passive personality and objective territorial jurisdiction. Other States have jurisdiction on the grounds of the attacker's nationality.[154]

Applicable offences related to Warfare are as follows:

Cyber warfare may be the most challenging to encompass and apply within the scope of criminal law.[155], [156] The only provision explicitly addressing any act fulfilling a war-like scenario in the Finnish Penal Code is the *Crime of aggression* (in force from 2016):

Chapter 11, Section 4a

A person, who factually has the competence and ability to command a State's political and military actions, or leads the aforementioned, commits an act of aggression which by nature, severity, or by scale conforms explicitly to United Nations (UN) Charter[157]*, shall be sentenced for a Crime of aggression imprisonment for at least four years and at most for a lifetime.*

– –

An act of aggression means the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations.

The UN Charter, article 2(4) states that:

'All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.'

It is ambiguous as to whether the article only refers to military force or also to other types of force, such as cyber force. Now, the question is: may a cyber attack, such as scrambling a State's banking data by infiltrating and corrupting its financial sector's computer networks,[158] constitute a force in the meaning of the UN Charter? This issue is not discussed thoroughly in this article; however, some considerations are provided to highlight the legal considerations of the question.

In principle, the content of the law must be clear in order for any criminal proceedings to take place. In accordance with, and in addition to Chapter 1 Section 15 of the Finnish Penal Code, the legal principles on interpretation of law start with the examination of the wording of the provision in question. Secondly, when necessary, the context of the wording (such as preparatory documentation of the provision) as

154 M. Schmitt, *supra* note 29.

155 *Ibid* at 17-18.

156 Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, (Yale Journal of International Law, Vol. 36, 2011), at 443. Available at SSRN: https://ssrn.com/abstract=1674565 or http://dx.doi.org/10.2139/ssrn.1674565

157 Charter of the United Nations, 24 October 1945, 1 UNTS XVI, available at: http://www.refworld.org/docid/3ae6b3930.html (Accessed 2 September 2017).

158 Matthew C. Waxman, *supra* note.

well as the systematic relationship to the law itself, legal system or to the objectives of the law (teleological interpretation) may be examined.

For instance the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations reads:

> *No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.*[159]

Even though the Declaration addresses the non-armed force in the context of international obligations, it does not do so directly under the provisions (namely art. 2(4) and 51) of the UN Charter governing *armed attacks (*commonly referred to *use of force)*. Although it seems that article 2(4) has a wider meaning, encompassing also various methods of non-armed coercion, not all coercive efforts of States would still fall into the scope of the provision. Highly destructive cyber attacks could be seen in some cases as an armed attack (use of force). However, should all forms of non-armed coercion be interpreted as a violation of article 2(4), the threshold of an armed defence action in accordance with article 51 would potentially be simply too low and thus work against the objectives of the Charter itself.

In an effort to overcome the challenge of a cyber attack (e.g. computer network attack), an analysis framework has been developed to determine whether an attack would fall into the scope of article 2(4) (use of force) and thus threaten international peace. The analysis model (commonly known as the Schmitt analysis) is based on seven criteria (severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, responsibility) used to evaluate a cyber attack and focuses on criteria that are dependent on the consequences of the cyber attack and thus is retrospective by nature. Limnéll suggests another criterion: *who* (including the level of confidence in attribution), *impact* (harmfulness), available instruments for response, existing Policy Guidelines and urgency of the response.[160] Limnéll seems to consider that that also the response side is equally important as the analysis of the attack.

As discussed earlier, the main challenge with using the Schmitt and Limnéll analysis is that it requires the aggressive State to be held responsible for the attack. This issue seems to be highly difficult to overcome. Acquiring solid evidence on the State's involvement may prove to be very challenging to the other State's investigation and intelligence authorities. In addition to the technical challenges, one trend seems to be that various private third-party actors (private companies, cyber volunteers etc.) are being used as *covers, fronts* or *decoys* to hide the command and control aspects of the State's involvement. Furthermore, because of the similar tools and techniques used, it is sometimes difficult to attribute cyber-attacks to particular groups, for example, financially motivated cybercriminals and Advanced Persistent Threat (APT) groups (i.e. state sponsored or condoned).[161]

There is always also the possibility that a State that has been attacked will not accuse another State of unlawful action nor take action against it for various political reasons. It seems though that purely legally speaking, the rule of *Control of Cyber Infrastructure* derived from International Law states that, 'a State shall not know-

159 Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (UN Declaration 2625 (XXV), 24 October 1970).

160 J. Limnéll, *supra* note

161 Europol, *Internet Organised Crime Threat Assessment IOCTA* (2017).

ingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.'[162] It means that the State is held responsible for both instances: (i) any cyber infrastructure (governmental or not in nature) located on their territory; and (ii) cyber infrastructure located elsewhere but over which the State in question has either *de jure* or *de facto* exclusive control. This rule applies also in cases even when the unlawful actions are only routed through State cyber infrastructure.[163] The issue of proving the State's awareness of such is not discussed here. As Limnéll states: 'However, it needs to be understood that the answer to the question, whether or not a cyber attack is an act of war, is a political decision and not a conclusion.' [164]

Now, while attempting to examine the issue it is important to highlight that much legal research or commentaries on cyber warfare begin from the onset by stating that cyber operations occurring below the level of a *use of force* in the scope of *jus ad bellum* (international law governing the resort to force by States as an instrument of their national policy) and the *jus in bello* (the international law regulating the conduct of armed conflict) are considered from defence purposes only as cyber criminality.[165], [166]

As the main argument, it must be noted that the attempt here is to address the issue of the applicability of the Finnish Penal Code to cyber operations that may be breaching the aforementioned threshold of *use of force*. Consequently, if such cyber operations are intended to coerce the government (that are not otherwise permitted under international law), the operation may constitute a prohibited *intervention* or a prohibited *use of force*, at least in cases where it causes damage.[167] However, the case of interpreting the meaning of Chapter 11, Section 4a of the Finnish Penal Code may prove erratic due to the obscure applicability and strong dispute over the article 2(4) of the UN Charter by the UN member States.

Furthermore, the attribution of such an operation under the responsibility of a particular State differs from the criminal liability of a person. In principle (although corporate criminal liabilities exist), only a person can be held criminally liable under the Penal Code as States can only be held liable directly under international law.[168] Personal liability has also a different, i.e. *higher* level for attribution in accordance with the Rome Statute of the International Criminal Court, article 8 *bis* '… act of aggression which, by its character, gravity and scale, constitutes a **manifest violation** of the Charter of the United Nations …'.[169]

In regard to the various offences falling into the scope of cybercrime, some issues may be noted: 1) the breaking-points of the evolution of regulation on cybercrime are until now found, on the one hand, in the mid-90s when the Internet

162 M. Schmitt, *supra* note 33.

163 See: Responsibility of States for Internationally Wrongful Acts, article 8 (2001), UN General Assembly resolution 56/83 of 12 December 2001, and corrected by document A/56/49(Vol. I)/Corr.4; Also International Court of Justice: Nicaragua Judgment, para. 115.

164 J. Limnéll, *supra* note 44.

165 Contrary to C. Vossen at 13.

166 'It must be noted that the Tallinn Manual utilises an effect-based approach to cyber attacks and exclusively focuses on second-order consequences, namely, injury, death and damage or destruction to objects. These effects are all extrinsic to the targeted computer or computer network, meaning that the first-order, intrinsic, consequences, such as alteration or deletion of information, are not sufficient to constitute a cyber attack.' See C. Vossen, at 16.

167 M. Schmitt, *supra* note 25–26 and 33–34.

168 Government proposal (legislative motion) HE 289/2014 vp on Amendments to the Rome Statute of the International Criminal Court by the 2010 Review Conference in Kampala (2014).

169 Rome Statute of the International Criminal Court (1998) reproduced with 2010 Kampala amendments. United Nations, Treaty Series, vol. 2187, No. 38544, Depositary: Secretary-General of the United Nations. Available at http://treaties.un.org (Accessed 5 October 2017).

became a mass phenomenon, and on the other hand in 2014/2015, the time when massive data breaches, attacks and other cyber surveillance incidents became a mass phenomenon; 2) the next significant evolutionary step seems yet to be known, but surely it will not take 20 years as nowadays it seems that a new disrupting digital innovation surfaces every 2–3 years.[170] The next phenomenon may well be related to cloud computing, robotics, artificial intelligence etc; 3) thus, it seems to be that more offences may be falling under the definition of cybercrime in the future; 4) cybercrime seems to be manifesting itself very differently from a criminal justice perspective as compared to the mainstream technology-oriented or defence-oriented cyber security perspectives. Thus, cybercrime may not be fully suitable in categorizing cyber threats as it fundamentally implies to the division between the highly debatable legal division of cyber war activities and other cyber activities, thereby creating serious instability in the scope of application of the laws under discussion; and 5) furthermore, also several offences may fall into more than one category in these often defence-oriented threat listings.

5 Conclusions

Although common understanding of cyber security and cybercrime is yet to be reached, one of the objectives of this article has been to decipher the relationship between cyber security and cybercrime and in particular from a legal perspective. Perspectives from various domains of security such as law enforcement, defence and communications governance regimes as well as the private sector seem to be diverging, even when the intention seemingly is to converge.

The main argument has been that cyber security, in fact, is mostly just the absence of cybercrime. Examining what constitutes contemporary security threats in cyberspace within the context of law, as well as examining recent developments in the multilateral policy framework, have substantiated the argument. The focus and foundation is clearly on malicious human activities in cyberspace and thus has shifted from the technologically centred data protection regime to crime prevention. The same could be understood also by differentiating the terms security and safety; by saying, like as for instance the EU External Action Service, that security relates to threats of intended harm (malicious intent) and that safety refers to unintentional harm (accident). The threats addressed to both policy and legal frameworks are the threats constituted by malicious intent; also called cybercrime. Equally, as State-sponsored cyber operations, and to a certain extent cyber war, seems to factually revert to cybercrime, the argument is even more substantiated.

Thus, it seems that even though a lot has been already done, further steps are sorely needed. Legislation is required in all areas, including criminalization, procedural powers, jurisdiction and international cooperation. While the last decade has seen significant developments in the promulgation of multilateral instruments aimed at countering cybercrime, legal fragmentation at the international and national level is also growing.[171] The global governance seems to be the most afflicted by the sluggish pace of development. Looking at all the multilateral efforts, it also seems that

170 Professor J. Limnéll (Cyber Security, Aalto University). *Lecture on Cyber Security* (at European Security and Defence College High Level Course, Tampere, 7 March 2017).

171 See, e.g. United Nations Office on Drugs and Crime. *Draft Comprehensive Study on Cybercrime* (February 2013) at 51.

so far, the European Union has grasped the best grip on the cross-border response to cybercrime. Taking the task from *talk-the-talk* to *walk-the-walk* means capitalizing on the already robust and consistent policy framework and moving on to passing legislation in criminalization, procedural powers, jurisdiction and international cooperation. Unfortunately, the global strategic response is yet to be realized. In all fairness, also in the EU the operational response, along with the impact on cybercrime, is yet to be witnessed. As Europol reported with the release of the 2017 IOCTA report: 'the response to unprecedented cyber-attacks is not good enough.'[172] The global scale, impact and rate of spread of cyber-attacks over the past year is unprecedented.[173]

Another argument has been that cyberspace differs from the tangible world of atoms; the physical world fundamentally. There are persistent challenges to the cyber world that require the approach to regulation to be equally expiated and adjusted to match the cyber laws-of-nature. Old wisdom tells us 'what got us here, won't get us there'. New thinking and ideas are needed – some old and entrenched ideas may have to be left behind as well. A disclaimer to the argument above is, however, that cyberspace and physical space are not completely different. The intention is not to say that legal concepts such as international law *per se,* instruments of procedural law as well as substantive elements of crime would not be mostly adequate and fit-for-purpose in cyberspace. However, some legal principles, such as the territoriality (including extraterritoriality) principle as a core principle of jurisdiction should be dismissed and a new concept of investigative jurisdiction should be endorsed.[174]

The third main argument has been, in regard to the factual (legal) nature of cyber security mentioned above, that there is both a deficit of and a competition for leadership in cyber security. Depending on whether the argument has been sufficiently backed up by the presented arguments, consequently, it would mean that the law enforcement authorities (including the relevant ministries) should have a much larger role and more leadership in cyber security. An absence of cybercrime contributes to trust in cyberspace. For instance, (online) non-cash payment fraud causes direct economic losses of at least EUR 1.44 billion a year and reduces consumers' trust, which seems to result in reduced economic activity and limited engagement in the digital market.[175] According to the most recent *Eurobarometer on Cyber Security*, the vast majority of Internet users (85 %) feel that the risk of becoming a victim of cybercrime is increasing. In addition, 42 % of users are worried about the security of online payments.[176]

For instance, the computer network attacks against SWIFT (Society for Worldwide Interbank Financial Telecommunication banking system), which provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment, have been referred to as cyber warfare or hybrid attacks due to originating from the Democratic People's Republic of North Korea. At least one successful case was the Central Bank of Bangladesh misplacing USD 81 million. As Mikko Hyppönen, the Research Director of F-Secure, stated in his keynote speech at the Next Web Confer-

172 *Europol: the response to unprecedented cyber-attacks "not good enough"* (SC Media UK 28 September 2017). Available at: https://www.scmagazineuk.com/europol-the-response-to-unprecedented-cyber-attacks-not-good-enough/article/696298/ (Accessed 3 October 2017).

173 Europol, *Internet Organised Crime Threat Assessment IOCTA* (2017) passim.

174 D. Svantesson, *Preliminary Report: Law Enforcement Cross-Border Access to Data* (2016). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874238. (Accessed 11 October 2017).

175 European Central Bank, *Fourth report on card fraud* (July 2015) [latest data available].

176 Explanatory Memorandum of the Proposal for a Directive of The European Parliament and of The Council of 13 September 2017, on Combating Fraud and Counterfeiting of Non-cash Means of Payment and Replacing Council Framework Decision 2001/413/JHA.

ence: 'Calling these attacks cyber or hybrid warfare is misleading, the attack was a crime of (aggravated) *theft* –a theft committed by a State'.[177]

However, it seems that the void in leadership has largely been taken by the defence and military authorities. Although this has been with good intentions, it is misplacing the focus and potentially causing strategic de-alignment with the core mandates of the security authorities. In examining the issue of strategic alignment of State security actors and their roles through the existing legal framework, the conclusion is that the core purpose of information and communications (ICT) authorities is to act as the *cyber fire brigade* providing *safety* in cyberspace. The military's core purpose is still to defend the State (i.e. conduct intelligence operations, develop resiliency and counter-measures as well as cyber weapons) against external military threats (i.e. acts of war) and, when needed, to support other security authorities in implementing their mandates (via legal assistance). The evolution of cyberspace, and recalling the *de lege* and *de facto* of the sovereignty of States, has not changed this fact, even despite the emergence of State-originated cyber and hybrid threats.

Finally, another argument has been that the prevalent and undeniable challenges of the attribution of cyber operations to State-actors significantly undermines the aforementioned military tasks. This is to say that a vast majority of even State-originated operations factually revert to cybercrime due to the covert and deceiving nature of cyber operations.[178] Thus, it seems justifiable that the strategic positioning of cyber security should be seamlessly aligned with the existing State criminal policy by following the well-established roles and responsibilities of other areas of crime. Comparably, this has also been discussed in terms of cybercrime situational awareness, e.g. in Finland.[179] This conclusion can also be compared to the infamous real-world case of Crimea, where the *unidentified* and *covertly* operating 'green men' took over the public institutions and later the territory of Crimea. Public institutions did not have adequate security and contingency plans or resilience to deal with the situation at hand. Analysis has shown that eventually it was the Ukrainian law enforcement authorities, challenged with a multitude of deficits, that consequently failed to maintain public order and security during the operation. Comparably, within EU States for instance, responding to a similar situation would clearly and undeniably be a law enforcement-led operation, as was the case in the recent terrorist attacks in Paris and Brussels. The same should apply in cyberspace as well.

To avoid any misunderstanding the author is not suggesting that the existing roles, responsibilities and structures should be disbanded or dismantled in any way. However, as it seems that getting a grip on the new, quickly evolving phenomenon would require a clarification of how the strategic leadership should be organized,[180] a comparison with existing criminal policy systematics is justified. As in all other crime areas in modern societies, public security and anti-crime has for a long time

177 (IS Digitoday 26 May 2016). Available at http://www.is.fi/digitoday/tietoturva/art-2000001912418.html (Accessed 26 September 2017).

178 See, e.g. Europol, *Internet Organised Crime Threat Assessment IOCTA* (2017) at 26: 'When discussing (cyber-physical) attacks on critical infrastructure, there is often a focus on the worst case scenario – sophisticated state-sponsored or condoned attacks on vulnerabilities in industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems in the likes of power plants and heavy industry. While these threats are undoubtedly real, such attacks are rarely, if ever, reported to law enforcement, instead more likely falling into the territory of national security. There are however far more common and more likely attack vectors and targets [to cripple the critical infrastructure of States], which do not require attackers to penetrate such isolated networks… it is clear that a greater variety of critical infrastructures are more vulnerable to "every-day" cyber-attacks, highlighting the need for a coordinated EU law enforcement and cross-sector response to major cyber-attacks on critical infrastructure.'

179 A. Leppänen, et al. *supra* note 19.

180 M. Lehto et al. *supra* note, passim.

been characterized by fragmented ownership, diversity of actors and an urge for cooperation. Cyber security is unequivocally a joint task and joint ownership of all stakeholders. The future of digital security is generated from trust, cooperation and responsibility.

FUNDAMENTAL RIGHTS CONFLICTS IN THE CONTEXT OF PURSUING INTERNET CRIME

Katja Weckström Lindroos*

1 Introduction

The EU Court of Justice (CJEU) has recognized the need to balance competing fundamental rights in *Promusicae,*[1] *Bonnier Audio*[2] and *UPC Telekabel*[3] decisions when interpreting directives and national legislation. Yet, it has left to national law to determine how fundamental rights should be balanced in national proceedings. In a recent Grand Chamber ruling on the fundamental rights of applicants for international protection, it was confirmed that member states must not only interpret national law in a manner consistent with European Union (EU) law but that they should also ensure that they do not rely on an interpretation that would be in conflict with the fundamental rights protected under EU law.[4] In addition to the more traditional four economic freedoms, fundamental rights are of growing importance in interpreting secondary legislation of the European Union.[5] Competing interests triggered in contemporary disputes may enjoy protection under Articles 11 (freedom of expression and information), 16 (freedom to conduct business), 17 (right to property), 36 (access to services of general economic interest) and 38 (consumer protection) of the Charter of Fundamental Rights. Likewise, the principles of legality and proportionality of criminal offences and penalties enshrined in Article 49 of the Charter of Fundamental Rights are important when assessing extending liability for illegal acts and eliminating trade of illegal goods.

The conflicts between fundamental rights are increasing in the digital environment and demands for less or more intervention by authorities are placed on courts, officials and legislatures. Legal traditions differ. Yet, the United States' constitutional tradition has great impact on activity and ideology, if not law, on the in-

* Professor of Commercial Law at UEF Law School, University of Eastern Finland. The author would like to thank Research Assistant Kaarina Leppänen for her excellent research support. Any errors remaining in the text are attributable to the author. Comments welcome at katja.lindroos@uef.fi.

1 Case C275/06 Promusicae [2008] ECR I-271, judgment of (Grand Chamber) 29 January 2008; See also P. Mezei and D. Hajdú, *Introduction to Digital Copyright Law* (Szeged: University of Szeged, Faculty of Law, 2015): 'The Role of Technology and Consumers´ Needs in the Evolution of Copyright Law'. Originally published in Éva Jakab (ed.), *Geistiges Eigentum und Urbeberrect aus der historischen Perspektive* (Szeged: Lectiones Iuridicae 10, Pólay elemér Alapitvány, 2014) 71-79.

2 Case 461/10 Bonnier Audio, judgment of (Third Chamber) 19 April 2012.

3 Case C-314/12, UPC Telekabel Wien GMbH v. Constantin Film Verleih, judgment of (Fourth Chamber) 27 March 2014; See also G. Mazziotti, *EU Digital Copyright Law and the End-User* (Berlin: Springer, 2010); A. Strowel (ed.), 'Internet Piracy as a Wake-up Call for Copyright Law Makers – Is the Graduated Response a Good Reply?' *WIPO Journal* (2009) 75-86.

