TILBURG LAW SCHOOL
TILBURG INSTITUTE FOR LAW AND TECHNOLOGY
LAW & TECHNOLOGY (LL.M)
2016-2017

MASTER THESIS
PROTECTION OF THE E-COMMERCE ECONOMY FROM CYBERCRIME
THROUGH AN APPROPRIATE PRIVACY LEGAL FRAMEWORK

AUTHOR: AKINPELU, AYOKUNLE OLUWATOBI
ANR: 898931

SUPERVISOR: QUELLE CLAUDIA
SECOND READER: K.K. E SILVA

TILBURG, JANUARY 2017
# TABLE OF CONTENTS

**List of Abbreviations** .............................................................

1. **Introduction** .............................................................................. 1
   1.1 Background ........................................................................ 1
   1.2 Aims and objectives ......................................................... 4
   1.3 Research question .......................................................... 4
   1.4 Research methodology .................................................. 5
   1.5 Overview of thesis ........................................................ 5

2: **Illegal Data Access in the e-Commerce Economy and the Cybercrime Directive** .................................................. 6
   2.1 Introduction ........................................................................ 6
   2.2 Illegal Data Access and the Cybercrime Directive ................. 6
   2.3 Challenges in Enforcing Article 3 of the Cybercrime Directive .... 10
   2.4 Conclusion ...................................................................... 14

3: **Illegal Data Access and the National Information System Directive** .................................................. 15
   3.1 Introduction ...................................................................... 15
   3.2.1 Scope of the Network Information System Directive ........ 16
   3.2.2 Data Security Requirement under the Network Information System Directive .................................................. 18
   3.4 Conclusion ...................................................................... 24

4: **Illegal Data Access and General Data Protection Regulation** .......................................................... 25
   4.1 Introduction ...................................................................... 25
   4.2.1 Scope of the General Data Protection Regulation ............. 26
   4.2.2 Data Security Requirement under the General Data Protection Regulation .................................................. 28
   4.4 Conclusion ...................................................................... 35

5. **Conclusion** .................................................................................. 37

**Bibliography**
LIST OF ABBREVIATIONS

B2B: Business to Business
B2C: Business to Consumer
E-Commerce: Electronic Commerce
GDPR: General Data Protection Regulation (GDPR)
NIS: Network and Information Security
CHAPTER ONE: INTRODUCTION

1.1 BACKGROUND

Information systems are increasingly important to the efficient operation of government; corporations and society in general, with that importance comes an increasing risk of information security breaches, compounded by systems’ networked nature.\(^1\) The Internet now connects over 2.1 billion people worldwide.\(^2\) In many nations, it provides the basic infrastructure for information services and systems essential for economic and social well-being. With so much riding on the internet and the modern information system it supports, many forms of criminal activity are migrating to this realm.\(^3\) As misuse and abuse of the internet continues to grow, many believe that there must be a greater emphasis on law in order to protect individuals and organizations in an internet environment that provides fertile ground for criminal activity as well as innovation and development.\(^4\) Yet, crafting effective legislation and regulation for this environment presents considerable challenges.\(^5\)

Each day sees numerous new individuals, organizations, and government agencies all over the world linking up electronically to get or exchange information and to execute business transactions of one kind or another.\(^6\) With its platform-independent technology and ubiquitous reach, the internet allows companies to open up new distribution channels, forge communities of buyers and sellers, increase revenues, and boost the bottom line.\(^7\) Electronic commerce is redrawing the global commerce map as national state boundaries become less significant to the mobility of capital with time difference no longer posing any problem to the conduct of business. Security and data protection concerns are major stumbling blocks for the growth of electronic commerce. Many e-commerce sites directly ask users for personal information for the purpose of carrying out electronic transactions.\(^8\) Without the exchange of data, electronic commercial transaction cannot be effectively carried out.\(^9\) With growing concerns on security and data protection, consumers hesitate in providing confidential data such as their home