4 Case C-601/15 PPU, J.N. v. Staatssecretaris vor Veiligheid en Justitie, judgment of (Grand Chamber) 15 February 2016, at 60.

5 Art. 2 and 6(2) TEU and the Charter of Fundamental Rights. The Lisbon Treaty places an obligation on the EU to accede to the European Convention on Human Rights; P. Craig The Lisbon Treaty- Law Politics and Reform (Oxford, 2010), at 201.

ternet.[6] Depending on personal conviction, online acts may be viewed as criticism of the regime, mere civil disobedience or criminal activity. These convictions fuel fundamental rights discourses in judicial processes. This chapter aims at revealing general principles underlying the practical resolution of fundamental rights conflicts. It discusses policing online activity in preventing criminal activity. It covers some measures against the spread of child abuse material (CAM) and securing fundamental rights in public administration. It also discusses enforcement against illegal sharing of copyrighted works and the consequences of shifting from public to private enforcement against criminal acts.

2 Police Constraints on Freedom of Expression Online

Constitutional values are necessarily expressed in specific terms when granting rights and freedoms to citizens. In many European nations, including Finland, these rights and freedoms have been viewed as constitutional guarantees as opposed to subjective rights. This means that rights are routinely guaranteed in the legislative process as opposed to redressable in judicial processes. The European Convention on Human Rights (ECHR)[7] lists the rights and freedoms each member state must guarantee its citizens, as well as how and when derogations from these rights by governments are permitted. With the exception of the prohibition against torture (Article 3 ECHR) and punishment without law (Article 7 ECHR), the freedoms and rights are not absolute.[8] The ECHR as interpreted by the European Court of Human Rights (ECtHR), has developed extensive principles and procedural requirements that must be put in place in order to secure protection for the rights and freedoms of natural and legal persons. In *K.U. v. Finland* the ECtHR recognized that the requirement of confidentiality of correspondence on the internet does not release the government from providing remedies to citizens against criminal activity online.[9] The EU recognizes this case law and allows its Court of Justice to deviate from it but only to the extent that EU law offers more extensive protection for fundamental rights than the ECHR.[10]

6 The state of the law in Europe naturally reflects European constitutional values (see section 2 below). The arguments furthered in policy discussion, and also by offenders in their defence, are influenced by an ideology based on minimum government intervention (the Framework for Global Electronic Commerce a.k.a. the Clinton Framework, published by President Clinton in 1999) and greater personal freedom online. The fundamental rights conflicts discussed in this chapter represent this ideological intersection in law.

7 European Convention of Human Rights, signed in Rome on 4 November 1950 and entered into force 3 September 1953 as amended by Protocols Nos. 11 and 14 and supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13.

8 Some specific derogations are listed in the Convention text (e.g. Article 2 and 4), while others are left to member state discretion.

9 Case of *K.U. v. Finland*, 2872/02, judgment of (Fourth Section) 2 December 2008. It was recognized that the legislator satisfied its obligation under Art. 8 through provision of remedies in the Freedom of Expression in Mass Media Act. Thus, the case related to a lack of remedy to pursue the crime (in 1999). The court emphasized that 'a positive obligation must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities or, as in this case the legislator. Another relevant consideration is the need to ensure that powers to control, prevent and investigate crime are exercised in a manner which fully respects the due process and other guarantees which legitimately places restraints on criminal investigations and bringing offenders to justice, including the guarantees in Articles 8 and 10 of the Conventions, guarantees which the offenders themselves may rely on', at 48.

10 Case of *Peter Puskar v. Finance*, C-73/16, *riaditeľstva* Slovneskej republiky, *Kriminálny úrad finančnej správy*, Opinion of Advocate General Kokott of 30 March 2017, at 123.

Article 10 of the ECHR reads:

> Freedom of expression
>
> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties, as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity, or public safety, for the prevention of disorder or crime, for the protection of health and morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Section 12 of the Finnish Constitution reads:[11]

> Freedom of expression and right of access to information
>
> Everyone has the freedom of expression. Freedom of expression entails the right to express, disseminate and receive information, opinions and other communications without prior prevention by anyone. More detailed provisions on the exercise of the freedom of expression are laid down by an Act. Provisions on restrictions relating to pictorial programmes that are necessary for the protection of children may be laid down by an Act.
>
> Documents and recordings in the possession of the authorities are public, unless their publication has for compelling reasons been specifically restricted by an Act. Everyone has the right of access to public documents and recordings.

The First Amendment of the United States' Constitution reads:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

11 Unofficial translation provided by Finlex available online at https://www.finlex.fi/en/laki/kaannokset/1999/en19990731.pdf
(visited 18 January 2018).

In *Packingham v. North Carolina* the U.S. Supreme Court held a statute criminalizing the use of social media accounts by former sex offenders as unconstitutional since it unduly restricts their freedom of speech.[12] Unlike the constitutional interpretation of the United States Supreme Court regarding *freedom of speech*,[13] the *freedom of expression* of Europeans is not absolute: the government may, and should,[14] lawfully restrict the freedom of one in securing the rights and freedoms of others.[15]

In Europe, the question therefore is not whether a government measure restricts a freedom or right but whether it does so unlawfully. If a legislative proposal is deemed to restrict a freedom or right unlawfully, the legislator has two options:

1) it can amend the proposal to remove unlawful restrictions; or
2) it can adopt the proposal according to the constitutional amendment procedure.

Each option serves to legitimize the legislation in question and renders it constitutional *per se*. Whether a piece of legislation is unconstitutional in application is a question that each national constitution (or legislation) renders assessable:

1) *ex ante* in the legislative process;[16]
2) *ex ante* or *ex post* by a special constitutional court or institution[17] or
3) in the form of *ex post* judicial review of legislative acts.[18]

In countries where the unconstitutionality of legislative acts is assessed solely in the legislative process before enactment, change is only possible by influencing democratic decision-making.[19] Some countries in Europe have separate constitutional courts (Germany, Poland), while others have permanent organs (France) that decide the constitutionality of acts. In some countries, like France, only the legislator can refer acts for review, while in others institutions or citizens may bring a case before the court or institution. The systems also differ in the authority attached to the decisions of the institution and its binding force on the legislator/government in theory and in practice.

The power of *judicial review* of all legislative acts by all courts (akin to the federal courts in the United States) is not present in Europe. Some countries grant their highest court(s) the right of *constitutional review*; however, the extent to which this right is exercised tends to be limited.[20] The contemporary era of constitutionalism

12 *Packingham v. North Carolina*, 582 U.S. ___ (2017) decision of 19 June 2017.
13 *Gitlow v. New York*, 268 U.S. 652 (1925), decision of 8 June 1925, progressively limited by *Yates v. United States*, 354 U.S. 298 (1957), decision of 17 June 1957, and *Brandenburg v. Ohio*, 395 U.S. 444 (1969), decision of 9 June 1969.
14 Case of *K.U. v. Finland*, 2872/02, judgment of (Fourth Section) 2 December 2008, at 49.
15 For an extensive comparison of the European Court of Human Rights' and the United States' approach to freedom of expression see K. Weckström, 'The Lawfulness of Criticising Big Business', *Lewis & Clark Law Review* (2007). Vol. 11, n. 3.
16 Perustuslakivaliokunta (The Constitutional Law Committee of the Finnish Parliament).
17 Bundesverfassungsgericht (The German Constitutional Court) or Conseil constitutionnel (the French Constitutional Council), which is attached to Parliament. The preliminary rulings procedure of the European Union Court of Justice is modelled on the French system of Priority Preliminary Rulings by the Constitutional Council.
18 All federal courts in the United States may review the constitutionality of a piece of federal legislation or state legislation that raises federal constitutional concerns.
19 Suomen perustuslaki (Finnish Constitution) 74 § and 106-107 §§.
20 Finnish Constitution 106-107§ restricting application to clear conflicts with existing law.

has increased constitutional interpretation in courts across Europe that seeks to find a *consistent interpretation* with constitutional values.[21] Such thorough consideration and reconciliation of all interests is still rare in lower and intermediary level courts. While a court decision may consider an act unconstitutional and refrain from its application in the circumstances of a given case, in general, a change in the state of the law requires a legislative amendment.[22]

A Finnish example illuminates the difference. Section § 106 of the Finnish Constitution allows the Supreme Courts of Finland the right to judicial review and non-application of legislative provisions in the circumstances of a specific case if the provision is in apparent conflict with constitutional provisions. Only the legislature can amend acts with an unconstitutional effect.

In a case before the Supreme Administrative Court, a Finnish citizen (A), who was a computer specialist, maintained the lapsiporno.info website,[23] which included information criticizing internet security measures to prevent the spread of CAM and its implementation by the police. To make a point about how legitimate sites were blocked by the police, A discovered the internet addresses of all the sites on the police CAM blocking list[24] and then published the blocking list along with links to foreign CAM – sites on the lapsiporno.info –website. Over the course of time, the site linked to 350 sites containing CAM, and by the time the case reached the Supreme Administrative Court, it linked to 19 sites.[25] The police blocked access to the site based on national legislation on preventive measures against the spread of child pornography.[26] The site would remain on the block-list until the grounds for the measure were removed.[27]

A argued that since his point was to expose weaknesses in policing and to debate internet security issues, the publication constituted constitutionally protected expression. A demanded that the police remove the site from its blocking list since the measure constituted a prior restraint on freedom of expression and thus was in apparent conflict (ilmeinen ristiriita) with Article 12 § 1 of the Finnish Constitution.[28] The Supreme Administrative Court of Finland stated that in assessing the constitutionality of a legislative act in the circumstances of a particular case (under § 106 of the Finnish Constitution[29]), the provision in question must clearly and unequivocally be in conflict with the constitutional mandate in question in order for a

21 EU Fundamental Rights Charter Article 52.

22 Finnish Constitution 3 § and 106-107 §§. Case of *K.U. v. Finland*, 2872/02, judgment of (Fourth Section) 2 December 2008, at 48-49; Case C275/06 *Promusicae* [2008] ECR I-271, judgment of (Grand Chamber) 29 January 2008.

23 This translates to childporn.info.

24 The police also investigated whether FC would face criminal charges for the spread of child pornography, but the charges were later dropped. Note here the connection to *K.U. v. Finland*, at 48 highlighting the difference between lawful government measures that protect others and measures that target offenders. The police are required to protect children under Art. 8 of ECHR but may be limited by Art. 8 and 10 of ECHR when prosecuting offenders. The list was also published on Wikipedia, which has not been subject to blocking by the Finnish police.

25 The police blocking list included sites that had no child pornography on them.

26 Laki lapsipornografian levittämisen estotoimista (1068/2006) (Act on blocking Child pornography)

27 By law the final authority to determine whether an item satisfied the criteria for placement on the black list lies with the police. Questions of fact are not subject to appellate review.

28 It was also argued that the site did not include any child pornographic material (only links to them) and that the law did not apply to Finnish sites, only to foreign ones. The court dismissed both claims as contrary to legislative intent, which would clearly undermine the purpose of the law. Korkein hallinto-oikeus (Supreme Administrative Court) (hereinafter:KHO), KHO 2013:136, judgment of 26 August 2013,.

29 § 106 of the Finnish Constitution allows ex post *non-application* of legislative provisions in the circumstances of a specific case if the provision is in apparent conflict with constitutional provisions. Only the legislature can amend acts that have unconstitutional effect.

court to desist from its application. Since the site was blocked only after the links were included, the measure did not constitute a prior restraint on expression. This remained so, even though it effectively prevented continued availability of lawful and protected expression, as well as future expression on the site.

In assessing the proportionality and predictability of the measure, the court relied on similar restrictions in the Freedom of Expression in Mass Media Act[30] and the Information Society Services Act,[31] which had both passed into legislation without raising constitutional concern in the Constitutional Committee. The court further considered the legitimacy of the measure

> 1) in light of the interest in protecting the constitutional rights of others (children);
> 2) in regard to whether it was sufficiently and specifically tailored to achieve its purpose; and
> 3) to ascertain whether it adequately safeguarded the right to a fair trial.

In light of the gravity of the interests protected by the availability of the blocking measure and the lack of protection of any right to distribute child pornography, the measure was proportionate to the end sought, regardless of its negative impact on socially valuable expression, because the opposite conclusion would render the law easily circumvented and ineffective in practice. A was free to engage in social criticism through other means or avenues. The blocking of the lapsiporno.info-website did not unlawfully restrict his exercise of freedom of expression.[32]

In this case it was clear that the criticism of the police and the doubtful effectiveness of internet filtering mechanisms was valid. The police blocking-list did include sites containing no child pornography. A was entitled to hold and express his opinion, but the means by which he can do so can be lawfully restricted. Means that are criminal or unlawful by legislative act do not constitute unlawful derogations from constitutionally protected freedoms or rights merely because of the hierarchal relationship between constitutions and legislative acts. The Finnish Constitution 3 § and 12 § unequivocally gives the power to enact laws to the legislator as long as procedural requirements are met. By special law the final authority to determine whether an item satisfies the criteria for placement on the block list lies with the police. Questions of fact are not subject to judicial review. Thus, the Supreme Administrative Court did not re-evaluate whether the police had been right, only whether they acted within their authority under the law.[33]

Some constitutional democracies prefer that this power lies solely with the legislature and consider 'government of judges' as illegitimate as rule by men.[34] While the fears connected to 'government of judges' may be debated as well as contested, the civil law tradition in Europe has generally been reluctant to entrust large ques-

30 Laki sananvapauden käyttämisestä joukkoviestinnässä (13.6.2003/460) (Act on the Exercise of Freedom of Expression in Mass Media) unofficial translation provided by Finlex available online https://www.finlex.fi/fi/laki/kaannokset/2003/en20030460.pdf (visited 18 January 2018).

31 Laki tietoyhteiskunnan palvelujen tarjoamisesta (5.6.2002/458) (Act on Provision of Information Society Services) since repealed and incorporated in the Information Society Code 7.11.2014/917. Unofficial translation provided by Finlex available online at https://www.finlex.fi/fi/laki/kaannokset/2003/en20030460.pdf (visited 18 January 2018).

32 KHO 2013:136, judgment of 26 August 2013.

33 KHO 2013:136, judgment of 26 August 2013.

34 Edouard Lambert, Le gouvernement des juges et la lutte contre la législation sociale aux Etats-Unis -L'expérience américaine du contrôle judiciaire de la constitutionnalité des lois (1921). For different interpretations of the concept 'government of judges' see M. H. Davies, 'A government of judges: An Historical Re-view', *The American Journal of Comparative Law*, Vol. 35, No. 3 (Summer, 1987) 559-580.

tions with regard to the balancing of competing interests to unelected officials. The function of the judiciary is grounded more in providing fair and impartial review than it is in truly functioning as checks and balances on the legislature.[35] Thus, while Europeans do not value rights and freedoms less, they trust the government more in achieving a fair balance between legitimate interests.[36] Naturally, some European citizens trust the government less than others due to their national histories of oppression, abuse and non-functioning government. This historical mistrust explains why many Eastern European states elected to institute a constitutional court as a check on government.

3 Protecting Rights against Acts of Ideology

There are naturally diverse views on whether laws should protect certain interests. Acts of ideology can be targeted against the government or against private property interests. However, the internet and the intangible nature of transactions raise other problems for legal interpretation. Can you be held criminally responsible for taking

1) something that is not in anyone's possession;[37]
2) something that is intangible;[38] or
3) something that is widely shared online?

The EU Fundamental Rights Charter specifically includes protection of intellectual property as property.[39] Finnish criminal law is in accord. The object of the theft is not really the item but usurping the rights of the owner to control the item.[40] Therefore, regardless of whether the rights position is strong or weak, theft occurs when its content is removed from its holder. However, an item which is not within the victim's possession, e.g. a wild animal or an abandoned item, cannot be subject to theft.[41] Quite perplexingly, however, it is not required that the item is actually in the possession of the owner. This can be explained with retaining ownership of, e.g. rented property. *Possession for the purposes of theft* may be realized through actual control (hallinta) or expressed desire to control (vallinta) through, e.g. property administration. It is not relevant whether the owner knows exactly where the property

35 Many fears stem from the unease connected with the effect on the impartiality of judges if they are elected on political grounds in Europe.

36 This statement is directed at structures of governance and government and the functioning of the legal system. Although many Eastern European states elected to institute a constitutional court as a check on government, the system of government still follows the civil law tradition and places the most extensive power in the hands of the democratically elected legislature.

37 For a detailed discussion on whether property rights may be taken in virtual worlds, see K. Weckström, 'Trademarks in Virtual Worlds: Law, Outlaws or New in-Laws?' *Journal of International Commercial Law and Technology* (2012) Vol. 7, Issue 2 (Weckström 2012a). For a detailed discussion of whether virtual furniture may be subject to theft, see K. Weckström, 'Chasing One's Tail: Virtual Objects as Intangible Assets, Intangible Property or Intellectual Property' in *Varallisuus, vakuudet ja velkojat* – Juhlajulkaisu Jarmo Tuomisto 1952 – 9/6 – 2012 (Turun yliopiston oikeustieteellinen tiedekunnan julkaisuja A-sarja 2012) (Weckstrom 2012 b).

38 For a detailed discussion of whether intangible items may be subject to theft, see (Weckstrom 2012 b).

39 Article 17 Right to property: 1. Everyone has the right to own, use, dispose of and bequeath his or her lawfully acquired possessions. No one may be deprived of his or her possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss. The use of property may be regulated by law in so far as is necessary for the general interest. 2. Intellectual property shall be protected.

40 Weckström 2012b, at 495; D. Frände et al., *Keskeiset rikokset* (Edita, 2010), at 354.

41 Weckström 2012b, at 496; Frände et al. 2010, at 354.

is (e.g. a misplaced phone) but simply that he is the true possessor or administrator of the item.[42]

Article 54 of the EU Fundamental Rights Charter also includes a provision against abuse of rights. The Charter cannot be interpreted as implying any right to engage in activity or to perform acts aimed at the destruction of other recognized rights and freedoms.

Furthermore, it is relevant that unlawful taking of property by the owner from, e.g. a renter may constitute theft.[43] The holder of the stronger right in the *subject matter* cannot usurp the *rights position* of the holder of a lesser right in the same or similar subject matter. The relativity of property rights may give rights against third parties that would not be valid against a holder of a prior right.[44] The nature of the infrastructure of property rights would seem to preclude relying on the right of a third party to breach another's right. The fundamental rights system is equally complex seeking to strike a balance between multiple competing interests. Adding multiple actors and layers of criminal activity or disinterested actors strains the interpretation of existing rules in practice. We will next discuss some examples relating to enforcement of rights against illegal file sharing.

The Supreme Court has assessed criminal liability for intermediaries that facilitate copyright infringement.[45] None of the verdicts were unanimous. In the *Mailbox*-case[46] the defendant had maintained an e-mail mailbox, which he allowed members to use if they shared a copy of a computer program. After gaining access the members could download the computer programs that other members had shared in the mailbox. At issue was whether the defendant could be held criminally liable (commercial copyright offence[47]) for the making available of copyrighted works for setting up the system (not only for the copies he had made and shared with others). While the system predominately was free of charge, the court found the defendant guilty of the aggravated offence based on

> 1) evidence that the defendant had gained access to several valuable computer programs;
> 2) evidence there was trading for payment;
> 3) the mailbox entailing copies of 443 software programs; and
> 4) the act being intentional and planned.