---

3. D Salane and E Misshula, Legislative and Regulatory Attempts to Address Cybercrime: The Good, the Bad and the Ugly (John Jay College of Criminal Justice Center for Cybercrime Studies Mathematics and Computer Science Department 2012).
5. Salane and Misshula (n 3) 2.
address, social security number, and credit card number over the internet for the fear of illegal data access. Careful review of the empirical evidence suggests that illegal access pose a significant threat to the future of electronic commerce in significant ways. They breach consumer trust and undermine the confidence of the public in the e-commerce economy which is major factor impeding the successful proliferation of e-commerce as identified by major corporations. According to reports by Better Business Bureau, a major reason people are hesitant about the use of electronic economy includes concern about the online payment security, reliability of companies and fear of data breaches. It further canvasses that there is a necessity to promote trust and confidence on the internet. Trustworthiness of the technology supporting the e-commerce transaction is of vital importance to consumer’s trust. The more consumers count on the supporting technology of the electronic commerce economy, the more they view it as a trusted relationship; the greater the premium that best practice companies will command. On the other hand, the greater the corresponding erosion of trust for the technology upon which electronic commerce is built the higher the level of distrust and aversion for engaging in electronic commerce transactions. Evidently, an unrestrained illegal access to data would erode trust and may lead to the collapse of the electronic commerce, this is a significant threat. Illegal access is usually the first step towards the commission of a data breach, particularly in the electronic commerce industry, which relies on the consumer’s data in order to effectively function, this thesis shall focus on the offence of illegal access; as the peculiar nature of electronic commerce as a platform making use of electronic data interchange makes it highly susceptible to illegal access than other forms of criminal activity. In response to optimism of law as a tool for curbing illegal access, the European Union has enacted the Cybercrime Directive which is a principal legal framework responding to the misuse and abuse of computer networks. One of the objectives of the Cybercrime Directive is to criminalise cyberattacks by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions. The Cybercrime Directive also provides for other types of offences which includes; illegal system interference; illegal data interference and illegal interception.

10 Bingi and Others (n 7) 26.
12 Gefen (n 11) 726.
14 Lee and Others (n 13) 842.
17 Cybercrime Directive, preamble 1.
19 Cybercrime Directive, art 5.
In defining conducts and behaviours that are punishable by the Directive, the Cybercrime Directive specifically declares illegal access to information systems\textsuperscript{21} as criminal and punishable in cases which are not minor. Illegal access to information systems\textsuperscript{22} refers to situations where someone, usually knowledgeable and skilled in computer techniques, breaks into an information system, without authorization from the controller, in order to gain access (or control) to its functions or data.\textsuperscript{23} An information system is defined as a device or group of devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purpose of its or their operation, use, protection and maintenance.\textsuperscript{24} The term information system applies not only to the networks supporting the communication of data between devices but also to the computer data (or digital data, present on a particular device or set of devices).\textsuperscript{25} Data can be defined as a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function.\textsuperscript{26} The challenge with the criminalisation of illegal data access according to the provision of Article 3 of the Cybercrime Directive is the enforcement; as illegal data access challenges traditional criminal investigation and the criminal justice system. The internet is an internationalized environment, the information network as well, so also is cybercrime. Illegal data access takes place over multiple regional or national jurisdictions. Further to internationalization is the pace at which cybercrime occurs. Cybercrime sometimes occur in a fraction of a second and sometimes spread at an astonishing speed. Unfortunately, internationalization makes evidence gathering difficult as digital information, which is evanescent by nature can be deleted or altered. Anonymity, another recurrent feature of the internet makes attribution and retribution difficult and sometimes impossible, and with internationalization, oversight and enforcement are hindered. In a system where activities are highly multiplexed, enforcement and oversight measures often require general surveillance and can infringe on privacy rights.\textsuperscript{27} It is against the backdrop of these challenges that is becomes pertinent to consider the instrumentality of information security and data protection as a check tool on illegal data access in the e-commerce sector. Information security means the ability of networks and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.\textsuperscript{28} Information security and is related to data protection and privacy and this has been reflected at various

\textsuperscript{21} Cybercrime Directive, art 3.
\textsuperscript{22} Cybercrime Directive, art 3.
\textsuperscript{23} Miguel and Others (n 15) 55.
\textsuperscript{24} Cybercrime Directive, art 2 (a).
\textsuperscript{25} Miguel and Others (n 15) 58.
\textsuperscript{26} Cybercrime Directive, art 2.
\textsuperscript{27} Cate (n 4) 62.

To circumvent the challenges arising from the criminalisation of the illegal data access as established in Article 3 of the Cybercrime Act, Article 16-17 of the NIS Directive[33] which relates to information security and Article 32-34 of the GDPR which relates to security of data processing and data breach notification can be explored. Preventing misuse and abuse of the information network, especially illegal data access need not be limited to the territorial nature of the criminal law as exemplified by Article 3 of the Cybercrime Directive and further made challenging by the architecture of the internet. Premised on the arising challenges of enforcing Article 3 and the necessity of protecting the electronic commerce from illegal data access, it becomes crucial to consider whether an effective enforcement of the provisions of Article 32-34 of the GDPR[34] and Article 16-17 of the NIS Directive would cover the gaps in Article 3 of the Cybercrime Directive and aid in the reducing and/or curbing illegal data access.

1.2 AIMS AND OBJECTIVES

The aim of this research is to consider the use of privacy and data protection laws and the NIS Directive in curbing illegal access within the electronic commerce economy. This research work will also consider and make recommendations as to the changes that may be effected in privacy and data protection laws as well as the NIS Directive in order to curb illegal access within the e-commerce economy and create a safe platform for consumers and user.

The objective of this research is to consider the effectiveness of Article 3 of the Cybercrime Directive and investigate the impact of Article 32-34 GDPR and Article 16-17 of the NIS Directive as a medium for reducing illegal data access, while promoting e-commerce economy and ensuring the protection of consumers and users.

1.3 RESEARCH QUESTION

Can the provision of Article 32-34 of the GDPR and Article 16-17 of the NIS Directive fill the gaps in the enforcement of Article 3 of the Cybercrime Directive?

SUB-QUESTION:

a) What are gaps in the enforcement of the Cybercrime Directive against illegal data access within the e-commerce economy?

---

32 NIS Directive.
33 NIS Directive.
34 General Data Protection Regulation.
b) How does Article 16-17 of the NIS Directive fill the observed gaps in the enforcement of the Cybercrime Directive?
c) What does the provision of Article 32-34 GDPR add to Article 16-17 NIS Directive and the gaps in the enforcement of the Cybercrime Directive against illegal data access within the e-commerce economy?

1.4 RESEARCH METHODOLOGY
In considering appropriate legal framework that is effective in protecting data within the e-commerce economy, attention is focussed on the NIS Directive and the GDPR as there scope is within the information society services as defined by the E-commerce Directive. While the e-Privacy Directive also provides for data security, its scope expressly excludes information society services and for which it becomes irrelevant to the e-commerce economy players. In order to consider the use of data regulation in curbing illegal data access within the electronic commerce economy, this research would make use of a library-based information system such as books, case reports, legislation, treaties, scholarly articles and news journal which are available via the library, internet, and Westlaw in answering the questions and prescribing an appropriate legal privacy framework for the protection of the e-commerce economy from cybercriminals. For the sake of brevity, reflections would primarily be taken from laws, policies and scholarly articles using the European Union as the focal point.

1.5 OVERVIEW OF THESIS
This thesis consists of five chapters:

- The first chapter serves as the introduction consisting of the introduction, aims and objectives, research questions, the methodology of conducting the research and an overview of the thesis chapters.
- The second chapter examines the provisions of the Cybercrime Directive in curbing the activities of cybercriminals and the challenges of enforcing the Directive in dealing with illegal data access.
- In the third chapter, an attempt is being made to examine data security under the National Information Directive. The essence of this is to consider the effect of the data security requirement under the e-commerce economy, with a view of discovering whether compliance with the provisions of the data security requirement would have an impact on the illegal data access. Further, an analysis of the National Information Security Directive would be undertaken in order to identify if the gaps observed in Article 3 of the Cybercrime Directive can be covered by the provisions of Article 16-17 of the National Information Security Directive.
- In chapter four, attempts would be made in examining the data security requirement as enshrined in Article 32-34 of the GDPR. Further, there would also be consideration into how the requirements help enhance data safety and security in the e-commerce economy.
- In chapter 5, there would be a conclusion stating an informed opinion to the effectiveness of the current legal regime for protection of the e-commerce economy from illegal data access and the lessons drawn would be emphasized.
CHAPTER 2