The defendant's sophisticated computers were forfeited to the government since they were essential for the execution of the crime.[48] When calculating the compensation (not damages) the Supreme Court rejected the right holders' requests for compensation based on the purchase price of the software. The law provides for reasonable

42 Weckström 2012b, at 496; Frände et al. 2010, at 355.
43 Weckström 2012b, at 496; Frände et al. 2010, at 355; W. Landes and R. Posner, *The Economic Structure of Intellectual Property Law* (Belknap Press 2003), at 29 and 31.
44 Ibid., at 29 and 31–32.
45 For a detailed discussion on direct and indirect liability for intermediaries see K. Lindroos, 'Ch. 8 Intermediary Liability for IP Infringement in Finland: Copyright vs. Copyleft—A Series of Legislative Proposals and Decade of Debates', in G B Dinwoodie (ed.), *Secondary Liability of Internet Service Providers* (Berlin: Springer Publishing, 2017); K. Weckström, 'Ch. 9, Preliminary Injunctions Against Intermediaries for Trademark and Copyright Infringement', in Katja Weckström (ed.), *Governing Innovation and Expression: New Regimes, Strategies and Techniques* (Turun yliopiston oikeustieteellisen tiedekunnan julkaisusarja A:132, 2013).
46 Korkein oikeus (Supreme Court) (hereinafter:KKO), KKO 1999:115, judgment of 1 November 1999.
47 Under the law in force the defendant was prosecuted for the copyright offence, which required commercial activity.
48 KKO 1999:115, judgment of 1 November 1999.

compensation, which mandates consideration of the circumstances of the case. The court found that the intentionality of the acts of the defendant required that the compensation be significant, weighed it against the hobby nature of the activity and concluded that it would be reasonable to calculate the compensation based on half of the purchase price (app. 680,000 FM[49]). The court rejected the supplemental claim for damages because no proof had been presented of actual damages. Of the dissenting judges one would have determined compensation at a rate of app. 100 % of the purchase price (1, 320,000, and the other would have accepted that compensation of 50 % and ordered damages of 132,000 FM).

The *Finnreactor* -cases involved a P2P-network, and the Supreme Court assessed the criminal liability (as complicit main offenders or abettors) of the administrators of the network as well as the compensation/damages payable to the right holders.[50] A private person that had shared files in the network was not held responsible as an administrator but was guilty of the petty offence of making available copyright infringing material.[51] The network divided its users into seven categories based on their ratio number, which indicated the frequency of shares to the network. The higher the ratio number of the user, the greater the rights, duties and perks. Users with a low ratio number could receive a warning, get demoted to a lower category or have their accounts closed. Starting from level 4 the users also had administrator duties. Level 4 administrators could promote or demote users between categories and delete files from the network (four defendants). Level 5 administrators could also delete or add users. These administrators would also advise users and monitor their sharing habits (five defendants). The highest level 6 administrators were also in charge of the technological functioning of the network (two defendants).

Each defendant was charged with the petty offence[52] as direct infringers/accomplices or alternatively as abettors. The level 5 and 6 administrators were found guilty as main offenders/accomplices,[53] while the level 4 administrators were found guilty for aiding and abetting.[54] Two of the abettors were juveniles. Although the Copyright Act had been changed (toughened) prior to the Supreme Court verdict, the defendants were convicted based on the old law.[55]

The court considered the issue from the perspective of the principle of legality, i.e. an act is punishable only if it is defined as such by law at the moment of commission. While interpretation is necessary and allowed,[56] acts may not be included by analogy if the act does not fall within the object of protection that can be derived

49 The amount of compensation is roughly equivalent to the price of three family homes, or 10 annual salaries.

50 KKO 2010:47, judgment of 30 June 2010.

51 KKO 2010:48, judgment of 30 June 2010.

52 *tekijänoikeusrikkomus*.

53 *tekijä/osallisuus*. For further information see M. Tolvanen and J. Tapani, *Rikosoikeuden yleinen osa: Vastuuoppi* (Talentum, 2008).

54 (avunanto).

55 According to general doctrines of criminal law, like the principle of legality and *in dubio pro reo*, an act is punishable only to the extent it was criminalized at the time of commission.

56 KKO 2002:11, judgment of 26 February 2002; KKO 2004:46, judgment of 19 May 2004; KKO 2005:27, judgment of 24 February 2005; KKO 2007:67, judgment of 26 July 2007 and KKO 2007:81, judgment of 23 October 2007; See also R. Smith, *Textbook on International Human Rights* (4th Edition, Oxford: Oxford University Press 2010), at 261.

from the essential elements of the crime and if the result cannot reasonably be anticipated by the offender.[57]

All the defendants argued that their actions did not constitute copyright infringement since they had not taken part in the actual copying or sharing of copyrighted works or possessed the copyrighted works at any time. The acts of the direct infringers were not the direct consequences of their acts as administrators of the network. Their administrative acts did not target single copyrighted works, nor had they any knowledge of the specific works that were available in the network.[58]

The Supreme Court referred to the *Mailbox*-case in determining that it is not required that the perpetrator actually makes physical copies available to the public, although this has been the main rule. Thus, the act of giving physical copies to someone else that makes them available to the public has not been considered copyright infringement.[59] However, the act of selling the licensing documents that had been removed from the software packaging did constitute the making available of copyrighted works, although the buyer did the actual copying of the software.[60] All these cases concerned an individual offender and not, as in this case, a group. The court thus had to consider whether the defendants' acts constituted copyright infringement individually or jointly.

According to Finnish (criminal) law[61] two or more people intentionally committing a crime together are each punished as main offenders. The prerequisite for complicity is knowledge that one's own acts in accord with the acts of others will satisfy the essential elements of the offence. If that is the case the offender is responsible for the result of the acts taken together, not merely for his own acts, as long as one's own acts constitute a significant contribution to the crime. A lesser contribution will be assessed as aiding and abetting[62] in the commission of a criminal offence.[63]

The Supreme Court takes as its (copyright law) starting point that electronic copies constitute 'the making of copies' that require the copyright holder's consent, whether it amounts to copying actual works or transfers between computers or other media equipment. Because the network required sharing of files for the actual copying of works, it did not fall within the exception of 'making a few copies for private use.'[64] [65] The acts of all users of the network nonetheless constituted the unlawful 'making available to the public' of copyrighted works without the copyright holder's consent. Subsequent case law no longer addresses the issue of copying, since copyright infringement occurs solely when making copyright content available to the public without the right holder's consent.[66]

The Supreme Court found that the torrent files that the network made available were essential for the users to accomplish the actual copying, as well as for the users

57 The principle of legality is enshrined in Sec. 8 of the Finnish Constitution and has its origin in Article 11 (2) of the UN Declaration of Human Rights and Article 7(1) of the European Convention of Human Rights. The international conventions also include a qualifier for the principle, e.g. in Article 7(2) ECHR: 'This article shall not prejudice the trial and punishment of any person for any act or omission which, at the time when it was committed, was criminal according the general principles of law recognised by civilised nations.' Article 49 of the Charter of Fundamental Rights of the European Union confirms protection of this fundamental human right.

58 KKO 2010:47, judgment of 30 June 2010, at 7.

59 KKO 1999:8, judgment of 28 January 1999.

60 KKO 2003:88, judgment of 3 October 2003.

61 Chapter 5:3 of the Penal Code.

62 *avunanto* For further information see M. Tolvanen and J. Tapani 2008.

63 Chapter 5:6.1 of the Penal Code.

64 Under section 56a § 2 of the Copyright Act such copying is not punishable as a crime.

65 KKO 2010:47, judgment of 30 June 2010, at 16.

66 See for example MAO 419/16, decision of 4 July 2016; MAO 55/17, decision of 7 February 2017 and MAO 565/17, decision of 15 September 2017.

to know which copyrighted works were available in the network. The network was specifically designed for the efficient distribution of copyrighted works. Thus, while the acts of each administrator were not essential for the actual sharing and copying of works, it did not preclude complicity or viewing the acts together as one. From this starting point it had to be assessed whether the acts of the specific defendant constituted a significant contribution to or the aiding and abetting of the crime.[67]

The fact that the activity was planned, based on a clear distribution of work and the duties of the administrators were specifically designed to maintain a high rate of availability of new material and increasingly efficient distribution of all available material (improving torrent files), satisfied the court in determining that the acts of the level 5 and 6 administrators were essential for the continued copyright infringements occurring on the network.[68] They had access to and knowledge of which works were popular and newly made available, and they were aware of their own role in the efficient operation of the network. Like the Court of Appeal, the Supreme Court found that the acts of the level 4 administrators did not constitute a significant contribution but instead satisfied the elements of aiding and abetting.

This case was not about criminal punishment since the petty offence carries a maximum penalty of a fine. The main issue on appeal was the amount of compensation for each of the defendants. The punitive elements built into the concept of compensation are unique to copyright[69] law in Finland. Finnish tort law caps damages to actual damages, which can be adjusted. The concept of reasonableness in tort law is thus severely strained to master the gap between tort law and intellectual property law. In essence compensation amounts to statutory damages, also a concept that is foreign to Finnish law. Statutory damages are normally used to cap actual damages in Finland.

The right to compensation[70] for the unlawful use of a copyrighted work does not require proof of intent or criminal negligence or of the defendant having received economic gain from the crime.[71] The right holder is entitled to reasonable compensation for the use of copyrighted works. Since the level 4 administrators were not criminally liable *for using* the works, only aiding in the use by others, they were not required to pay compensation. Even if the level 4 administrators were also ordinary users of the network, such use did not incur criminal liability nor could it influence the assessment of whether compensation should be paid.[72] Thus, the Supreme Court relieved these defendants of the duty to pay compensation that the lower courts had issued.

The level 5 and 6 administrators were jointly liable to pay compensation.[73] Their individual share of the compensation was however capped at 10 % of the total amount of compensation. One defendant that had been an administrator for a shorter period than the others was responsible for a smaller share.[74] The starting point for calculating the compensation is the licensing fee for the lawful use of the work. The purchase price is problematic as a basis for calculations since it includes value added tax and other unrelated costs that are not attributable to the use of the

67 KKO 2010:47, judgment of 30 June 2010, at 17 and 18.
68 KKO 2010:47, judgment of 30 June 2010, at 19.
69 The same provision is duplicated into all intellectual property laws but has been applied mainly in copyright cases.
70 *hyvitys* Tekijänoikeuslaki (8.7.1961/404) 57 §; See also P-L. Haarmann, *Tekijänoikeus ja lähioikeudet* (Talentum, 2005).
71 KKO 2010:47, judgment of 30 June 2010, at 24.
72 KKO 2010:48, judgment of 30 June 2010 and KKO 2010:47, judgment of 30 June 2010, at 27.
73 KKO 2010:47, judgment of 30 June 2010, at 25.
74 KKO 2010:47, judgment of 30 June 2010, at 41.

work.[75] According to settled case law, it is often not reasonable to order the payment of compensation equal to the amount of normal licensing fees.[76] Thus, the punitive element built into the concept of compensation is quite limited by the compensation culture in Finnish law.[77] The amount of compensation must be based on the court's assessment as well as on the special circumstances of the case and not, e.g. on the number of copies made, the purchase price of a legal copy or the normal licensing fee for a legal use.

The intent and premeditation, the efficiency of the network in effecting actual sales and harming the right holder had a bearing on the court's assessment in that the compensation must be substantial. However, the structure of the network did tempt users to copy works that may have remained unused; and that would not have been ascertained had they not been freely available. The fact that the number of copies made of any individual works was largely outside the control of the defendants also precludes using the full number of works as a basis for the calculation. Thus, the court concluded that the compensation amounts to 15 % of the claimed purchase price for non-musical works, 25 % of the wholesale price for musical works and 50 % of the licensing fee for use of musical works (as it is based on what is paid to artists).[78] Because the Tort Damages Act does not apply to this type of compensation, the amount could not be adjusted[79] based on (general) reasonableness or other grounds.[80]

4 The Right to a Fair Trial and Shifting from Public to Private Enforcement

The *Finnreactor* cases and subsequent court practice relating to blocking access to The Pirate Bay site has cemented criminal liability in Finland for illegal file-sharing of copyrighted works on the internet.[81] In *IFPI v. Elisa* the courts relied on the criminal convictions of administrators in Sweden to apply for a blocking order. Right holders have since pushed for stricter enforcement in *The Pirate Bay* cases.[82] However, a recent amendment of the Copyright Act demands that courts take account of the interests of the direct infringer, users of internet services, the intermediary and the right-holder. While the goal of Sections 60a - 60g of the Copyright Act are to

75 KKO 2010:47, judgment of 30 June 2010, at 34 rejecting earlier case law KKO 1998:91, judgment of 21 August 1998 and KKO 2001:42, judgment of 27 April 2001.

76 KKO 2010:47, judgment of 30 June 2010 and KKO 1989:151, judgment of 21 December 1989; KKO 1999:115, judgment of 1 November 1999 and KKO 2002:101, judgment of 3 December 2002.

77 KKO 2010:47, judgment of 30 June 2010, at 35.

78 The dissenting judge would have ordered higher compensation (20 %, 30 % and 100% respectively based on the number of actual copies).

79 *sovittelu* For further information see M. Hemmo, *Vahingonkorvauksen sovittelu ja moderni korvausoikeus,* (Suomalainen lakimiesyhdistys, 1996).

80 KKO 2010:47, judgment of 30 June 2010, at 42.

81 For a detailed account on intermediary liability for criminal activity see K. Weckström, 'Ch. 9 Preliminary Injunctions Against Intermediaries for Trademark and Copyright Infringement', in K. Weckström (ed.), *Governing Innovation and Expression: New Regimes, Strategies and Techniques* (Turun yliopiston oikeustieteellisen tiedekunnan julkaisusarja A:132, 2013).

82 IFPI Finland representing *EMI Finland OY Ab*, *Sony Music Entertainment Finland Oy*, *Universal Music Oy and Warner Music Finland Oy* brought actions against teleoperators *Elisa*, *Sonera* and *DNA* in Helsinki District Court in order to block internet access to The Pirate Bay site for Finnish subscribers. Judgement of Helsinki District Court No. 11/41552, 26 October 2011 and Judgement of Helsinki Appellate Court (No. 1687) 15 June 2012; See also A. Strowel (ed.), 'Internet Piracy as a Wake-up Call for Copyright Law Makers – Is the Graduated Response a Good Reply?', *WIPO Journal* (2009) 75-86.

secure the right of the copyright owner to efficient remedies against online infringement, this right visibly competes with the rights of others in the new Sections 60c - 60f.[83] Sections 60c - 60f address both minimum requirements for when an injunction may issue, as well as statutory guidance on the division of cost. It is accepted that intermediaries take some part in the fight against rampant copyright infringement. Yet, courts are advised to give more weight to third party interests in all stages of proceedings.[84]

The amendment of the Copyright Act is a result of a decade of copyright debates in the Finnish Parliament.[85] The CopyRight argues for strong protection and advance remedies against intermediaries that are 'effective, proportionate and dissuasive' preventive measures against copyright infringement according to Article 11 of the Enforcement Directive and Article 8 of the INFOSOC Directive.[86] The CopyLeft argues against strong protection and advance narrowly-tailored or no remedies against intermediaries. These arguments rely on Article 9 of the Enforcement Directive, the fundamental rights of internet service providers (freedom of enterprise) and users (freedom of expression) and the prohibition against imposing an obligation to monitor the internet, contrary to Article 15 of the E-Commerce Directive.[87]

Under Section 60a of the Finnish Copyright Act an intermediary is required to release subscriber data relating to an IP address that is frequently using Bittorrent software for sharing torrent files. This obligation applies to a subscriber that 'makes material protected by copyright available to the public to a significant extent'.[88] The 'significance threshold' (merkittävissä määrin) has not been clearly defined.[89] Yet, the Market Court routinely refers to the decisions of the EU Court of Justice in *Promusicae* and *Bonnier*[90], which requires the national court to strike a fair balance between the fundamental rights at stake when interpreting Section 60a of the Finnish Copyright Act.[91] The Market Court has further distinguished between the right to access subscriber data and the right to compensation for copyright infringement

---

83 The courts in The Pirate Bay cases were corrected. They should have balanced competing rights instead of merely considering the copyright owners' interest in efficient remedies.

84 Hallituksen esitys (Government proposal for Amendment to Copyright Act) HE 181/2014, at 32 and 35.

85 The debate is discussed extensively in K. Lindroos, 'Ch. 8 Intermediary Liability for IP Infringement in Finland: Copyright vs. Copyleft—A Series of Legislative Proposals and Decade of Debates', in G. B. Dinwoodie (ed.)*, Secondary Liability of Internet Service Providers* (Berlin: Springer Publishing, 2017).

86 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30 April 2004) and Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society OJ L 167, 22/06/2001, at 10 – 19.

87 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market OJ L 178 , 17/07/2000, at 1 – 16; See also ECHR ruling in Case of *Delfi v. Estonia* 64569/09 ruling of (Grand Chamber) 16 June 2015 confirming that Article 15 of the E-Commerce Directive represents a primary source of law for all members of the European Union and is hence a relevant source for the interpretation of the obligations of governments under ECHR Art. 10 at Section IV.B.

88 Tekijänoikeuslaki 8 July 1961/404 (Copyright Act) unofficial translation of the Copyright Act provided by Finlex available online https://www.finlex.fi/fi/laki/kaannokset/1961/en19610404 (visited 18 January 2018).

89 For a detailed account on the Market Court cases relating to the release of contact information see. K. Weckström, 'Striking the Balance on Liability and Access to Contact Information when Service Is Used to distribute Copyrighted Digital Content Striking the Balance on Liability and Access to Contact Information when Service Is Used to distribute Copyrighted Digital Content', in T. Pihlajarinne et. al (eds.), *Online Content Distribution* (Edward Elgar Publishing forthcoming, 2018).

90 Case C275/06 *Promusicae* [2008] ECR I 271, judgment of (Grand Chamber) 29 January 2008; Case 461/10 Bonnier Audio, judgment of (Third Chamber) 19 April 2012.

91 Markkinaoikeus (Market Court) (hereinafter:MAO) judgment of 4 July 2016, (MAO 419/16); MAO 423/16, judgment of 7 July 2016; MAO 424/16, judgment of 7 July 2016; MAO 425/16, judgment of 7 July 2016; MAO 55/17, judgment of 7 February 2017.

under Section 57 §. The copyright owner may access contact information relating to the user or subscriber of an IP address that is identified as sharing torrent files, but it does not entail access to all subscriptions of that user.[92] Furthermore, the right holder must prove that the subscriber is the likely sharer of files in order to have the right to compensation. Thus, a subscription in itself is not enough for a finding of copyright infringement.

It may be worth noting that the shift from criminal to private enforcement may make a difference for the assessment. In the *Finnreactor* cases there was clear evidence of acts of infringement. The defence rested on a lack of knowledge of the illegal nature of the act. Criminal liability exists both for one's own acts of infringement for file sharing[93] as well as acts contributing to the infringement of others.[94] In contrast, one is not responsible for the criminal acts of other users merely on the basis of one's subscription or ownership of the technical equipment.[95] In private enforcement the right holder must offer proof that the defendant has committed copyright infringement.

Recent cases before the Market Court have included intricate technical evidence. While one case was dismissed due to the lack of proof that the defendant had engaged in file sharing, it is evident that merely raising some doubt is not sufficient to avoid liability.[96] The right holder needs to offer credible evidence that the defendant committed acts of copyright infringement. This entails evidence that removes other possible culprits when the particular acts occurred and places the defendant at the scene of the crime. The mere possibility that someone else may have accessed the defendant's computer or network is an insufficient defence.[97] Instead, the defendant needs to offer credible evidence in rebuttal relating to others committing the act of infringement. The Court denied compensation when the defendant presented evidence showing that he was outside the network range when the infringing acts occurred.[98] The Court awarded compensation when the defendants denied having committed acts of infringement without offering credible or plausible evidence to that effect.[99]

Plaintiff need not eliminate reasonable doubt as in criminal prosecution. Similarly, the court has discretion to weigh evidence without favouring the defendant according to the principle of *in dubio pro reo*. This distinction may seem of lesser importance since the amount of compensation awarded for infringement is calculated in the same way. The right to a fair trial includes a presumption of innocence in all trials. Finnish criminal sanctions are lenient by international standards. However, private enforcement standards in intellectual property cases are on a par with European and international enforcement. Thus, relying on private enforcement may be beneficial for right holders since compensation may serve the same deterrent function regardless of the public or private nature of proceedings.