ILLEGAL DATA ACCESS IN THE E-COMMERCE ECONOMY AND THE CYBERCRIME DIRECTIVE

2.1 INTRODUCTION

Electronic commerce according to the E-commerce Directive is defined as any Information Society service, that is, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purpose of clarity and by the legislative definition, “at a distance” means that the service is provided without the parties being simultaneously present; “by electronic means” means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; “at the individual request of a recipient of services” means that the service is provided through the transmission of data on individual request. Illegal data access has however gained widespread attention as businesses of all sizes become increasingly reliant on digital data, cloud computing, and workforce mobility. With sensitive personal and business data stored on local machines, on enterprise databases, and on cloud servers, breaching a company’s data has become as simple – or as complex – as gaining access to restricted networks. According to a European Commission Report, some of the most serious incidents of attacks against information systems are directed against electronic commerce companies. This chapter examines illegal data access under the Cybercrime Directive and the challenges in enforcing the provisions of the Cybercrime Directive.

2.2 ILLEGAL DATA ACCESS AND THE CYBERCRIME DIRECTIVE

The Cybercrime Directive was enacted with the purpose of establishing minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems and also aims to develop a legal framework to prevent such offences and to improve cooperation between law enforcement bodies. Importantly as well, is the need to ensure the smooth operation of systems in the Union which are vital for the development of the internal market and of a competitive and innovative economy. Thus, the interests protected in this recital are inclusive of the economic development of the internal market. The jurisdiction

37 Gaur (n 36).
of the Cybercrime Directive is inclusive of both territorial and personal jurisdiction.\textsuperscript{41} Member States are required to establish jurisdiction over illegal data access when the unlawful intrusion occurs in whole or in part within their territory;\textsuperscript{42} by one of their nationals, at least in cases where the act is an offence where it is committed.\textsuperscript{43} As regards the commission of the offence in whole or in part, the Member States shall ensure that illegal access is an offence, when the offender is physically present on its territory, whether or not the offence is against an information system on its territory;\textsuperscript{44} or the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory.\textsuperscript{45} While the Cybercrime Directive does not establish extra-territoriality, it requires Member State to keep it adequately informed where it does in cases where the offender has his or her habitual residence in its territory;\textsuperscript{46} or the offence is committed for the benefit of a legal person established in its territory.\textsuperscript{47} Generally Member States tend to legislate some form of extra-territorial jurisdiction for illegal data access,\textsuperscript{48} the extra-territorial effect is heavily qualified and does not generally include instances, where the offender is not a resident within its territory, non-citizens and resident in jurisdiction where illegal data access is not criminalized.

Instructively, the provisions of Article 3 is applicable to both natural and legal persons. Member states are enjoined to take necessary measures to ensure that legal persons can be held accountable for a breach of Article 3, committed for their benefit by any person, acting either individually or as part of a body of the legal person, and having a leading position within the legal person, based on one of the following: a power of representation of the legal person; an authority to take decisions on behalf of the legal person; an authority to exercise control within the legal person.\textsuperscript{49} The liabilities for the commission of illegal access by a legal person shall however not exclude criminal proceedings against natural persons who are perpetrators or inciters of, or accessories to the intrusion.

\textsuperscript{41} Cybercrime Directive, art 12.
\textsuperscript{42} Cybercrime Directive, art 12(1) (a).
\textsuperscript{43} Cybercrime Directive, art 12(1) (b).
\textsuperscript{44} Cybercrime Directive, art 12(2) (a).
\textsuperscript{45} Cybercrime Directive, art 12(2) (b).
\textsuperscript{46} Cybercrime Directive, art 12(3) (a).
\textsuperscript{47} Cybercrime Directive, art 12(3) (b).
\textsuperscript{48} Member States used as case study in this thesis do really try to establish some form of extra-territoriality in their criminal law to but such is not uniform, and there are fundamental differences. See Netherlands: art 4a Dutch Criminal Code II (Wetboek van Strafvoering); Germany: s 7 German Criminal Code (Strafgesetzbuches durch); UK: Serious Crime Act, s 43.
\textsuperscript{49} Cybercrime Directive, art 10.
Article 3 of Cybercrime Directive stipulates that illegal access to information systems is considered a criminal offence,\(^{50}\) and punishable for a maximum term of at least two years.\(^{51}\) This category of offence comprises of a series of computer attacks, known in literature as hacking.\(^{52}\) Illegal access to information systems includes accessing without right, whole or part of a device that can run executable code or accessing any software or any content related data on such a device\(^{53}\) and/or illegal access and/or use of passwords, access codes and encryption codes.\(^{54}\)