The right to a fair trial does not extend to a preference for public or more lenient sanctions. Once infringement is established, the defendant is required to pay reason-

92 MAO 55/17, judgment of 7 February 2017 citing Lakivaliokunnanlausunto (Statement by Parliament Committee) LaVL 5/2005 (hereinafter: LaVL) which introduced Section 60a into the Copyright Act. See also MAO 565/17, judgment of 15 September, at 95.
93 KKO 2010:48, judgment of 30 June 2010.
94 KKO 2010:47, judgment of 30 June 2010.
95 LaVL 2005/5.
96 MAO 55/17, judgment of 7 February 2017; MAO 419/16, judgment of 4 July 2016 and MAO 565/17, judgment of 15 September 2017.
97 MAO 419/16, judgment of 4 July 2016 and MAO 565/17, judgment of 15 September 2017.
98 MAO 55/17, judgment of 7 February 2017.
99 MAO 419/16, judgment of 4 July 2016 and MAO 565/17, judgment of 15 September 2017.

able compensation.[100] Costs for public prosecution in criminal trials is born by the state. In civil trials the *Loser pays* principle applies. Thus, while the defendant is not required to confess to a crime that s/he did not commit, it may be costly to raise the bar for the plaintiff to present evidence to prove guilt.[101] In all cases, the defence was unsuccessful in diminishing the award for litigation costs and attorney fees, since more hours and technical experts were required to disprove unsubstantiated claims by the defendant.[102]

5 Conclusion

This chapter has discussed some fundamental rights conflicts relating to the public and private policing of criminal activity on the internet. The examples illustrate the complex framework for interpretation regardless of context for the fundamental rights conflict. This chapter reveals general legal principles underlying practical resolution of fundamental rights conflicts. The ECHR commits the continent to a constitutionalism that rests on democratic decision-making. The government must act to secure remedies for violations of rights online. Yet, government actors may be limited in prosecuting crime online based on the respecting of the offender's fundamental rights. The European Union further recognizes fundamental rights as they result from the constitutional traditions common to the Member States. Rights should be interpreted in harmony with those traditions. Member States must favour an interpretation of national or EU law that prevents a conflict and strikes a fair balance between the fundamental rights interests at stake. This is true for all actors of government. However, in private enforcement, where a private right stands against a private right, the public interest does not weigh in unless the law provides specific parameters for fundamental rights balancing. The right to effective judicial protection applies to both parties involved.[103] Yet, private citizens should be aware of the context of pursuing a fundamental rights claim in court. Private redress is not a vehicle for changing the law in Europe.

100 Section 57 of the Copyright Act.
101 MAO 565/17, judgment of 15 September 2017.
102 MAO 419/16, judgment of 4 July 2016 and MAO 565/17, judgment of 15 September 2017.
103 Case of *K.U. v. Finland*, 2872/02, judgment of (Fourth Section) 2 December 2008 and respectively Case C275/06 *Promusicae* [2008] ECR I-271, judgment of (Grand Chamber) 29 January 2008, at 61.

NEW CHALLENGES POSED BY CYBERCRIME IN INTERNATIONAL POLICE COOPERATION

Giulio Calcara

1 Introduction

The Internet has changed modern society mostly for the better and affected the way we live.[1] However, such a change has come at a steep price.[2] Most everyday activities are transposed to the web, making the cyberspace a fertile ground for criminal activities. Traditional criminal offences are enabled by the Internet and allowed to proliferate at an alarming rate. Furthermore, previously inconceivable forms of high-tech crimes have emerged in recent years. Both traditional offences committed through the Internet and new high-tech crimes are designated under the umbrella term cybercrime.[3]

Cybercrime has become a crime area that encompasses several criminal offences with specific traits: they constantly change in parallel with the advancement of technology[4], they are transnational in nature[5], and they often grant anonymity to criminal offenders.[6] Due to the aforementioned factors, constant cooperation among police services of different countries has become a necessity in order to tackle criminal activities in cyberspace.[7] Such cooperation usually takes place on a bilateral basis or through international police cooperation entities such as INTERPOL or Europol.[8]

This specific contribution analyses the role of the major international police cooperation entities in the fight against cybercrime from the standpoint of a European Union member state and uses Finland as an example. It does this by focusing on the challenges they encounter from the legal perspective during their activities. Primarily, the differences in the substantive criminal law and the procedural laws of the various countries remain a hindrance in the process of enabling cooperation.[9] As a consequence, these differences may give rise to several legal issues during operations.

1 J. Clough, *Principles of Cybercrime* (Cambridge: Cambridge University Press, 2015).
2 *Ibid.*
3 INTERPOL, *Cybercrime*, available online at https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (visited 13 October 2017).
4 R. Broadhurst, 'Developments in the global law enforcement of cyber-crime', 29(3) *Policing: An International Journal of Police Strategies & Management* (2006) 408-433.
5 R. McCusker, 'Transnational organised cyber crime: distinguishing threat from reality', 46(4-5) *Crime, law and social change* (2006) 257-273.
6 H.L. Armstrong and P.J. Forde, 'Internet anonymity practices in computer crime', 11(5) *Information management & computer security* (2003) 209-215.
7 G. Calcara, 'Role of INTERPOL and Europol in the Fight against Cybercrime, with Particular Reference to the Sexual Exploitation of Children Online and Child Pornography', 7 *Masaryk University Journal of Law and Technology* (2013) 19-33.
8 T.T. Vendius, 'Proactive Undercover Policing and Sexual Crimes against Children on the Internet', 2 *European Review of Organised Crime* (2015) 6-24.
9 J. Clough, *supra* note 1, at 24.

In conclusion, the contribution provides proposals on how new approaches in the field of police cooperation can be devised and what issues should be addressed.

2 The Nature and the Complexity of Cybercrime

Cybercrime may take place in many different forms and countries, and international entities have different ways of defining cybercrime. On a general and intuitive level, it is possible to make reference to cybercrime when a computer or a technological device is the target of a specific criminal offence or is the medium by which criminal conduct has taken place. Nevertheless, in certain cases it is possible to make reference to cybercrime when relevant information is stored inside a computer or a technological device that relates to a criminal offence that has happened outside cyberspace.[10]

One thing about cybercrime is certain: it has not yet been tackled effectively and it is a crime area that deserves to become a priority in the agenda of governments around the globe. As Alexander Seger, the head of Cybercrime Division of the Council of Europe, states:

> Most cybercrime is never reported, particularly in the private sector where organisations tend to stay clear of criminal justice. A large share of reported cybercrime is never investigated, few of the offences that are investigated result in prosecutions and, of those, few end up with court rulings.[11]

This information needs to be connected with the fact that an increase in cybercrime around the world is foreseen,[12] which will directly affect EU citizens. There are a number of reasons for why such an increase has occurred. First, countries that were previously lacking proper Internet connections are now starting to catch up, thus providing avenues for new potential cybercriminals. At the same time, EU countries are relying more and more on the Internet for offering services, and citizens are turning to the web for carrying out multiple activities such as home banking for economic transactions.[13] As such, the picture is rather gloomy, and it is vital for police services around the globe to be aware of the changes in crime trends and to develop strategies to work more efficiently in a complex and evermore digitalized society.[14]

10 A. Seger, 'Evidence in the Cloud and the Rule of Law in Cyberspace', 7 *Europe's World*, December (2015) available online at http://europesworld.org/?p=10119.

11 *Ibid.*

12 Internet Organised Crime Threat Assessment (IOCTA), *THREAT ASSESSMENT ON INTERNET FACILITATED ORGANISED CRIME* (2011), available online at https://www.europol.europa.eu/activities-services/main-reports/threat-assessment-internet-facilitated-organised-crime-iocta-2011 (visited 13 October 2017).

13 *Ibid.*

14 W. Ph. Stol and J. Jansen, *Cybercrime and the Police* (The Hague: Eleven international publishing, 2013).

2.1 Defining Cybercrime

Cybercrime is in constant evolution.[15] Due to the advancements in technology, virtually all forms of criminal activity might at some point involve a cyber aspect.[16]

Given the fact that cybercrime has become a constant unwelcomed presence in the modern world, it is somehow surprising that there is still a lack of consensus on what the term cybercrime actually should entail.[17] Likewise, in relevant literature and legal documents several other terms are used to define a large group of criminal offences with similar traits and with a technological or digital background, such as Internet crime, high-tech crime and computer-related crime.

All these terms have however something in common. They tend to refer to at least one of the following three different categories, most often the first two:[18] cyber-dependent crime, cyber-enabled crime or computer-supported crime.

The first category, cyber-dependent crime, refers to those offences that base their existence on the use of a computer or technological device as a way of carrying out criminal conduct,[19] such as hacking, which remains the most notorious criminal offence of this category.[20]

The second category, cyber-enabled crime, refers to offences that used to take place outside the cyberspace and now have the potential of emigrating to the cyberspace. The use of a technological device has the sole purpose of amplifying the effects of the criminal conduct on a wider scale. A classic example is the spreading of child pornography through the Internet.[21] The use of cyberspace allows a capillary distribution of illegal content, which in past decades was simply not conceivable. The traditional offence, once it transforms itself into a cyber-enabled crime, may also slightly change its nature and characteristics, becoming more complex and structured.[22] The object of the criminal offence might be the same, but the conduct can be drastically different.

The third category, computer-supported crime, refers to those criminal offences that are not necessarily directly connected to the use of any technological device or to cyberspace. However, some details of a traditional criminal offence might leave traces on a computer device or in cyberspace. For instance, when information, which

15 Internet Organised Crime Threat Assessment (IOCTA), *INTERNET ORGANISED CRIME THREAT ASSESSMENT* (2017), available online at https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf (visited 13 October 2017).

16 M. Aiken, C. Mc Mahon, C. Haughton, L. O'Neill and E. O'Carroll, 'A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online', 11(4) *Contemporary Social Science* (2016) 373-391, at 385; C. Mc Mahon, 'All crime is cybercrime', An Garda Síochána Analyst Service Annual Conference. Dublin, Ireland 13 December 2013; A. Kasper, 'Legal aspects of cybersecurity in emerging technologies: Smart grids and big data' in T. Kerikmäe (ed.) *Regulating eTechnologies in the European Union: Normative Realities and Trends* (Tallinn: Springer International Publishing, 2014) 189-216, at 191.

17 S. Gordon and R. Ford, 'On the definition and classification of cybercrime', 2(1) *Journal in Computer Virology* (2006) 13-20.

18 J. Clough, *supra* note 1, at 9.

19 *Ibid*; For the purpose of this contribution, it is interesting to note that the same category is denominated by INTERPOL with the name of *'advanced cybercrime'* (or high-tech crime), and it makes reference in particular to *'sophisticated attacks against computer hardware and software'*. The difference is subtle, yet relevant. In the first instance the focus of the category seems to rest on the conduct, in the second on the object of the criminal offence. See: INTERPOL, *Cybercrime*, *supra* note 3.

20 J. Clough, *supra* note 1; M. Mc Guire and S. Dowling *Cybercrime: a review of the evidence, Research Report 75, Summary of key findings and implications*, Home Office, October 2013, available online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf (visited 13 October 2017), at 5.

21 J. Clough, *supra* note 1.

22 INTERPOL, *Cybercrime*, *supra* note 3.

makes a reference to a crime that has happened outside cyberspace, is stored in some sort of digital archive.[23]

2.2 Cybercrime Legislation

Unsurprisingly, there is a wide array of diverse legal approaches to the issues posed by cybercrime. The root of such a diversity lies in the fact that certain criminal offences may deal with specific interests that are viewed differently among countries.[24] Particularly revealing is how a universally condemned criminal offence such as child pornography is regulated in different ways.[25]

Another phenomenon that causes large discrepancies among legislations, more specifically in regard to criminal procedure areas, is the fact that certain countries seek to take advantage of evolving technologies by providing havens for cyber-criminals.[26] This can be achieved by granting *de facto* impunity to offenders through the creation of unreasonably strict privacy regulations for Internet users with the sole purpose of assuring almost complete anonymity and/or by not properly regulating the issues posed by different kinds of content hosted online inside the country.[27]

Among the constellation of different domestic criminal laws, there are international instruments created with the purpose of building a common legal framework among countries in the area of cybercrime, such as the Council of Europe Convention on Cybercrime, known simply as Convention on Cybercrime or Budapest Convention on Cybercrime. It is a binding international convention that addresses cybercrime from the points of view of substantive criminal law, various aspects of procedural criminal law, and international cooperation.[28] One of the aspirations behind the creation of the Budapest Convention was to devise a legal instrument with a global reach,[29] thus the convention ensures the possibility of signatories outside of the members of the Council.[30] Among members outside of the Council of Europe to join the convention, there are countries such as the United States, Canada, Japan, Australia, and Israel.

The Convention has brought a significant contribution to the harmonization of laws among its parties. In its Chapter I Section 1 it focuses on four groups of offences and provides a basic definition for them: 'Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems; Title 2 – Computer-related offences; Title 3 – Content-related offences; Title 4 – Offences related to infringements of copyright and related rights'.[31]

An extension to the Convention came in 2003 with the, 'Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.'

However, the convention does not address or regulate cybersecurity, which is perhaps one of the most concerning and growing areas of cybercrime. Cyber threats

23 J. Clough, *supra* note 1.
24 *Ibid.*
25 Y. Akdeniz, *Internet child pornography and the law: national and international responses* (New York: Routledge, 2016).
26 J.N. Geltzer, 'The new pirates of the Caribbean: How data havens can provide safe harbours on the Internet beyond governmental reach', 10 *Southwestern Journal of Law & Trade in the Americas* (2003) 433-453.
27 *Ibid.*
28 A. Savin, *EU Internet law* (2dn ed., Cheltenham: Edward Elgar Publishing, 2017).
29 J. Clough, *supra* note 1.
30 *Ibid.*
31 Art. 2-10 of the Convention on Cybercrime.

to national security, which are said to include economic espionage, crime, cyber war, and cyber terrorism, have indeed been left out by the Convention.[32]

Chapter I Section 2 of the Convention focuses on procedural measures concerning powers and procedures for criminal investigations and proceedings such as: 'Title 2 – Expedited preservation of stored computer data; Title 3 – Production order; Title 4 – Search and seizure of stored computer data; Title 5 – Real-time collection of computer data'. According to Article 14(2) the provisions involving the procedural measure have to be implemented by the parties not only on the criminal offences addressed in Section 1 but also on 'other criminal offences committed by means of a computer system' and 'the collection of evidence in electronic form of a criminal offence'. This significantly extends the scope of the procedural measures, which have to be applied among the parties well beyond the limited range of offences dealt within the Convention.[33]

Chapter III of the Convention focuses on international cooperation. Article 23 states that the parties shall cooperate with each other. While the provision is generic in nature, it signals the need for cooperation in the field of cybercrime. Finally, the same chapter deals also with provisions in matters of extradition and mutual assistance among parties.[34]

Another international instrument, which aims to tackle the cybercrime phenomenon, even though only partially and in specific circumstances, is the United Nations (UN) Convention Against Transnational Organized Crime.[35] As the name suggests, the UN Convention does not focus directly on cybercrime issues but deals with the fight against transnational organized crime. It is, however, relevant to notice that the UN Convention provides avenues for judicial and police cooperation whenever serious crime is conducted by criminal networks on a transnational level. In many instances cybercrime tends to satisfy the definition of "serious crime" given by the UN Convention, and furthermore it is frequently transnational in nature and carried out by organized criminal groups.[36] The UN Convention is a truly international instrument with a lot of potential to have an impact with 189 state parties. However, it has yet to be implemented consistently.[37] In recent times there have been calls to use the tools of the UN Convention in specific regard to the fight against cybercrime.[38]

32 E. Gruodytė and M. Bilius, 'Investigating Cybercrimes: Theoretical and Practical Issues', in T. Kerikmäe (ed.) *Regulating eTechnologies in the European Union: Normative Realities and Trends* (Tallinn: Springer International Publishing, 2014) 217-249. For more information on the issues of Cyber threats to national security, see: J. Nye, *Cyberpower* Harvard Kennedy School: Belfer Center for Science and International Affairs, 10 May 2010, available online at: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf (visited 13 October 2017).

33 Savin, *supra* note 28.

34 Art. 24-35.

35 Broadhurst, *supra* note 4.

36 *Ibid.*

37 UN News Centre, *UN anti-crime chief urges better use of Convention against Transnational Organized Crime*, 17 October 2016, available online at: http://www.un.org/apps/news/story.asp?NewsID=55321#.WXXuEhiw3EY (visited 13 October 2017).

38 *ibid.*

3 The Role of International Police Cooperation in the Fight Against Cybercrime

It is a complex task to identify all the major challenges that police services might encounter whenever they are involved in the fight against cybercrime. First of all, police services are constrained by one of the key principles in criminal justice, which is the principle of territoriality.[39] This principle is particularly relevant in cybercrime operations, which are more often than not, transnational in nature. In this regard, a challenge afflicting police services and forces is how to collect evidence outside their own state.[40]

Due to the transnational nature of the cybercrime phenomenon, systematically implementing a sole domestic approach is bound to fail. That leaves police cooperation as the most viable solution. However, even international police cooperation presents challenges and limitations. First and foremost, international police cooperation depends on the willingness of police services, and ultimately governments of countries, to actively engage in cooperation.[41] Additionally, even where there is a will to cooperate, several legal issues might arise and hamper the cooperation processes. The endemic and everlasting obstacles to police cooperation are the differences in domestic criminal laws, such as a lack of common definitions in regard to criminal offences, and the differences in criminal procedures. As Gerspacher points out, irreconcilable differences in national laws and criminal justice systems among countries may not be the only obstacles to engaging in international police cooperation. Other underlying aspects that are at the basis of a fruitful international police cooperation are 'positive relations between states on issues of ideology, varying practices, human rights and civil liberties.'[42] Indeed, when those are lacking it might be difficult to carry out systematic cooperation in the long run.

There are several ways of activating cooperation among police forces or services of different countries, and naturally that remains true also in the field of cybercrime.

Cooperation can be based on a bilateral (both formal or informal) agreement, or it can be conducted through a multilateral structure of cooperation[43] like police cooperation organizations and agencies.

While bilateral forms of cooperation are still commonly used,[44] with cybercrime becoming more and more a global issue, police organizations and agencies can and should obtain a central role. Countries are called to realize the need and urgency of a systematic multilateral approach in the fight against transnational crime.[45]

In this section, the focus is on the study of the origin, the role, and the *modus operandi* of two of the most influential actors in international policing and the fight against cybercrime: INTERPOL and Europol. Furthermore, the origin and the devel-

39 *Ibid.*
40 Gruodytė and Bilius, *supra* note 32.
41 M. Stalcup, 'Interpol and the Emergence of Global Policing', in W. Garriott (ed.), *Policing and contemporary governance: The anthropology of police in practice* (New York: Palgrave Macmillan, 2013) 231-261.
42 N. Gerspacher, 'The history of international police cooperation: a 150-year evolution in trends and approaches', *9*(1-2) *Global crime* (2008) 169-184, at 178.
43 L. Guille, 'Police and judicial cooperation in Europe: bilateral versus multilateral cooperation' in F. Lemieux (ed.), *International Police Cooperation: Emerging Issues, Theory and Practice Devon* (New York: Routledge 2010) 25-41.
44 *Ibid.*
45 Gerspacher, *supra* note 42.

opment of the brand new Joint Cybercrime Action Taskforce (J-CAT) is presented and discussed.

3.1 Interpol

INTERPOL has a long history. The forerunner of INTERPOL was founded in 1923 under the name International Criminal Police Commission (ICPC). At the time, the ICPC was only a small, mainly Western-European regional entity.[46] The function of the ICPC was limited in promoting informal collaboration between the police forces of different states. The modalities of creation of the commission were unconventional,[47] since no legal treaty was signed between states.[48] The lack of a treaty instituting the commission was an intentional choice of the delegates. The scope was to leave the commission exempted from legal restraints or obligations.[49] Such a choice would eventually come back to haunt INTERPOL in the following years[50] and place the organization in an uncomfortable limbo of uncertainty in regard to its own legal status for a significant amount of time.[51] Furthermore, for an extensive period of time INTERPOL still maintained a reputation of being a high-profile "officers' club".[52]

The International Criminal Police Organization (ICPO-INTERPOL), simply known as INTERPOL, was formally born in 1956 with the adoption of the Constitution.[53] Nowadays, INTERPOL looks substantially different from the time of the ICPC. It is officially an international organization dedicated to international police cooperation. However, no treaty has yet been signed.[54] The organization now consists of 192 member countries.[55] The organization's Constitution remains its main legal document, which sets the organization's aims in the Article 2 as follows:

> (1) To ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the "Universal Declaration of Human Rights";
> (2) To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes.