For the illegal access to be viewed as a criminal offence, there must have been an intentional access without right to the whole or any part of an information system by infringing a security measure.\(^{55}\) Hence, the Cybercrime Directive does not impose criminal liability where the objective criterion is met but the acts are committed without criminal intent,\(^{56}\) such as instances where a person is not aware that access was unauthorised or in cases of mandated testing for the protection of information systems.\(^{57}\) It is therefore a prerequisite that there must be the presence of a malicious intention as a motive behind the illegal access and/or access without legal permission from the owner, or other right holder of the system.\(^{58}\) The infringement of a security measure coupled with intent is a therefore prerequisite for determining whether a conduct should be incriminating as a criminal offence.\(^{59}\)

Further, the Cybercrime Directive also stipulates that the offence of illegal access of an information system does not include minor cases even when there has been a breach of security measures.\(^{60}\) A case is considered minor when the damage caused by the offence and/or the risk to public or private interests, such as to the integrity of a computer system or to computer data, or to the integrity, rights or other interests of a person, is insignificant or is of such a nature that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary.\(^{61}\) While the Cybercrime Directive provides clarity on minor cases, there is no definition of security measures anywhere within the Cybercrime Directive.\(^{62}\) Since the requirement of the Cybercrime Directive are minimal requirement, it thus becomes imperative to consider the implementation of Cybercrime Directive within the leading jurisdiction of the European Union; United Kingdom, Netherlands and Germany.

\(^{51}\) Cybercrime Directive, art 9(2).
\(^{54}\) Moise (n 52) 377.
\(^{55}\) De Hert and Others (n 50) 505.
\(^{56}\) Cybercrime Directive, recital 17.
\(^{57}\) Cybercrime Directive, recital 17.
\(^{58}\) Miguel and Others (n 15) 55.
\(^{59}\) Miguel and Others (n 15) 55.
\(^{60}\) Cybercrime Directive, art 3.
\(^{61}\) Cybercrime Directive, recital 11.
\(^{62}\) Miguel and Others (n 15) 55.
In the Netherlands, the Criminal Code II makes provision for unauthorized access by prescribing punishment for both intentional and unlawful access to a computerised device or system and computer trespass. Unlawful access is deemed committed if access to the computerised device or system is gained by breaching a security measure; by a technical intervention; by means of false signals or a false key or by assuming a false identity. As regards computer trespass, this occurs when a person has unlawfully accessed a computerised device or system and subsequently copied the data stored, processed or transferred for his own purpose or that of another. Computer trespass also occurs when a person uses a public telecommunication network to access the computerised device or system to which he has unlawfully gained entry. The Dutch Criminal Code II further requires that a security measure be violated before there is a commission of an unauthorized access. Illegal access is punished with imprisonment of up to two years for the basic offence of unlawful access, and up to four years in its qualified forms (copying data or hacking onwards from the hacked computer).

The implementation of the Cybercrime Directive by Germany was through the German Criminal Code (GCC). The GCC stipulates that data espionage as a criminal offence and punishable by a maximum term of three years. Data espionage under the GCC is to be read as illegal data access or hacking for which an offence can only arise upon the circumvention of a security measure. The ambit of the legislation in the German Criminal Code is severely limited to illegal access to data strictly as the wordings of the section specifically mentioned.
the limitation to data\textsuperscript{74} with data being defined as only those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.\textsuperscript{75}

The position of the United Kingdom quite differs from those of the Netherlands and Germany. In the UK, the Computer Misuse Act (CMA) describes illegal access to computer material and illegal access with intent to commit or facilitate commission of further offences as criminal offences.\textsuperscript{76} Sec.1-3 of the CMA criminalizes hacking activities including the commission of hacking activities with the purpose of committing further crimes.\textsuperscript{77} The Computer Misuse Act provides that anyone who without authorisation access a computer to perform any function with intent to secure access to any program or data held in any computer is guilty of an offence;\textsuperscript{78} if the access he intends to secure is unauthorised;\textsuperscript{79} and he knows at the time when he causes the computer to perform the function that that is the case.\textsuperscript{80} Again, the Act does not require that there must have been a breach of security before the commission of the offence.

Within the researched member states, there is observed some level of harmonization. However, none of the Member States considered made a provision for minor cases. This stricter position is a positive point, since the Cybercrime Directive was enacted to establish a minimum definition of offences. While the legislation of the Netherlands and Germany requires a breach of security measures, the UK provides a more flexible scope of criminalization. This difference could be related to the differences between civil law and common law traditions.\textsuperscript{81}

\subsection*{2.3 CHALLENGES IN ENFORCING ARTICLE 3 OF THE CYBERCRIME DIRECTIVE}

The Internet as a globally connected system have grave impact on the implementation of the Cybercrime Directive.\textsuperscript{82} Illegal data access can occur over multiply jurisdictions and cause damage in another jurisdiction.\textsuperscript{83} Territorial, personal, subject matter jurisdiction are crucial elements in the enforcement of cybercrime legislations.\textsuperscript{84} Jurisdiction as a legal term means the reach of the law of one State over acts and individuals and thus entails responsibility for regulation.\textsuperscript{85} It is a mechanism used to establish how and over whom what law applies.\textsuperscript{86} Jurisdiction is currently first and foremost a State territorial concept, and there is general consensus on the principle that within the territory of a sovereign State, the laws of that State apply.\textsuperscript{87} The Cybercrime Directive establishes extraterritorial jurisdiction in cases where the

\begin{thebibliography}{99}
\bibitem{74}German Criminal Code, s 202a (1).
\bibitem{75}German Criminal Code, s 202a (1).
\bibitem{76}Samantha and Others (n 73).
\bibitem{77}J Clough, ‘Principles of Cybercrime’ (Cambridge University Press 2012) 114.
\bibitem{78}Computer Misuse Act 1990, s 1 (a).
\bibitem{79}Computer Misuse Act 1990, s 1 (b).
\bibitem{80}Computer Misuse Act 1990, s 1 (c).
\bibitem{81}Samantha and Others (n 73).
\bibitem{85}K Soukieh, ‘Cybercrime Shifting Doctrine of Jurisdiction’ (2011) 10 Canberra Law Review 221.
\bibitem{87}Samantha and Others (n 73).
\end{thebibliography}
offence is committed by its national in a territory where illegal data access is a crime. The Cybercrime Directive further requires that a Member State should have jurisdiction over the offence when the offender is within its territory irrespective of whether the offence is against an information system within its territory and in circumstances where the illegal access is against an information system in its territory irrespective of whether the offender is physically present within its territory. Data can be accessed through internet networks that span the globe, a hacker can operate from a location outside the jurisdiction of the European Union which criminalises illegal data access by the Cybercrime Directive. The global nature of illegal access to data poses legal challenges in the enforcement of Article 3 of the Cybercrime Directive, since the cyberspace has no geographic boundaries, data infringers are free to operate from anywhere in the world. Most illegal data access occurs outside of countries with strong regulatory framework inclusive of the European Union. The challenge would therefore be the enforcement of extra-territorial jurisdiction in cases where the hacker has committed and offence against an information system in the EU without being physical present with the territorial boundaries of the member state. While any country can assert jurisdiction over an offence, that does not automatically translate to the enforcement of the jurisdiction. As a general principle, at least in common law countries, serious criminal offences will not be tried in absentia. With the multi-jurisdictionality of the internet, if a state does not criminalise a particular conduct, persons within its jurisdiction may act with impunity in committing offences that affect other jurisdictions. The practical ability to prosecute the offender who is physically within the jurisdiction of another state comes into question, especially when the state has no interest in prosecuting. Usually, states make use of extradition, which is the willful surrender by a state for the purpose of prosecution and is usually supported by bilateral treaties in form a Mutual Legal Assistance Framework which requires dual criminality;