The definition of what is "ordinary law crime" has shifted and expanded throughout the years. For example, in the past the organization did not deal with terrorism relat-

46 M. Deflem, 'International Police Cooperation —History of', in R.A. Wright and J.M. Miller (eds), *The Encyclopedia of Criminology* (New York: Routledge. 2005) 795-798.
47 M. Fooner, *Interpol: Issues in World Crime and International Criminal Justice*, (New York: Plenum Press, 1989).
48 M. Deflem, 'Interpol', in P.N. Stearns (ed.), *The Oxford Encyclopedia of the Modern World*, (New York: Oxford University Press, 2008), 198-199.
49 *Ibid.*
50 Fooner, *supra* note 47.
51 J. Sheptycki, 'The Accountability of Transnational Policing Institutions: The Strange Case of Interpol', 19 (1) *Canadian Journal of Law and Society* (2004) 107-134; R.S.J. Martha, 'Challenging Acts of INTERPOL in Domestic Courts', in A. Reinisch (ed.), *Challenging Acts of International Organizations Before National Courts* (New York: Oxford University Press, 2010) 206-238.
52 Gerspacher, *supra* note 42.
53 INTERPOL, *History*, available online at https://www.interpol.int/About-INTERPOL/History (visited 13 October 2017).
54 *Ibid.*
55 See INTERPOL website, available online at https://www.interpol.int (visited 13 October 2017).

ed offences.[56] Today, INTERPOL is involved in supporting cooperation in more than 18 different crime areas.[57]

The structure of the organization is set in the Article 5 of the Constitution. INTERPOL consists of the following bodies: the General Assembly, the Executive Committee, the General Secretariat, the National Central Bureaus (NCB), the Advisers, and the Commission for the Control of Files. Of these, the General Secretariat and the NCBs are the main bodies that focus on international police cooperation activities.

Among its various functions, the General Secretariat works mainly as the central hub for circulating information and police and judicial documents among the members of the organization.[58] The NCBs serve as connection points among member countries and INTERPOL.[59] On a more specific level, each member country has the obligation of building a NCB which '… shall ensure liaison with: (a) The various departments in the country; (b) Those bodies in other countries serving as National Central Bureaus; (c) The Organization's General Secretariat.'[60]

The traditional *modus operandi* of INTERPOL consists mainly of the International Notices System[61] and the Diffusions System.[62] Both these systems are methods used by INTERPOL to circulate information or documents among the organization and member countries.

Notices are regulated by the INTERPOL´s Rules on the Processing of Data (RPD) and are published by the General Secretariat of INTERPOL after a request by NCBs or other authorized entities. They are divided into different colours, with each one signalling a different kind of information, alert or request done for the purpose of police cooperation. The Red Notice is probably the most well-known. A Red Notice is published in order to locate and arrest an individual 'with a view to extradition or similar lawful action'.[63] Other types of notices are the Blue, Green, Yellow, Black, Orange and Purple Notice.[64]

Diffusions are another method for circulating documents and for requesting cooperation. On the whole, they might have the same purposes as the notices but are regulated differently by the RPD. They are less formal and can be sent directly from

56 That however is not true anymore. INTERPOL is one of the key actors in counterterrorism activities and operations. See: M. Deflem, *The Policing of Terrorism: Organizational and Global Perspectives* (New York: Routledge, 2010), at 113; M. Deflem, 'Global rule of law or global rule of law enforcement? International police cooperation and counterterrorism', 603(1) *The annals of the American academy of political and social science* (2006) 240-251.

57 D. Higgins and R. White, 'Collaboration at the Front Line: INTERPOL and NGOs in the same NEST' in G. Pink and R. White (eds.), *Environmental Crime and Collaborative State Intervention* (Palgrave Macmillan, 2016) 101-116, at 103.

58 Art. 26 of INTERPOL´s Constitution.

59 D.L. Sheehan, 'INTERPOL: An International Perspective on Police Training and Development', in M.R. Haberfeld, Curtis A. Clarke and Dale L. Sheehan (eds), *Police Organization and Training: Innovations in Research and Practice* (New York: Springer, 2012) 169-178, at 170.

60 Art. 32 of INTERPOL´s Constitution.

61 INTERPOL, *International Notices system*, available online at www.interpol.int/en/News-and-media/Publications/Fact-sheets/International-Notices-system/ (visited 13 October 2017).

62 *Ibid.*

63 *Ibid.*

64 *Ibid.*

an NCB to one or more NCBs.[65] All notices and diffusions are circulated through the information system of INTERPOL, which works around the clock.[66]

It is crucial to notice that INTERPOL aids cooperation between police services and forces of 192 different countries. As a consequence, cooperation may be carried out among police services of countries with extremely different legal traditions and systems.[67] Due to the large number of operations and member countries, INTERPOL´s information system has been misused several times; sometimes for negligence, but at times intentionally.[68] Several legal concerns have been caused by the Red Notice system.[69] Nevertheless, INTERPOL remains the main truly international asset in the fight against cybercrime due to its global reach and high functionality.

In regard to cybercrime, INTERPOL has developed a plan for the years 2016-2020 called 'Global Cybercrime Strategy'.[70] The strategy mainly focuses on building the capacity of the member countries of INTERPOL in the fight against cybercrime. Interestingly enough, in one of INTERPOL´s so-called *action streams* the organization refers to the need for promoting legislative harmonization among member countries.[71] Furthermore, INTERPOL seems to propose itself as an international coordinator of transnational and international police investigations through researching trends in crime, facilitating investigations in cyber-attacks, aiding the collection and the preservation of digital evidence, and in locating the perpetrators of cybercrime.[72]

In recent years, INTERPOL has built a Global Complex for Innovation (IGCI) in Singapore. This centre aims to be involved in the fight against cybercrime with a view on enhancing digital security and promoting proactive research.[73]

3.2 Europol and the European Cybercrime Centre (EC3)

Similar to INTERPOL, Europol has changed significantly over the years, especially considering its short existence.[74] Several legal documents have characterized the genesis of Europol and changed its legal status.

65 *Ibid.*

66 The Information system has two tools to circulate information: the I-24/7 and the I-link. See: INTERPOL, *Data exchange*, available online at https://www.interpol.int/INTERPOL-expertise/Data-exchange/I-24-7 (visited 13 October 2017); M. Deflem and S. McDonough, 'International Law Enforcement Organizations' in S. Kethineni (ed.), *Comparative and International Policing, Justice, and Transnational Crime* (Durham, North Carolina: Carolina Academic Press, 2010) 79-102, at 89-93.

67 M. Savino, 'Global Administrative Law Meets "Soft" Powers: The Uncomfortable Case of INTERPOL Red Notices', 43 *New York University Journal of International Law and Politics* (2010) 263-336, at 276.

68 See for example the extensive report on the matter by NGO Fair Trials. Fair Trials, *Strengthening respect for human rights, strengthening INTERPOL*, November 2013, available online at www.fairtrials.org/wp-content/uploads/Strengthening-respect-for-human-rights-strengthening-INTERPOL4.pdf (visited 13 October 2017).

69 C.R. Both, 'International Police Force or Tool for Harassment of Human Rights Defenders and Political Adversaries: Interpol's Rift with the Human Rights Community', 8 *ILSA Journal of International & Comparative Law* (2001) 358-360.

70 Interpol, *Global Cybercrime Strategy – Summary*, February 2017, available online at https://www.interpol.int/content/download/34471/452245/version/4/file/007-04_Summary_CYBER_Strategy_2017_01_EN%20LR.pdf (visited 13 October 2017).

71 *Ibid.*

72 *Ibid.*

73 *Ibid.*

74 S. Rozée, C. Kaunert and S. Léonard, 'Is Europol a Comprehensive Policing Actor?' 14(3) *Perspectives on European Politics and Society* (2013) 372-387.

The origin of the European Police Office (Europol) dates back to 1992 when it was cited in the Maastricht Treaty.[75] The Convention of Europol was written in 1995, and Europol started to be operative only four years later.[76]

In 2009 the "COUNCIL DECISION of 6 April 2009 establishing the European Police Office (Europol)" replaced the Europol Convention. The Council was then replaced in 2016 by the new Europol Regulation called: 'REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA'

Europol is not an international organization like INTERPOL, but an EU Agency, which has its headquarter in the Hague.[77] In time Europol has become more and more used as a means of cooperation by the member states of the EU[78] and has a budget of 85 million euros.[79] Each member state possesses a Europol National Unit (ENU). The ENUs represent the connection points between Europol and the police service or force of each member state.[80] Furthermore, in order to expand its functional range of action, Europol has signed strategic agreements with third states and organizations, including INTERPOL.[81]

The role of Europol is one of collecting, analysing, and sharing information among member states. Furthermore, it provides assistance to the police services of member states and helps coordinate transnational and international operations.[82]

One of the characteristic features of Europol's *modus operandi* is the use of the so-called Europol Analysis Projects.[83] These are thematic projects that are situated inside Europol's information processing system called Europol Analysis System.[84] The projects focus on specific crime areas and serve various purposes.[85] In particular, they serve as tools for facilitating the work of Europol specialists and EU law enforcement entities in the analysis of information related to different crime areas, in the coordination of meetings, in the circulation of expertise, and the sharing of information in the support of police operations and in the processes of judicial cooperation.[86] Like INTERPOL, Europol cannot start investigations on its own,[87] but it has the significant capacity of urging national police services to do so.[88]

In recent years, as a reaction to the ever-growing expansion of the cybercrime phenomenon, a European Cybercrime Centre (EC3) has been created inside Eu-

75 S. Miettinen, *Criminal law and policy in the European Union*, Vol. 3 (New York: Routledge, 2013).
76 Rozée et al., *supra* note 74.
77 *Ibid.*
78 M. Bergström and A. J. Cornell (eds), *European police and criminal law co-operation* (Oxford: Hart Publishing, 2014).
79 *Ibid.*
80 Rozée et al., *supra* note 74.
81 *Ibid.*
82 *Ibid.*
83 EUROPOL, *EUROPOL ANALYSIS PROJECTS*, available online at https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects (visited 13 October 2017).
84 *Ibid.*
85 *Ibid.*
86 *Ibid.*
87 *Ibid.*
88 A. J. Cornell, 'EU Police Cooperation Post-Lisbon', in M. Bergström and A. J. Cornell (eds), *European police and criminal law co-operation* (Oxford: Hart Publishing, 2014) 147-163, at 154.

ropol.[89] The European Commission proposed the creation of such a centre back in 2010, but only in 2012 did it issue a communication titled 'COMMUNICATION

FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre'.[90]

The centre was developed in 2013[91] and became fully operative in 2014.[92] EC3 has already proven to be effective, producing an impressive number of results in areas such as the dark net, the deep web and the underground economy.[93]

EC3 has a three-level functional structure.[94] First, there is an operational level. On the operational level EC3 has three main focuses. The first focus is on cybercrimes that are committed in the context of organized crime, and specifically the ones which involve significant economic gain for the offenders with particular reference to online and payment fraud. The second focus is on cybercrimes that cause serious harm to the victims, including the sexual exploitation of children. The third focus is on cyber-attacks directed at the EU's information systems.[95]

Second, there is the forensic expertise level. With its forensic teams, EC3 is involved in providing operational support to EU member states and conducting researching activities.[96]

Lastly, there is the strategy level. There are two strategic teams inside the EC3.[97] One of them is involved in 'strategic analysis', 'formulation of policy' and 'legislative measures and the development of standardised training'.[98] The other one has an outreach function, which is particularly significant in the fight against cybercrime.[99] The outreach function refers to the capacity of Europol in cooperating with other entities such as other law enforcement services outside EU, the academic community, the private sector and non-law enforcement organizations.[100] There is something worth noticing about this matter. A unique phenomenon that sprung out of the latter function is the role of EC3 in negotiating directly with countries and international organizations outside the EU. The EC3 is *de facto* partly bypassing the traditional roles of national governments and diplomatic channels.[101] The legal basis for entertaining negotiations with third countries and international organizations lies nowadays in the new Europol Regulation Article 23.

According to Art. 23, Europol, and as a consequence the EC3, can essentially make various kinds of agreements with third countries for operational cooperation as long as no personal data is exchanged in the operations. Where the transfer of personal data becomes a necessity, which is often the case in a policing operation,

89 A. Barrinha and H. Carrapiço , 'The EU's emerging security actorness in cyber space: Quo vadis?', in L. Chappell, J. Mawdsley and P. Petrov, eds. *The EU, Strategy and Security Policy: Regional and Strategic Challenges* (New York: Routledge, 2016) 104-118, at 109.

90 T.T. Vendius, 'Europol's Cybercrime Centre (EC3), its Agreements with Third Parties and the Growing Role of Law Enforcement on the European Security Scene', 3 *European Journal of Policing Studies* (2015) 151-161.

91 EUROPOL, EUROP*EAN CYBERCRIME CENTRE - EC3*, available online at https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (visited 13 October 2017).

92 Barrinha and Carrapiço, *supra* note 89.

93 Vendius, *supra* note 90.

94 EUROPOL, *EC3*, *supra* note 91.

95 *Ibid.*

96 *Ibid.*

97 *Ibid.*

98 *Ibid.*

99 Vendius, *supra* note 90.

100 *Ibid.*

101 *Ibid.*

Art. 25 sets a number of alternative conditions as a basis for this. The first condition is that there is a so-called *adequacy decision* made by the Commission in order to ascertain that 'the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection'.[102] The second one is the presence of a previous international agreement between the EU and that specific entity 'adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals'.[103] The last one is the presence of a previous cooperation agreement between Europol and that entity made in accordance with the previous legal framework governing Europol.[104] Art. 25 paragraph 5 authorizes the Executive Director to allow the exchange of personal data on a case by case basis with the previous mentioned entities in specific matters of urgency in police cooperation activities.

Allowing Europol to entertain relationships with third countries and international organizations and entities assures the relevance of the European agency in the fight against cybercrime also outside the EU's borders. This is necessary for Europol to be truly effective, as a large number of threats to EU citizens might come from outside the EU. On the other hand, the fact that Europol and the EC3 are bypassing diplomatic channels and governments in securing international agreements might be a source of controversial outcomes. These agreements are not under supervision of any member state's parliament or European parliament, and as a consequence they are not subjected to any sort of democratic process.[105]

3.3 The Joint Cybercrime Action Taskforce (J-CAT)

Soon after the birth of EC3, a brand-new tool for cooperation was developed: the Joint Cybercrime Action Taskforce, which is currently known by the acronym of J-CAT.[106]

The taskforce has been operative since September 2014, inside the EC3,[107] and has the function of supporting the fight against cybercrime both inside and outside EU borders.[108] According to Europol's website the main objective of the taskforce is as follows: 'to drive intelligence-led, coordinated action against key cybercrime threats and targets by facilitating the joint identification, prioritisation, preparation and initiation of cross-border investigations and operations by its partners.'

Among the crime areas in which the taskforce is involved are high-tech crimes, online fraud and the sexual exploitation of children online. Furthermore, it is specialized in countering activities in cyberspace which have the purpose of facilitating the commission of cybercrimes.[109]

Members of the taskforce are a group of liaison officers from the police services and forces of Australia, Austria, Canada, Colombia, France, Germany, Italy, the Netherlands, Spain, the United Kingdom and both the FBI and the Secret Ser-

102 Art. 25, 1. (a) of the REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

103 Art. 25, 1. (b).

104 Art. 25, 1. (c).

105 Vendius, *supra* note 90.

106 Aiken et al., *supra* note 16.

107 *Ibid.*

108 EUROPOL, *JOINT CYBERCRIME ACTION TASKFORCE (J-CAT)*, available online at https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce (visited 13 October 2017).

109 *Ibid.*

vice of the United States of America.[110] Additionally, the EC3 is officially one of the members and acts as the Secretariat of the taskforce.[111]

J-CAT's *modus operandi* is quite simple. J-CAT's board receives proposals on various cases. It then decides which operations should be conducted, and a country is chosen to be in charge for every specific investigation.[112]

While the J-CAT remains located inside the EC3, and the EC3 operates as the main supporter, the taskforce is not officially a part of Europol and it is a separate EU taskforce.[113] This has been a calculated strategic choice. The country in charge of the investigation for the J-CAT remains free to make agreements with third countries in order to conduct the operations, while having at its disposal the resources of the EC3.[114] Since the taskforce is not part of Europol, the country in charge is free to discard the conditions, requirements and legal safeguards of the new Europol regulation for making agreements with third countries. It would be possible, for example, to cooperate with Russia, which does not possess and probably will not possess in the immediate future an agreement to cooperate with Europol, even though a significant number of cybercrimes originate from that country.[115] It is possible to identify the creation of the J-CAT as a solution to circumvent part of legal frameworks that have been limiting the functions of Europol.

Indeed, the taskforce has proven to be truly effective and has carried out a significant number of successful operations in the crime areas that it pursues.[116] It is interesting to notice that the J-CAT has been successful in its own mission by bypassing the legal limitations that govern Europol and the EC3, while still being lead by the EC3 and situated inside the EC3.

Some questions arise. In particular, it is necessary to address the issue of whether it would have been perhaps more reasonable to devise a different legal framework for Europol since it might be afflicted by too strong limitations. Secondly, it is necessary to evaluate whether circumnavigating *de facto* Europol regulations, while using a taskforce governed by Europol, is the right solution to overcome legal impediments. The last consideration becomes even more controversial when the country in charge's police service of an investigation by the J-CAT is one of the EU member states.

4 Specific Challenges Posed by Cybercrime in International Police Cooperation

In the fight against cybercrime, international police organizations and agencies may stumble across various obstacles. There are legal and practical issues which are common in cooperation activities. The legal issues originate mainly from the lack of harmonization of criminal law and judicial procedures, whereas the practical challenges are rooted in the three main characteristics of cybercrime, which have been previous-

110 *Ibid.*
111 T. Reitano, T. Oerting, and M. Hunter, 'Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce', 2(2) *The European Review of Organised Crime* (2015) 142-154.
112 *Ibid.*
113 *Ibid.*
114 *Ibid.*
115 *Ibid.*
116 EUROPOL, *(J-CAT)*, *supra* note 108.

ly identified: cybercrime evolves in parallel with the advancement of technology,[117] it is transnational in nature[118] and it often grants anonymity to the offenders.[119]

The continuous evolution of cybercrime puts both domestic and international police services in an uncomfortable position.[120] There is a constant need for capacity building, and in regard to this international organizations, such as INTERPOL, are called to play a key role. An endless effort is needed, and more resources should be put into researching new criminal trends, the advancement of technology and its implications on cybercrime, and in training police services. The training and the building of national police services' knowhow is paramount in order to facilitate a fruitful international cooperation. However, in this field problems persist still at the European level. Particularly revealing is that the EC3 has been addressing the issue with concerned tones, underlying the fact that at the present time 'no EU-wide standards for training and certification exist yet, and the alignment of existing programmes within the Member States and broader implementation of the current EU-wide initiatives is necessary.'[121]

The fact that cybercrimes are transnational in nature and grant anonymity to offenders has various ramifications. For example, there is a common challenge afflicting national police services or forces whenever they are investigating transnational cybercrime: how to collect evidence outside their own state territory.[122]

For instance, Finland, which is a party to the Convention on Cybercrime, only has the possibility to access extraterritorial stored computer data located in another country that is a party of the Convention if there is explicit consent from the relevant authority or if it is publicly available according to Article 32 of the Convention on Cybercrime.[123] When both requirements are not met, there arises the need to proceed with traditional requests of mutual legal assistance.[124]

Such requests are the traditional *modus operandi* when the computer data is located in a country that is not party to the Convention.

The process of mutual legal assistance is often time consuming, and thus, inefficient. In cybercrime investigations there is a need for speed and secrecy due to the risk of data being deleted from cyberspace.[125]

Sometimes computer data are stored in clouds in unidentifiable countries.[126] Obtaining evidence becomes more problematic when it is difficult to understand to which country the request for mutual legal assistance should be directed to.[127]

As Gruodytė and Bilius suggest, INTERPOL and Europol could be used to systematically channel requests of assistance, but realistically in the process of gathering evidence they might not be useful due to the enormous number of cybercrimes: 'Europol or Interpol cybercrime centres could provide help, but knowing the amount

117 Broadhurst, *supra* note 4.
118 McCusker, *supra* note 5.
119 Armstrong and Forde, *supra* note 6.
120 IOCTA, 2017, *supra* note 15.
121 *Ibid.*
122 Gruodytė and Bilius, *supra* note 32.
123 *Ibid.*
124 *Ibid.*
125 Council of Europe, *Explanatory Report to the Convention on Cybercrime*, European Treaty Series - No. 185, 23 November 2001, available online at https://rm.coe.int/16800cce5b (visited 13 October 2017), at 133.
126 A. Seger, 'Evidence in the Cloud and the Rule of Law in Cyberspace', *Europe's World*, 7 December 2015, available online at http://europesworld.org/?p=10119 (visited 10 October 2017).
127 T. De Zan and S. Autolitano, *EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace*, Documenti Istituto Affari Internazionali IAI, November 2016, available online at http://www.iai.it/sites/default/files/iai1617.pdf (visited 13 October 2017), at 11.

of cybercrime such way seems unsatisfactory when fighting against cybercrime.'[128] Furthermore, the quantity of cybercrime is so vast that relying constantly on this method could ultimately engulf these systems of cooperation.[129]

It is relevant to point out that accessing stored computer data is regulated differently in the various countries. It is ultimately an issue of obtaining data and data retention. One of the key issues that should be addressed by organizations and agencies promoting cooperation is how to make sure that evidence is preserved and obtainable in cyberspace.[130]

It is relevant to point out that some EU countries possess appropriate laws to make sure that police services can obtain relevant data from Internet service providers (ISPs) in the context of policing activities, while others do not. The situation used to be different, when an EU directive used to harmonize the laws among member states, which allowed ease in cross-border investigations inside the EU.[131] However, in 2014 this directive was deemed invalid by the Court of Justice of the European Union (CJEU), making the situation complex once again from the transnational policing point of view.[132]

Finally, differences in methods of investigating among police services pose significant challenges during cross-border investigations of cybercrime.[133] More specifically, the challenges arise from what is deemed to be legal in the context of pre-trial investigations. This is not only a global issue but also a regional one; there are major differences in investigation techniques present in the EU.[134] For example, certain states allow proactive investigations in the form of undercover operations, while in other countries that is possible only in very limited circumstances. On this, Vendius suggests: 'national police forces are left in a legal vacuum on the EU level when it comes to actual investigations and the use of special investigative measures as there are no common rules regulating how far police forces can go.'[135] This is particularly relevant in child pornography cases, where allowing the use of cross-border covert operations could have a significant impact.[136]

5 Sharpening the Tools of International Police Cooperation

As it has been shown throughout this contribution, in order to increase the impact of international policing organizations and agencies involved in the field of cybercrime, there is a need to increase the harmonization of laws.[137] While progress has

128 Gruodytė and Bilius, *supra* note 32, at 243.

129 Indicative of the need for policing agencies to concentrate efforts only in limited areas is the fact that the operational level of the EC3 focuses only on cybercrimes that give significant economic gain to the offenders, cause serious harm to the victims or on cyber-attacks directed at the information systems of the EU. See: EUROPOL, *EC3*, *supra* note 91.

130 It is certainly encouraging that Jurgen Stock, INTERPOL´s current Secretary General, has recently addressed the issue in an interview.
The interview is available online at http://www.channelnewsasia.com/news/catch-up-tv/conversation-with/jurgen-stock-9030928 (visited 13 October 2017).

131 IOCTA, 2017, *supra* note 15.

132 ECLI:EU:C:2014:238 (case C-293/12).

133 Vendius, *Proactive Undercover*, *supra* note 2.

134 *Ibid.*

135 *Ibid.*

136 *Ibid.*

137 M. Edelbacher, 'Austrian international police cooperation' in D.J. Koenig, and D.K. Das (eds), *International Police Cooperation: A World Perspective* (Oxford: Lexington Books, 2001) 121-128.

been made on the regional EU level with the Convention of Cybercrime, on the global level there are still significant differences among the legislative approaches to cybercrime.

The process of harmonization should not be limited only to the level of substantive criminal law, but it should be extended also to the field of criminal procedure and methods of investigation. The development of a legal framework that allows common investigative rules on the international level would be the optimal solution.[138] At this time, this suggestion seems more utopian than realistic.

As INTERPOL´s Secretary General has pointed out, there is a need to approach the fight against cybercrime in a more holistic manner.[139] International police cooperation agencies and organizations should not only be focused on the exchange of information among national police services, but they should try, at least to an extent, to reach out to the targets of cybercrime such as the private sector[140] and individuals.

Reaching out to the private sector offers countless possibilities. It facilitates a shift in the realm of police cooperation activities: operations can transform from being only reactive in nature, to embracing also proactive elements. This has also been pointed out in the new Report of Europol 'Internet Organised Crime Threat Assessment (IOCTA) 2017', where there is a specific reference on how, 'Public-private partnerships are also key in enabling a more pro-active and agile approach to combatting cybercrime.'[141] Furthermore, it is possible to see potential benefits in increasing cooperation among social media platforms and both national and international police agencies.[142] Social media is both a fertile ground for cybercrime and for information relating to cybercrime. Moreover, social media is populated with citizens who might possess information on cybercrime which they may not be aware of and that they would be more than willing to share. Recently, Europol has started to exploit this phenomenon. For example, an impressive online campaign has been organized by Europol to identify objects present in the areas of child abuse and child pornography material.[143] Several objects have been taken out from the material and have been presented on Europol's websites and shared with Facebook and Twitter users. Recognizing the provenience of the objects helps police to understand where the abuse took place and which country has jurisdiction. In the campaign 'Stop Child Abuse', a note reads: ' … The objects are all taken from the background of an image with sexually explicit material involving minors. For all images below, every other investigative avenue has already been examined.'[144] This means that the campaign has been used in *ultima ratio*, after regular investigations have become stale. Questions should at this point be made as to whether it could be possible to expand this method and to devise a more systematic form of community policing on the international level in order to help international policing agencies in collecting data.[145] Resorting to the public in this way would not be done as a last resort, but instead

138 EUROPOL, *(J-CAT)*, *supra* note 108.

139 http://www.channelnewsasia.com/news/catch-up-tv/conversation-with/jurgen-stock-9030928

140 INTERPOL, *Coordinating efforts to better combat cybercrime focus of INTERPOL working group*, available online at https://www.interpol.int/News-and-media/News/2016/N2016-040 (visited 13 October 2017).

141 IOCTA, 2017, *supra* note 15.

142 G. Calcara, M. Forss, M.J. Tolvanen, and P. Sund, 'The Finnish Internet Police (Nettipoliisi): towards the development of a real cyber police', 6(2) *European Journal of Law and Technology* (2015); D. Trottier, *Social media as surveillance: Rethinking visibility in a converging world*. (Uppsala: Routledge, 2016).

143 EUROPOL, *STOP CHILD ABUSE – TRACE AN OBJECT*, available online at https://www.europol.europa.eu/stopchildabuse (visited 13 October 2017).

144 *Ibid.*

145 Calcara, *supra* note 142.

it would be part of a concerted effort in bringing down cybercrime.[146] In time, and through constant interaction with the public, increasing international police organizations' and agencies' role in community policing could also serve as a way of incrementing trust among the general public.

The issue of trust, or the lack of it, is a real one. It is possible to consider that up to 90 % of cybercrime goes unreported worldwide.[147] Unfortunately, at this time a vicious circle is in place: the less crime is reported, the less police services can successfully fight cybercrime, which ultimately leads to the general public not trusting police. What is certain is that in order for the police to be successful, crime needs to be reported.[148] An increase in reports can surely start a positive domino effect at the national and ultimately international level.

Additionally, there is a need to assure that evidence of cybercrime is preserved. Victims have to be instructed by police how to do this, and thus again there is a need for building trust and to incentivate the reporting of crime.[149]

Finally, crime prevention needs to become a collective and global responsibility. The general lack of interest and awareness in cybercrime ultimately benefits criminal groups. Indeed, offenders tend to prey on the victims' lack of knowledge. Simple acts performed by citizens, such as regularly updating systems and technological devices, can already have a significant impact in the prevention of cybercrime.[150]

6 Conclusion

Cybercrime is a serious threat to citizens around the globe. It is a transnational phenomenon that is impossible to tackle on the domestic level. It requires constant, concerted and systematic cooperation among police services around the globe.

The work of international policing agencies should be aided by national governments. In particular, there is a need for the harmonization of laws and procedures on the regional and international level in order for cooperation to be successful and continuous in time.

Furthermore, domestic and international police agencies should try to reach out to the private sector and individuals in order to increase their functionality, and ultimately, their chances of success in the fight against cybercrime.

146 *Ibid.*
147 http://www.channelnewsasia.com/news/catch-up-tv/conversation-with/jurgen-stock-9030928
148 *Ibid.*
149 *Ibid.*
150 *Ibid.*

FUTURE SCENARIOS IN LAW AND TECHNOLOGY

NEUROSCIENCE AND JUDICIAL PROCEEDINGS, PAST AND PRESENT. WHAT WILL THE FUTURE BRING?

Jordi Nieva Fenoll

1 Introduction: A Recent, though not Novel, Reality

[1]Benjamin Libet[2] was not the first to publish studies on neuroscience; in fact, others had done so much earlier. Nor can it be said that his conclusions play any role in the study of the law today, despite the uproar he recently generated.[3] To summarize them in a sentence, albeit imprecisely, 'brains do not commit crimes; people commit crimes'.[4] Let us examine this piece by piece.[5]

To begin with, the electroencephalogram (EEG) has long been present in the courts of law. This technology, which dates from the early twentieth century,[6] is probably the most basic of neuroscientific techniques, but it is also the most widespread, both in medicine and law, and is widely known in society in general. The EEG is used to diagnose brain death in hospitals, in addition to detecting the famous—and

1 The present work was made possible to a large extent thanks to the materials and facilities made available to me at the Max Planck Institute in Luxembourg. I would like to extend my gratitude to the personnel, especially the director, Burkhard Hess, for his support.

2 Libet, Benjamin, *Mind Time*, Frankfurt 2005. Libet, B. /Freeman, A. /Sutherland, K., *The Volitional Brain: Towards a Neuroscience of Free Will*, Thorverton 1999.

3 See, for all, Vv.Aa. (Demetrio Crespo dir.). *Neurociencias y Derecho Penal*, Buenos Aires 2013. Rubia, Francisco J., *El fantasma de la libertad*, Barcelona 2009. Aavv (Taruffo/Nieva dirs.), *Neurociencia y proceso judicial*, Madrid 2013. Díaz Arana, Andrés Felipe, *Las mentes libres en el Derecho penal*, InDret 1/2016, pp. 1 et seq. Pérez Manzano, Mercedes, *Fundamento y fines del Derecho penal. Una revisión a la luz de las aportaciones de la neurociencia*, InDret 2/2011, pp. 1 et seq. Feijoo Sánchez, Bernardo, *Derecho Penal y Neurociencias. ¿Una relación tormentosa?*, InDret 2/2011, pp. 1 et seq. Pardo, Michael S. / Patterson, Dennis, *Fundamentos filosóficos del Derecho y la neurociencia*, InDret 2/2011, pp. 1 et seq.

4 'Brains do not commit crimes; people commit crimes'. Morse, Stephen J., 'Brain Overclaim Syndrome and Criminal Responsibility: A Diagnostic Note', *Ohio State Journal of Criminal Law*, vol. 3, p. 397.

5 For uses of neuroscience in the process in general, see Jones, Owen D., 'Seven Ways Neuroscience Aids Law', *Neurosciences and the Human Person: New Perspectives on Human Activities*, 2013, pp. 1 et seq., Jones, Owen D. /Wagner, Anthony D. /Faigman, David L. /Raichle, Marcus E., "Neuroscientists in court", *14 Nature Reviews Neuroscience 730 (2013)*, pp. 730 et seq.

6 Berger, Hans, ‚Über das Elektrenkephalogramm des Menschen', *Archiv für Psychiatrie und Nervenkrankheiten*, 1929, 87, pp. 527 et seq.

hotly debated[7] P-300 wave.[8] Other techniques, among many, are computed tomography (CT), positron emission tomography (PET) and single-photon emission computed tomography (SPECT).[9] At the same time, magnetic resonance imaging (MRI) is increasingly being used in courts of law, although it remains infrequent.[10] It is used to demonstrate the presence of anatomical damage such as damage to the frontal lobe,[11] which affects the capacity to empathize and thus affects a person's ability to assess the unlawfulness of their actions or even to avoid such action. These are two important aspects that we will examine next. For some time they have played a part in legal proceedings; more often than not to diagnose mental illness rather than to predict the future behaviour of a criminal.

The latest innovation to be widely used is functional magnetic resonance imaging (fMRI),[12] which, like magnetoencephalography (MEG),[13] has the great advantage of not requiring the injection of substances into the body or exposure to ionizing radiation. Instead, this technique simply uses the blood oxygen level-dependent (BOLD) signal to detect changes in oxygenation in the blood by means of the magnetic differences that provoke these changes. Despite it being the most accurate technique due to its high spatial resolution, although the temporal resolution of the MEG is superior,[14] it has had some bad luck, so to speak, because it is occasionally being used in the courts simply to influence gullible judges.[15] When analyzing the physiology of the brain, it is the test that, in visual terms, impresses most. By illuminating parts of the brain a correlation between the illumination of the brain section with an action carried out by the individual may be interpreted. It may also be used, for example, to achieve greater precision in the surgical extraction of brain tumors. But this imagery has also been used in an attempt to interpret certain cognitive functions, and thanks to the striking quality of the imagery these attempts have unfortunately resulted in the rather frequent publication of articles that are unacceptable from a scientific point of view.

All this will be subject to analysis in the present work, not from a technical point of view, since I am poorly qualified to do so, but rather from a legal and also purely logical perspective. I will address some of the claims being made about the neuroscientific potential of these techniques, which not only belong to the realm of science fiction but also are quite impossible. This is not due to a lack of scientific advancement; there are quite simply some aspects of the mind that are unreachable. The brain is not a flash drive that we can connect to a computer and read. The brain is neither a storage device nor a processor. It is an organ of the body that is not to be compared with anything else that we may be familiar with today. This is not because there is nothing more efficient than the brain, as sectorally speaking there is,

7 See also Greely, 'Neuroscience, mindreading, and the Courts: the example of pain', cit. p. 191.

8 For an explanation of the development of this test in Spain, see Libano Beristain, Arantza, 'Neurociencia y proceso penal', Justicia n. 2, 2015, pp. 246 et seq.

9 Moya Albiol, Luis / Romero Martínez, Ángel, 'El cerebro violento', Moya Albiol (ed.), *Neurocriminología*, Madrid 2015, pp. 43 et seq.

10 Shen, Francis X., 'Neuroscience, Mental Privacy, and the Law', *Harvard Journal of Law & Public Policy*, vol. 36, 2, 2013, p. 660.

11 This happened in 2010 in the case of John McCluskey, who escaped the death penalty thanks to neuroscientific analysis. See Denno, Deborah W., 'The myth of the double-edged sword: an empirical study of neuroscience evidence in criminal cases', *Boston College Law Review*, vol. 56, 2015, p. 494.

12 See FILIPI, Massimo, *fMRI techniques and protocols*, Totowa NJ 2009.

13 Neuronal activity is detected through the magnetic fields that produce the electrical currents of the brain.

14 Gosseries, O. / Demertzi A. / Noirhomme Q. / Tshibanda J. / Boly M. / Op De Beeck M. / Hustinx R. / Maquet P. / Salmon E. / Moonen G. / Luxen A. / Laureys S. / De Tiège X., 'Que mesure la neuro-imagerie fonctionnelle: IRMf, TEP & MEG'**,** *Revue médicale of Liège*, 2008 May-Jun; 63 (5-6), 231-7.

15 See Moreno, Joelle Anne, 'The Future of Neuroimaged Lie Detection and the Law', *Akron Law Review*, vol. 42, 3, pp. 731 and 736.

as for example was demonstrated when Deep Blue defeated, not uncontroversially, Kasparov. Simply put, the brain may only be compared with another brain because it is a concept in itself, completely self-referential, like the liver or the stomach. It is important not to forget this and wander off into the land of fantasy literature.

2 The Legal Uses of Neuroscience

Most of the legal uses of neuroscience have been mentioned in the previous section. Each will now be explored separately. Although these uses may produce relevant results, none are particularly spectacular, at least for legal purposes.

2.1 The Detection of Behaviour-modifying Brain Alterations

In criminal proceedings, and in civil proceedings to assess disability, it is very important that the mental capacities of the defendant are determined. Criminal proceedings decide on a possible exemption, or mitigation, of criminal responsibility, for example, as the result of a psychological anomaly or alteration that prevents the defendant from comprehending the unlawfulness of the action or acting in compliance with said comprehension. This is equally applied in civil proceedings to determine disability in order to define physical or psychological disease or disability that prevents the individual from having full control of their actions.

To this end, cognitive interviews are carried out to allow the psychologist or psychiatrist to evaluate the mental state of the person. Neuroscience, however, has opened a complementary field to that evaluation, particularly with the MRI, when useful.[16] It has been used in several cases to detect certain brain injuries that have decisively undermined the behaviour of a person and hence show that they were not responsible for their actions.[17] This has also been taken into account to assess the maturity of an individual for this purpose, something that has saved people in the US from the death penalty in cases in which the crime was committed when they were under age; the adolescent brain is not considered by law to be sufficiently developed to fully understand the unlawfulness of an act.[18] Moreover, Denno identified in the US a small but noteworthy number of proceedings, 800 from 1992 to 2012, in which neuroscientific test results were presented as evidence, with 64.25 % of these cases centring on assessing the presence of brain damage in the defendant.[19] Some US courts, following the Strickland[20] line of jurisprudence regarding the adequate performance of the defence, have required lawyers to make use of neuroscientific evidence to defend the innocence of their clients.[21]

16 See Vv.Aa. (Moya Albiol, Luis (dir.)) *Neurocriminología. Psicobiología de la violencia*, Madrid 2015.
17 Bandes, Susan A., 'The promise and Pitfalls of Neuroscience for Criminal Law and Procedure', *Ohio State Journal of Criminal Law*, vol. 8, 2010, p. 120. Moreno, Joelle Anne, 'The Future of Neuroimaged Lie Detection and the Law', *Akron Law Review*, vol. 42, 3, p. 723.
18 See Roper v. Simmons, 543 U.S. 551 (2005). See also Graham v. Florida, 560 U.S. 48 (2010). On this subject see Pozuelo Pérez, Laura, 'Sobre la responsabilidad penal de un cerebro adolescente', InDret 2/2015, pp. 1 et seq.
19 Denno, Deborah W., 'The myth', cit. p. 501.
20 Strickland v. Washington, 466 U.S. (1984).
21 Denno, Deborah W., 'The myth', cit. p. 507 et seq.

2.2 The Prognosis of Danger

Just as the mental state of a person is evaluated when a crime occurs, so the same techniques can be used to form a prognosis about future behaviour.[22]

Assessing the future behaviour of the defendant has always been an ordeal for judges and psychologists,[23] not only when carrying out sentencing, especially if they are to be released, but also in terms of controversial measures such as permanent surveillance following completion of the sentence. But perhaps the scenario in which the most is at stake is in interim relief; the court must evaluate the possibility of flight risk, the destruction of evidence and repeat offending in the defendant.[24] Under normal circumstances, neuroscientific analysis may only be used to assess the risk of repeat offending, and only partly

The answer to the question *will they do it again* has a rather elusive answer. MRIs may only evaluate possible personality patterns, like the psychological interview, but they cannot guarantee that the individual will repeat the offence or not. However, since MRIs are easily accessible and not very invasive, they may be more frequently used in the future as advances are made in this field of research.

2.3 The Detection of Lies

The area in which neuroscientific study has attracted the most attention, and the most criticism.[25] is the evaluation of deception. Certain terms like *brain fingerprinting*, which uses the EEG in particular, have sparked panic, probably unnecessarily,[26] in an area of the doctrine on the possibility of a thought reading machine.

However, the potential of this technology is, to date, not only limited but in all truth extremely finite, if not wholly speculative. The EEG has been used, for example, to track the P-300 wave, so named because it is produced approximately 300 milliseconds after the subject is exposed to the stimulus. Meanwhile, the fMRI is used, as explained previously, to reveal changes in oxygenation in the cerebral blood

22 Bandes, Susan A., 'The promise and Pitfalls of Neuroscience for Criminal Law and Procedure', *Ohio State Journal of Criminal Law*, vol. 8, 2010, p. 120. Denno, 'The myth', cit. p. 526.

23 Andrés Pueyo, Antonio / López, S. / Álvarez, E., *Valoración del riesgo de violencia contra la pareja por medio de la SARA*, Papeles del Psicólogo, 2008. Vol. 29(1), pp. 107 et seq. Redondo Illescas, Santiago / Andrés Pueyo, Antonio, *Predicción de la violencia: entre la peligrosidad y la valoración del riesgo de violencia*, both in Papeles del psicólogo: revista del Colegio Oficial de Psicólogos, Vol. 28, Nº. 3, 2007 (issue dedicated to predicting violence), pp. 157 et seq. Andrés Pueyo, Antonio, *Delincuencia sexual, trastorno mental y peligrosidad*, Revista Española de Medicina Lega, 2013, 39, 1-2. Craig, L. / Beech, Ar., *Towards a guide to best practice in conducting actuarial risk assessments with sex offenders*. Aggress Violent Behav. 2010, 15:278-93. Fazel S. / YU, R. *Psychotic disorders and repeat offending: systematic review and meta-analysis*, Schizophr Bull. 2011, 37:800-10. Redondo Illescas, Santiago / Pérez, Meritxell / Martínez, Marian, 'El riesgo de reincidencia en agresores sexuales: investigación básica y valoración mediante el SVR-20', *Papeles del Psicólogo*, n. 3, vol. 28, 2007. Andrés Pueyo, Antonio / Arbach, Karin, 'Valoración del riesgo de violencia en enfermos mentales con el HCR-20', *Papeles del Psicólogo*, n. 3, vol. 28, 2007.

24 On this subject, see Nieva Fenoll, Jordi, *Hacia una nueva configuración de la tutela cautelar*, Diario La Ley, n. 8773, 1-6-2016.

25 See Kahn, 'Neuroscience, Sincerity and the Law', *Bergen Journal of Criminal Law and Criminal Justice*, 2/2015, p. 204. See also Hakun, J. G. / Ruparel, K. / Seelig, D. / Busch, E. / Loughead, J. W. / Gur, R. C. / Langleben, D. D., *Towards clinical trials of lie detection with fMRI*, Social Neuroscience, 2009, Vol. 4, 6, pp. 518 et seq. Moreno, 'The Future of Neuroimaged Lie Detection and the Law', cit. p. 732. Schleim, Stephan, ‚Bildgebende Verfahren der Neurowissenschaften in der strafrechtlichen Ermittlungspraxis: Eine kritische Perspektive auf den Stand der Forschung' in Stephan Barton, Ralf Kölbel, Michael Lindemann (dir.), *Wider die wildwüchsige Entwicklung des Ermittlungsverfahrens*, p. 370.

26 See Morse, Stephen J., 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', *Marquette Law Review*, 2015, vol. 99, pp. 39 et seq. Shen, 'Neuroscience, Mental Privacy, and the Law', cit. p. 656.

flow and consequent magnetism to observe what areas are activated when the subject thinks or performs an action.

The P-300 wave is used to identify an electrical reaction in the brain when observing an already familiar event, place or person. Apparently, if the subject observes something that they have already seen and retained in their memory (this second point is crucial), the P-300 wave would be activated so that even if the subject states they know nothing about the observed item, their brain would reveal that they do in fact remember it.

When explained in these terms, it certainly seems like a spectacular technique, but this frequently used explanation is riddled with shortcomings that we will examine below. For now, it suffices to say that the research on this wave is far from satisfactory in terms of scientific rigor.

The results obtained from fMRI is even more impressive. This method could, theoretically, assess whether a subject is lying consciously. It represents a kind of twenty-first century polygraph, although it may share the outcome of the original[27] (which was disappointing for reasons that will soon be explained), most likely due to the same fundamental reasons, which result in a double error. In the first place, lying does not always cause a physical reaction. It is a fundamental error to think that the cognitive effort of lying is always more intense than that of telling the truth.[28] On many occasions the exact opposite can occur when one tries to make a truthful declaration without overlooking anything, taking care not to generate false memories

It is important not to forget that the concept of a lie, like that of the truth, is philosophical. The objective notion of a lie does not really exist, and despite being clearly counterintuitive, this conditions the entire study. This does not mean that during proceedings the 'truth' cannot be reached or that one cannot conclude that what a witness says is a 'lie'. The point is that neither notion is precise enough to undergo direct experimental observation. We shall look at this later.

In any case, rushed publication[29] of the results of these tests and, in particular, the sale of such tests by companies to defendants desperately seeking acquittal, have unfortunately and unjustly placed this field of knowledge within the edges of pseudoscience.[30] Certainly, neither the EEG nor the fMRI has anything to do with parapsychology or alternative therapies, but the manipulation of the conclusions of these tests can irretrievably lead scientists down that same path.

3 The Technical Limitations of Neuroscience

As previously stated, the limitations of all the techniques described herein are unquestionable. Faced with the euphoria unleashed by certain scholars, some have be-

27 In short, total frustration. See National Research Council (Committee to Review the Scientific Evidence on the Polygraph), *The polygraph and lie detection*, 2003, pp. 212 et seq.

28 On this subject, see Burgoon, Judee K., 'When is Deceptive Message Production More Effortful than Truth-Telling? A Baker's Dozen of Moderators', *Front. Psychol.*, 24-12-2015. http://journal.frontiersin.org/article/10.3389/fpsyg.2015.01965/full. Sporer, Siegfried L., 'Deception and Cognitive Load: Expanding Our Horizon with a Working Memory Model', *Front. Psychol.*, 7-4-2016. http://journal.frontiersin.org/article/10.3389/fpsyg.2016.00420/full. See also Pardo, 'Neuroscience Evidence, Legal Culture, and Criminal Procedure', cit. pp. 312, 314. Schleim, Bildgebende Verfahren der Neurowissenschaften in der strafrechtlichen Ermittlungspraxis: Eine kritische Perspektive auf den Stand der Forschung', p. 387.

29 See the enormous increase in publications on the law and neuroscience since 2006 in Jones/Wagner/Faigman/Raichle, 'Neuroscientists in court', cit. p. 731.

30 See some of the titles listed by Moore, Adam D. *Privacy, Neuroscience, and Neuro-Surveillance*, 13-4-2016 pp. 1-2. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2764437.

gun to speak ironically of Brain Overclaim Syndrome[31] (BOS) as a disease these scholars may be afflicted with. In any event, studies on brain damage detected by MRI have successfully reported scientific evidence—especially in legal proceedings—that demonstrate that an individual's behaviour was conditioned by these injuries.

In the US in particular, pathology in the frontal lobe freed McCluskey from the death penalty after he was found guilty of shooting a couple in a car and then setting it on fire.[32] An EEG that revealed brain damage[33] helped another defendant (Nelson), who also escaped the death penalty after stabbing his wife 60 times as well as killing his stepchildren.[34] Both of these cases are from 2010. Brain damage caused by substance abuse, psychotic illness, accidents, tumors or blows to the head[35] have also been presented as mitigating circumstances by using some of the diagnostic techniques mentioned above. In 2012, a defendant named Simmons,[36] accused of stabbing and injury resulting in the death of a woman, underwent a PET scan that revealed brain injury originating from a near-drowning in childhood and substance abuse in adolescence, which had resulted in a functional deficit in the thalamus, an area of the brain related to the self-control of violent and inappropriate behaviours. In the Bryan case, a SPECT image was used to demonstrate brain damage that was significant enough to have caused paranoid disorder in the defendant.[37] MRIs have also been used to measure the size, shape and density of the brain structures in Alzheimer patients, for example.[38]

But as Morse states in a breakthrough analysis, 'We have no idea how the brain enables the mind or how action is possible'.[39] Furthermore, the analyses involving fMRIs are still too recent to reach any conclusions on the legal consequences of their use.[40] What is more, as Morse himself affirms, no criminal has the built-in cunning to avoid neurological detection when they commit a crime,[41] and no technique has developed a truly specific marker to detect a psychiatric pathology or even indicate a lack of rationality or self-control in an individual to establish a predisposition to committing a crime; however, this does open the possibility of predicting future behaviour or the current judgement abilities of the person because they are based on the evaluation of the subject at the present time.[42]

One of the reasons for these deficiencies is the difficulty of field study. fMRIs are expensive[43] and slow. In order to have sufficient statistical evidence, one would

31 Morse, 'Brain Overclaim Syndrome and Criminal Responsibility: A Diagnostic Note', cit. pp. 397 et seq. See also Maero, Fabián, 'Cuando las neurociencias engañan' in http://www.psyciencia.com/2016/30/cuando-las-neuroimagenes-enganan-una-entrevista-investigador/?utm_content=bufferf72ab&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer, 30-6-2016.

32 Denno, 'The myth', cit. p. 494.

33 See also, using the same technique, Stankewitz v. Wong, 29-10-2012. http://cdn.ca9.uscourts.gov/datastore/opinions/2012/10/29/10-99001.pdf. Denno, 'The myth', cit. p. 523.

34 Denno, 'The myth', cit. p. 495.

35 Denno, "The myth", cit. p. 504.

36 Denno, "The myth", cit. p. 516. The case has the following reference: Supreme Court of Florida, Eric Simmons v. State of Florida, 18-12-2012. http://www.floridasupremecourt.org/decisions/2012/sc10-2035.pdf.

37 Denno, "The myth", cit. p. 536.

38 Greely, "Neuroscience, mindreading, and the Courts: the example of pain", cit. p. 181.

39 Morse, 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', cit. p. 59.

40 Morse, 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', cit. p. 59.

41 Morse, 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', cit. p. 60.

42 Morse, 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', cit. p. 60, note 48.

43 Approximately $1,000,00 per hour. Greely, 'Neuroscience, mindreading, and the Courts: the example of pain', cit. p. 194.

need a great number of subjects selected at random from different environments. This is something that has not yet been carried out.[44]

One additional difficulty is centred on the problem of the 'ecological validity' of the conclusions. Studies are carried out in a laboratory and not during real–life like events like those that lead to court proceedings, and therefore the results are not contrasted.[45] Ultimately, these analyses do not demonstrate that the activity of a brain region is a suitable marker to indicate provocation or propensity for a certain behaviour, but instead they show that the region may involve diametrically opposed behaviours, such as affection and hatred.[46] Furthermore, there is a problem that nearly always occurs in scientific research. Conclusions are based on comparative statistical, and therefore probabilistic, analysis.[47] This is based on the data derived from the analysis of a group of subjects without knowing to what extent the comparison is really possible, taking into account which area of the brain -is activated in every case.[48] All this would indicate, at least in legal terms, that despite the various inaccuracies we should for now continue to turn to the behavioural analyses of psychologists and psychiatrists, and we should do this without assuming that a cerebral anomaly determines behaviour in cases in which behavioural analysis shows no abnormality in a subject.[49] The same occurs, it would seem, at least for the time being, with the so-called 'neuroscience of pain'[50] and even with the detection of psychotic diseases. The differences in the brains of healthy and mentally ill subjects, while statistically relevant, are too small.[51]

Without a doubt, however, the most controversial technique is lie detection. Although Morse himself is more optimistic with respect to the future, if not to the present, in regard to these techniques,[52] many authors think just the opposite.[53] It has been demonstrated that it is possible to learn to cheat on an fMRI lie detection test.[54] It has even been called, exaggeratedly and perhaps inappropriately, but graphically, 'ordeal by radio waves.[55]

The analysis is based on the possible identification of a superior activity in the prefrontal cortex, the area that many have associated with ethics,[56] when a subject

---

44 Morse, 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', cit. p. 60.
45 Morse, 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', cit. p. 61.
46 Morse, 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', cit. p. 61.
47 SChleim, Bildgebende Verfahren der Neurowissenschaften in der strafrechtlichen Ermittlungspraxis: Eine kritische Perspektive auf den Stand der Forschung', p. 374.
48 Morse, 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', cit. p. 62.
49 Morse, 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', cit. p. 62.
50 Morse, 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', cit. p. 63. See also Greely, Henry T., 'Neuroscience, mindreading, and the Courts: the example of pain', *Journal of Health Care Law & Policy*, vol. 18, 2015, pp. 179 et seq.
51 Morse, 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', cit. p. 66.
52 Morse, 'Criminal Law and Common Sense: An Essay on the Perils and Promise of Neuroscience', cit. p. 71.
53 Kahn, Jonathan, 'Neuroscience, Sincerity and the Law', *Bergen Journal of Criminal Law and Criminal Justice*, vol. 3, 2, 2015, p. 204. Greely, Henry T. /Wagner, Anthony D. *Reference Guide on Neuroscience*, in 'National Research Council (Federal Judicial Center), *Reference Manual of Scientific Evidence*', 3ª ed. Washington D.C. 2011, p. 803. Pardo, Michael S., 'Neuroscience Evidence, Legal Culture, and Criminal Procedure', *American Journal of Criminal Law*, vol. 33, 2006, p. 306.
54 Ganis, Giorgio, Rosenfeld, J. Peter, Meixner, John, Kievit, Rogier A., Schendan, Haline E., *Lying in the scanner: Covert countermeasures disrupt deception detection by functional magnetic resonance imaging*, NeuroImage 55, 2011, pp. 312 et seq.
55 Kahn, 'Neuroscience, Sincerity and the Law', p. 209.
56 Deyoung C. G., Hirsh J. B., Shane M. S., Papademetris X., Rajeevan N., Gray J. R., 'Testing predictions from personality neuroscience'. *Psychological Science*, 2010, 21, 6: pp. 820 et seq. Yang Y. / Raine, A., *'Prefrontal structural and functional brain imaging findings in antisocial, violent, and psychopathic individuals: a meta-analysis', Psychiatry Research*, 2009, 174, 2.

lies.[57] Some studies, more spectacular than promising,[58] have been carried out, including that led by Gallant at the University of Berkeley, which showed different YouTube videos to volunteers while they underwent fMRI scanning. What was surprising was that researchers in a second blind analysis managed to guess with sufficient accuracy which video the volunteer had been watching. It is easy to conclude from such an experience that we may in the future be able to know what a person in a vegetative state imagines,[59] something that theoretically could make communication with these patients possible, but all this is clearly excessive at present.

What is certain is that a subjective mental state cannot be inferred by changes of oxygenation in certain areas of the brain,[60] and in no case can one infer, by sheer impossibility, a mental state from the past.[61] In experiments related to pain, an attempt is made to inflict this sensation on the volunteer to observe the reaction of the brain while they reported discomfort. The same procedure is followed when volunteers are asked to lie.[62] But the problem is the same as before. Each brain is different, and it is difficult for two brains to react in the same way to an identical stimulus.[63] What is more, in analyzing only the brain of a person to establish a pattern of reactions, one must assume the honesty of the subject when determining this pattern or carry out a deception test, something that is almost impossible, at least within a legal scope.

On the other hand, one should not forget that declarations in court are practically never made under completely calm conditions, let alone with absolute sincerity. All declarants try to give a good impression, and it follows that they will make a rhetorical effort that will lead them to hide, disguise or add information, even when they try to be honest. Without entering into the interesting topic of false memories, which are also lies (certainly the most frequent kind) or indeed the many situations in which some consider the ethical choice to be not to tell the truth and in fact lie, it is extremely difficult for an honest declarant not to lie in any way at all. What is more, if a declaration were to be made under fMRI to answer a single question, one considered key to the case, the informative isolation in the formulated question could ultimately distort the information obtained.

In addition, one must not lose sight of an important fact: fMRIs do not identify, and nor can they conceptually identify, a lie. As we saw earlier, a lie is merely a philosophical concept. Instead, this technique could try to establish the cognitive and emotional processes associated with the act of lying.[64] This would not mean, logically, that an increase in activity in a certain area of the brain necessarily implies that the person is lying, which brings us back to the important point that the concept of a lie is philosophical. When we look at the path this type of research has taken, we are reminded of the historical pursuit of confession in legal proceedings, something that still endures, incomprehensibly, today. What is effective, although more complex, is to investigate the facts through evidence, while the 'simplest' solution, at least in appearance, is to look for a confession, though it may take us further from reality.

57 Pardo, 'Neuroscience Evidence, Legal Culture, and Criminal Procedure', cit. p. 307, 310. Masip, Jaume / Herrero, Carmen, 'Nuevas aproximaciones en detección de mentiras I y II', *Papeles del Psicólogo*, 2015, vol. 36 (2), p. 91.

58 Anwar, Yasmin, 'Scientists use brain imaging to reveal the movies in our mind', *Berkeley News*, 22-9-2011. http://news.berkeley.edu/2011/09/22/brain-movies/

59 Greely, 'Neuroscience, mindreading, and the Courts: the example of pain', cit. pp. 187 et seq.

60 Kahn, 'Neuroscience, Sincerity and the Law', p. 210. Greely, 'Neuroscience, mindreading, and the Courts: the example of pain', cit. p. 180.

61 Important accuracy for legal proceedings by Kahn, 'Neuroscience, Sincerity and the Law', p. 213.

62 Greely, 'Neuroscience, mindreading, and the Courts: the example of pain', cit. p. 180.

63 Greely, 'Neuroscience, mindreading, and the Courts: the example of pain', cit. p. 182.

64 Tong, Frank / Pratte, Michael S., *Decoding Patterns of Human Brain Activity*, vol. 63, Annual Review of Psychology, 2012, p. 502. See also pp. 497 et seq.

The future focus of study should therefore be oriented not to locating the 'lie' itself, but to ascertaining the facts without depending on the lie.[65] In this way, neuroscience can help considerably by determining the behavioural patterns of the subject rather than establishing that they are lying here and now.

Research has also been carried out to determine whether a person recognizes a place or face. Laboratory experiments appear to have been able to predict with fMRI whether a volunteer thought they recognized the face but not whether they truly recognized it.[66] The same has been done with the EEG and the P-300 wave, although some difficulty lies in determining whether the volunteer truly recognizes what he is seeing or merely that their attention is drawn to it.[67] The problem, therefore, is akin to the conceptual dilemma of a lie that we have seen before.

The fMRI has been commercialized, as mentioned earlier, by two companies,[68] one of which is no longer active in its sale. The problem of this test is exactly the same as before: its 'ecological validity', that is to say, its success beyond a laboratory environment with a very limited (4 to 30) group of volunteers.[69] In addition, as Kahn[70] points out, these experiments usually suffer from the WEIRD[71] problem: most of the voluntary subjects in these experiments fall into these categories, and their results have been extrapolated to everyone.[72] Considering the diversity of the global population, these subjects are in fact, as suggested by the word *weird*, the odd ones out.

Ultimately, it need not come to a *boutade*. The extreme example that comes to mind is that of carrying out fMRI on a dead salmon that had been shown a series of images of people to demonstrate that the salmon indeed 'thought' on seeing the images.[73] The technical limitations of these tests are absolutely evident, even to a layperson. Such tests would fail to meet the quality standards, which we will look at next, and currently remain in an excessively speculative realm, although that may change in the future, of course.

4 The Evidentiary Limitations of Neuroscience

Everything that has been described thus far falls within the scope of expert evidence, which has always been very complicated to assess. A judge has none of the technical knowledge of the expert and can hardly make a corrective contrast of their expert opinion, which leads inevitably to full, uncritical acceptance or rejection without cause.[74] In either case, the test is not actually assessed.

65 See also the interesting reflections and ideas of Masip / Herrero, 'Nuevas aproximaciones en detección de mentiras II', cit. pp. 96 et seq.
66 Greely, 'Neuroscience, mindreading, and the Courts: the example of pain', cit. p. 190.
67 Greely, 'Neuroscience, mindreading, and the Courts: the example of pain', cit. pp. 190-191.
68 No Lie MRI (http://www.noliemri.com/) and Cephos (http://www.cephoscorp.com/ The latter no longer uses this technique commercially.
69 Greely, 'Neuroscience, mindreading, and the Courts: the example of pain', cit. pp. 192-194. See also Schleim, Bildgebende Verfahren der Neurowissenschaften in der strafrechtlichen Ermittlungspraxis: Eine kritische Perspektive auf den Stand der Forschung', pp. 381 et seq.
70 Kahn, 'Neuroscience, Sincerity and the Law', p. 209.
71 Western, Educated, Industrialized, Rich, Democratic.
72 See Pardo, 'Neuroscience Evidence, Legal Culture, and Criminal Procedure', cit. p. 315.
73 Bennett, Craig M. / Baird, Abigail A. / Miller, Michael B. / Wolford, George L., 'Neural correlates of interspecies perspective taking in the post-mortem Atlantic Salmon: An argument for multiple comparisons correction'. http://prefrontal.org/ files/posters/Bennett-Salmon-2009.pdf.
74 For a more extensive account see Nieva Fenoll, Jordi, *La valoración de la prueba*, Madrid 2010, pp. 285 et seq.

Fortunately, in the 1990s the US Federal Supreme Court developed jurisprudence based on a series of three sentences and named it after one of the parties of the first case, Daubert.[75] This jurisprudence,[76] which led to an amendment of article 702 of the *Federal Rules of Evidence* in 2011,[77] was used in an attempt to address the difficulty of assessing a test that a judge has insufficient knowledge of. In the US, there is the added disadvantage that legal proceedings may involve trial by jury if the defendant does not waive this right, found in the Sixth Amendment, which creates a problem where the parties use very showy or spectacular expert tests, especially expert reports based on fMRI or MRI, that in reality lack scientific backing. Thus, the Supreme Court provided judges with five quality criteria and declared tests that failed to meet them as inadmissible to prevent them from influencing the jury. These five criteria are listed below: 1) the technique has been developed by scientific methods, that is to say, it has been verified empirically. This includes addressing any claim of falsification or rebuttal; 2) the technique used is described in the literature, having undergone peer review; 3) the degree of error of the technique has been reported; 4) standards and controls for the reliability of the technique are in place; and 5) returning to the Frye standard of 1923, there must be consensus in the scientific community on the technique used.

Taken together it is obvious that neuroscientific evidence that tries to demonstrate brain damage capable of affecting behavioural patterns will struggle to meet these criteria. It seems clear that neuroscience has managed to identify approximate functions of the different areas of the brain, but it would be foolhardy to claim that a certain injury or anatomical particularity in one of these areas is systematically and directly related to a certain behaviour. Thus, this analysis is for now always complementary to the traditional behavioural study performed by psychologists and psychiatrists, which, despite the existence of DSM-5,[78] also presents deficiencies and inaccuracies. Notwithstanding these limitations, as we have already seen, the courts have admitted these kinds of neuroscientific evidence in these cases,[79] following the line of Strickland jurisprudence.[80] It should be noted most seriously that regardless of how impressive they may seem, these tests cannot be given absolute credibility by judges. Instead, they must be evaluated together with the rest of the submitted material in the trial, along with the results of the behavioural analysis.

However, in terms of lie detection, courts in the US have rejected the validity of fMRI because it obviously does not meet the Daubert standard.[81] In fact, the verdict of the Semrau case was mainly based on the Frye standard, which is derived from the remaining criteria when dissent in the scientific community is moderately serious.[82] Bearing in mind the previous section, we only need to emphasize the *rebus sic stantibus* correction of this conclusion.

---

75 *Daubert v. Merrell* Dow Pharmaceuticals, 509 U.S. 579 (1993), General Electric Co. v. Joiner, 522 U.S. 136 (1997) and *Kumho Tire Co. v. Carmichael*, 526 U.S. 137 (1999).

76 This developed the Frye standard of 1923.

77 **Rule 702. Testimony by Expert Witnesses.** A witness who is qualified as an expert by knowledge, skill, experience, training or education may testify in the form of an opinion or otherwise if
(a) the expert's scientific, technical or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
(b) the testimony is based on sufficient facts or data;
(c) the testimony is the product of reliable principles and methods; and
(d) the expert has reliably applied the principles and methods to the facts of the case.

78 Diagnostic and Statistical Manual of Mental Disorders. American Psychiatric Association, *DSM-5.*, 2014.

79 Denno, Deborah W., 'The myth', cit. p. 507 et seq.

80 *Strickland v. Washington*, 466 U.S. (1984).

81 *United States v. Semrau*. 693 F.3d 510 (2012). http://www.ca6.uscourts.gov/opinions.pdf/12a0312p-06.pdf

82 See also in the same sense, Moreno, 'The Future of Neuroimaged Lie Detection and the Law', cit. pp. 724-725.

5 The Possible Constitutional Limitations of Neuroscience

While all this has doubtless legal relevance, examining the area of constitutional limitations is most important given the effect on fundamental rights that will be studied.[83] In order to shape this, it is necessary to understand, if only provisionally, that conclusions based on the study of brain injury are really effective and may, of course, be used as grounds for acquittal, as usually is the case, but they may also provide condemning evidence if the defendant is shown to have no brain injury whatsoever.

Regarding the potential of neuroscientific skill in the detection of lies, it is necessary to make a prognosis of how the law would treat this subject if, in the future, such evidence could really determine, more or less, the honesty of a person, something that at present is not really possible.

The conclusions on the matter of doctrine are contrasting and necessarily futurist, with an evident controversy that, more than anything, reveals the newness of the study in this area.[84]

5.1 The Right to Remain Silent and not Provide Evidence against Oneself

Let us suppose that the defendant refuses to make a statement or undergo a neuroscientific test that could effectively detect deception. Would their right to remain silent be affected? Let us say, for example, that the defendant refuses to undergo an MRI to study their brain anatomy. Would this go against the right to not provide evidence against oneself?[85]

This problem is not new. The US Federal Supreme Court addressed the question by creating the Frye standard in the case of the polygraph, creating jurisprudence that was used for 80 years,[86] until the technique was scientifically disregarded.[87] But this prompted the central question of the right to keep silent,[88] or rather, the question of whether the polygraph was compatible or not with this right.

What we should not lose sight of is that this right was created in seventeenth century England[89] to avoid torture or any type of pressure to force a suspect to confess. Since then, as new means of investigation in criminal proceedings have arisen, a growing trend has held that the court, and even the police, may access biological evidence from a suspect because their free will is not relevant, or rather, it is possible to obtain these materials without it.[90] Thus, this evidence could be obtained without

83 For more on this subject see Libano Beristain, Arantza, 'Neurociencia and penal process', Justice n. 2, 2015, pp. 249 et seq.

84 A useful summary of doctrinal views may be found in Shen, 'Neuroscience, Mental Privacy, and the Law', cit. pp. 694 et seq.

85 For more on this subject see Libano Beristain, 'Neurociencia y proceso penal', p. 253.

86 *United States v. Scheffer*, 523 U.S. 303 (1998).

87 National Research Council (Committee to Review the Scientific Evidence on the Polygraph), *The polygraph and lie detection*, 2003, pp. 212 et seq.

88 On the same subject, see Ormazabal Sanchez, *El derecho a no incriminarse*, Madrid, 2015, p. 39.

89 See MerkeL, Laura, 'Apuntes clave sobre el origen, sentido y futuro del derecho al silencio', Justicia 2016, 1, in press.

90 It is the 'testimonial nature' of the evidence in particular, so to speak, that depends on the will of the defendant, as opposed to the "physical nature" of the evidence, that would make it independent of their will. Pardo, 'Neuroscience Evidence, Legal Culture, and Criminal Procedure', cit. p. 329.

any need to exert even minimal state coercion, which is exactly what this right aims to avoid. This shift has developed mainly with regard to DNA testing.[91]

The key element that has determined until now the limits of admissibility in relation to this fundamental right has been based on the necessity of active collaboration from the defendant.[92] With neuroscientific expertise to study brain anatomy, the defendant does not really have to provide any 'active collaboration'; they only need to place themselves in a certain position so that a machine may examine them. This is certainly a type of collaboration, but it is passive and similar to that required for an x-ray or an identification lineup. Evidence may be obtained from all these mechanisms, but what is important to note is that the defendant could undergo these techniques even if in a vegetative state. The collaboration required is obviously not very different from that provided when fingerprints are taken.[93]

If we apply this conclusion to the topic at hand, a superficial analysis could cursorily admit the anatomical study of the brain by judicial authorization, either by using MRI or another diagnostic method that is in no way physically harmful to the person and that does not require any truly active collaboration. It could even be said that the aim of this test is always exculpatory or extenuating. In other words, it is carried out to observe if the behaviour of the defendant may have been influenced by brain injury, as already stated, in a way that is complementary to a behavioural study. Clearly, if no injury were found, the test would not benefit the subject in any way, but the result would be exactly the same as if it had not been performed.

To be precise, the brain is not a sample of blood, saliva, or urine. It is not even comparable with the DNA that may be extracted from this kind of evidence. As occurs in DNA testing,[94] the problem is the investigative potential of the evidence. Very few things can be obtained from hair or urine, but the potential for retrieving information from the brain is impressive and much more extensive than with DNA. As we will see in the following section, the brain and the *self* are one and the same. In other words, the brain is privacy in its purest state. It is inadvisable to establish any comparison with other biological tests; the evidence on which they are based simply does not compare with gray matter.

The conclusion is even simpler when we look at lie detection because it is actually possible to follow in part the doctrinal and case law guidelines. In these analyses active collaboration[95] from the defendant is in fact a determining factor, and coercion may take place, which would furthermore have disastrous effects on the scientific

91 See Libano Beristain, Arantza, *La intervención judicial en la prueba del ADN (commentary on the sentences of the Second Chamber of Supreme Court nº 501/2005, of the 19th of April, 2005 and nº 1311/2005* of the 14th of October, 2005), Revista de derecho y genoma humano, Nº 23, 2005, pp. 197-198. Martín Pastor, José, *La recogida por la policía judicial de muestras biológicas para la práctica de la prueba pericial de ADN en el proceso penal y el régimen de sometimiento del sujeto pasivo de las medidas de inspección, registro o intervención corporal*, La ley penal, n. 89, 2012, pp. 3 et seq.

92 Of the three elements to consider in infringement of the right to not self-incriminate established by American jurisprudence—compulsion, incrimination, and testimony— "active collaboration" refers to the first. See Pardo, "Neuroscience Evidence, Legal Culture, and Criminal Procedure", cit. p. 328.

93 See also Pardo, 'Neuroscience Evidence, Legal Culture, and Criminal Procedure', cit. p. 328. SHEN, 'Neuroscience, Mental Privacy, and the Law', cit. p. 703.

94 See Miranda Estrampes, Manuel / Nieva Fenoll, Jordi, 'Comentario a la sentencia Maryland vs. King del Tribunal Supremo Federal de los Estados Unidos de América (3-VI-2013)', *Revista de Derecho y Genoma Humano*, n. 39, julio-dic. 2013, pp. 119 et seq.

95 Shen, 'Neuroscience, Mental Privacy, and the Law', cit. p. 704.

viability of the test.[96] Coercion may activate areas of the brain that could wrongly make the defendant appear to be lying. Indeed, beyond the infringement of a fundamental right, using force to carry out a lie detection test would make it non–viable due to the more than likely distortion of the results, even if one day such results could be scientifically confirmed.[97] Consequently, there is no need to enter into a debate on fundamental rights in this matter. The detection of lies is either voluntary or it cannot be carried out, not even by coactively placing the defendant in the fMRI scanner or some future device.

Another question, obviously, is if the refusal to undergo lie detection testing would be considered incriminating evidence in a way that resembles what is being attempted surreptitiously, and unfortunately, since the Murray judgment at the European Court of Human Rights[98] with regard to the right to be silent. That debate, which has also arisen in regard to DNA testing in civil paternity suites,[99] is however completely inappropriate in criminal proceedings. This is not only because one would be faced with not just an impossible, in my opinion, application of the institution of the burden of proof in criminal proceedings,[100] but also because even if it were applied, the result would be used *against the defendant*, something that is completely incompatible with the presumption of innocence. Beyond that, with such a rule we would make an exception to the free appraisal of evidence in criminal proceedings, something that would not be acceptable from any point of view.

5.2 The Right to Privacy

As mentioned previously, the MRI and other similar methods to detect anomalies in the brain, while apparently acceptable in regard to the previous right, are radically inadmissible from the perspective of the right to privacy,[101] and therefore performing such a test without the consent of the defendant is not legally viable.

The inside of the skull has been compared with the interior of a home.[102] If the latter cannot be accessed without the consent of the defendant or by judicial warrant, there is even more reason to prohibit access to something irrefutably more private

96 Curiously, the same was demonstrated by Hanns-Joachim Scharff in World War II, which should have had the effect of abolishing torture in interrogations since then. According to Simpson, David, 'Because we could', *London Review of Books*, vol. 32, n. 22, 18-11-2010, pp. 27-28: 'one fascinating story I had not previously come across: that of Hanns-Joachim Scharff, one of the most successful interrogators of World War Two. The Hollywood Nazi comes dressed in a leather coat and wielding a pistol, pliers, bright lights and burning cigarette ends: he has ways of making you talk. Scharff apparently never used violence. His methods involved "a combination of language proficiency; relaxed, casual conversation over the course of several weeks if time permitted; and above all other things, empathy". Did we know about his methods? Yes, we did. After the war Scharff was invited by the US Air Force to lecture about his experiences, and what he taught them should have found its way into the manuals. A number of other interrogation experts agree that non-violent procedures are by far the most effective way of obtaining information. But no one has made a movie about them.'

97 I clarify this with the opinion expressed in Nieva Fenoll, *La duda en el proceso penal*, Madrid 2013, p. 159.

98 *Murray v. United Kingdom*, S. 8-2-1996: '(…) The national court cannot conclude that the accused is guilty merely because he chooses to remain silent. It is only if the evidence against the accused "calls" for an explanation which the accused ought to be in a position to give that a failure to give any explanation "may as a matter of common sense allow the drawing of an inference that there is no explanation and that the accused is guilty"'.

99 See article 767.4 of the Code of Civil Procedure.

100 See Nieva Fenoll, 'La razón de ser de la presunción de inocencia', *InDret* 1/2016, pp. 1 et seq.

101 See Lever, Annabelle, 'Neuroscience v. Privacy? A Democratic Perspective'. http://www.alever.net/DOCS/Neuroscience%20v.%20Privacy.pdf. Moore, Adam D., *Privacy, Neuroscience, and Neuro-Surveillance*, 13-4-2016 pp. 1-2. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2764437. Libano Beristain, 'Neurociencia y proceso penal', p. 253.

102 Pardo, 'Neuroscience Evidence, Legal Culture, and Criminal Procedure', cit. p. 325.

like the cranial cavity. The comparison is accurate but with one very important reservation: *the brain must not be explored by judicial authorization except in cases of mental disability*. Certainly, in any search what must always exist is a founded suspicion in order to carry out the test, the *probable cause* of the Fourth Amendment, and when present[103] it is possible for a judicial authority to order a forced entry and search. But under no circumstances may the same logic be used with neuroscientific evidence.

The reason, which will be reiterated in the following section, is that the brain does not enclose our privacy: it is privacy itself. It makes up our whole life, our personality, our ideas, and much more. It is our conscience in the most proper sense of the word, and our mental pathologies form part of it. Therefore, unless state control of consciences is being pursued, not even a judge can order this test. Even in the current age of the advancement of science in which only anatomical anomalies, electrical currents, and blood flow may be observed, often with doubtful interpretation, what is ascertained leaves us completely vulnerable to the state. It makes our person, our inner selves, dependent on the decision of a judge, and our right to privacy is completely annulled.

With other evidence, like the interception of communications, entry and search, or even DNA testing, only a part of that privacy is revealed. But with this test, we may in the future ascertain personal or ideological tendencies, things that are the basis of our privacy. It is one thing for a psychologist to use a cognitive interview to deduce behavioural patterns with the expert ability of science, but it is quite another for the state to enter our brain directly. With the current advance of neuroscience, this already presents a danger if, for example, someone wanted to remove subjects with a certain brain anomaly from society. The more neuroscience advances, the greater such dangers will be.

The state cannot, in my opinion, enforce the use of these tests, not even through judicial warrant, since it would be denying a civil right without any leeway whatsoever. This is unacceptable in a democratic society. The only viable way forward is for the defendant to give consent, as has been the case until now, save for some exceptions. Unless we wish to tumble into a social model that will be described in the next section, these tests should not be carried out.

If this were allowed, once society accepts the idea that these neuroscientific tests are commonplace and 'good', the next governmental decision may be to arbitrarily and scandalously establish that performing such studies should be systematic in any criminal proceeding.[104] One thing is to occasionally include them as a complementary test to determine the possible existence of a mental condition *alleged by the defendant and performed at all times with their consent*, but it is quite another for the state to analyse our brains systematically, given that, as mentioned before, ideologically relevant information may also be obtained. This is an extraordinarily slippery slope, and we need only look at history for proof. Although the science behind these analyses currently has little potentiality, we cannot rule out that politically relevant data, such as religious or political inclinations, may be obtainable in the future; in fact, research in this area is already being carried out.[105] Therefore, systematic use of these studies, like any other general inquiry, should be excluded.

---

103 Shen, 'Neuroscience, Mental Privacy, and the Law', cit. p. 699.

104 See also Pardo, 'Neuroscience Evidence, Legal Culture, and Criminal Procedure', cit. p. 327. Shen, 'Neuroscience, Mental Privacy, and the Law', cit. p. 707.

105 Jost, John / Nam, H. Hanna / Amodio, David M. / Van Bavel, Jay J., 'Political Neuroscience: The Beginning of a Beautiful Friendship', *Advances in Political Psychology*, vol. 5, supp. 1, 2014, pp. 3 et seq.

6 The Future: What Kind of World do We Want?

The use in criminal proceedings of the techniques outlined above has, like all other scientific matters, an unclear future. What is true is that anyone claiming that something is impossible in science may be proven wrong within a few years. But what is also certain is that many people shout from the rooftops about future scenarios that never come to be. In the 1970s, after having landed on the moon, we imagined the human species colonizing the solar system by the end of the millennium. This has yet to occur, nor does it even seem possible in the near future.

Regrettably, neuroscientific research is victim to the occasional guru, who clouds the truly useful findings of serious researchers. In my opinion, the most disquieting interpretation of these studies, the possibility of 'reading minds', is in fact quite remote. It may of course be feasible, however, to identify behavioural patterns with these tests, and this would be extremely dangerous if it led to widespread use for the purposes of ideological or sexual persecution, for example, as mentioned above.

Therefore, it is first and foremost advisable not to use these tests systematically in criminal proceedings. And when they are used, consent should always be obtained from the defendant until the scientific evidence is, as I stated earlier, more robust. But regardless of whether such evidence is acquired one day, we must not forget that our innermost privacy, that is to say, our very selves or egos (if they exist), are hidden in our brains.

This being the case, I must reiterate that these tests should not be accessed by judicial warrant, given that this warrant, in theory, can limit but never completely suppress a fundamental right, although this has not generally been underscored by legal doctrine to date. Fundamental rights are our only defence as citizens against the power of the state. At present, private home searches are exceptional, and so should it continue to be the case, with the precise aim of protecting our privacy. Increasingly more tools are being developed to protect our communications, and despite a rather troubling period in that respect, things now appear to be going along the right path; thanks mainly to telecommunication companies that are rightly resisting pressure from governments.

I must emphasize that our brains must never be analysed by the state unconditionally. Only with our authorization, and not that of a judge, can such testing in my opinion take place and always for exculpatory and never inculpatory purposes. The reason is simple. Our minds are the last, non-waivable substrate of privacy, and for that reason the state cannot under any circumstances access them without our consent. If we allowed it, all remaining protection of our privacy would cease, rendering the important measure of civil protection from the state completely useless.

This would mean the realization of everything every dictatorship has aimed for: mind control through ideological control, in theory, but ultimately extendable to any scope. Whatever the advancement of technology in this area, and without becoming perhaps unjustifiably alarmed, it is necessary to hold absolutely firm that access to our minds depends exclusively on ourselves. Anything else would mean a loss of our freedom.

POLIISI
POLICE UNIVERSITY COLLEGE

Technology is continuously reshaping society. Finding legal and practical solutions to prevent and contain undesired phenomena, such as cybercrime, and to promote cybersecurity is becoming a matter of survival.

The aim of this book is to reflect on the relationship between crime, law, and technology. Finland is among the leading countries in the process of digitalization and modernization of its infrastructures. For this reason, the country is the optimal starting point for the exploration of such a topic.

This book explores the relationship among crime, law, and technology by addressing three distinct thematic areas: “Finnish and Nordic Legislation on Cybercrime”, “Local and Global Challenges in the Fight against Cybercrime”, and “Future Scenarios in Law and Technology.” Although most of the time Finland is the example used, the general issues discussed in this book are common across the globe.

9 789518 153576

Police University College • Vaajakatu 2, FI-33720 Tampere • tel. +358 295 480 121 • www.polamk.fi