88 Cybercrime Directive, art 12(1) (b).
89 Cybercrime Directive, art 12(2) (a).
90 Cybercrime Directive, art 12(2) (b).
95 Clough (n 94) 710.
96 Clough (n 94) 710.
that is the offence committed must be an offence under the laws of both jurisdictions.\textsuperscript{103} Many illegal data access affects more than one country\textsuperscript{102} hence criminals need not be present at the same location as the target.\textsuperscript{103} As the location of the criminal can be completely different from the crime site, many unauthorized illegal data access are transnational and offenders seek to avoid countries with strong cybercrime legislations.\textsuperscript{104} With the existence of countries without legislation against illegal data access, offenders would continue to use them to disrupt investigation and possible prosecution.\textsuperscript{105}

Anonymous technology and encryption pose a considerable threat to government and private institutions by enabling criminals to operate surreptitiously, without fear of being detected.\textsuperscript{106} However, because online anonymity consists of the ability to control the electronic information used to identify oneself,\textsuperscript{107} and in the context of telecommunications, criminals are indistinguishable from legitimate users of anonymous technology.\textsuperscript{108} While experienced criminals know how to conceal their tracks in cyberspace, anonymous software makes it possible for anyone to erase the marks identifying the source of the communication, so that pinning a person down to a geographic location becomes technically impossible.\textsuperscript{109} Everything on the Internet-from email to an electronic heist\textsuperscript{110} is information; investigators must locate the true source of the communication to connect the hack with a real person in the physical world.\textsuperscript{111} The infrastructure of the Internet, however, does not provide a ready mechanism for tracing the "electronic trail" leading from the crime back to the perpetrator,\textsuperscript{112} and with the lack of communication data when the offender is offline, the "electronic trail" becomes

\footnotesize

\textsuperscript{101} European Convention on Extradition, opened for signature 13 December 1957, ETS No 24 (entered into force 18 April 1960), art 2(1) ("European Convention on Extradition").


\textsuperscript{103} Podgor (n 83) 730.


\textsuperscript{105} Weber (n 104) 425.


\textsuperscript{108} J Riekkinen, ‘Evidence of Cybercrime and Coercive Measures in Finland’ (2016) 13 Digital Evidence and Electronic Signature Law Review 49.

\textsuperscript{109} Riekkinen (n 108) 49.


impossible.113 With much of illegal data access taking place on the Deep Web or the DarkNet,114 a skilled hacker can determine to remain anonymous, this then requires a high level technical expertise tracking which is time-consuming at best, impossible at worst.115 In instances where the hacker is outside the jurisdiction, the process is further compounded with the slow process of obtaining necessary assistance from foreign authorities.116 In instances where the offender is identified, locating the offender makes a matter of normal police work, which can be made easier by obtaining IP addresses, which is then linked with a physical address or location.117 This then serves as a basis for further investigation, but while such information are crucial for a successful investigation, it does not guarantee a breakthrough as several persons may have access to same device and with criminals frequently exploring security vulnerabilities, to take over control of devices and network connections of other persons,118 that marks the end of the investigation.119 The enforcement of Article 3 of the Cybercrime Directive requires the identification of hackers. Unfortunately, the technology underpinning online anonymity creates both legal and technical challenges to such identification.120

Also challenging to the administration of the Cybercrime Directive is evidence-gathering.121 Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established.122 Evidence of illegal data access are dynamic, broad and increasingly a significantly differs from evidence of traditional crime.123 Locating, obtaining and preserving electronic evidence in the investigation of illegal access requires a different tactics from law enforcement than the traditional investigational procedure.124 If they exist, they must first be located through digital investigations, usually in the online environment and with the ever-increasing internet traffic and storage capacity, as well as the duplicability and transferability of computer data there is no shortage of potential electronic evidence, the sources are

---
115 Riekkinen (n 108) 50.
119 Riekkinen (n 108) 52.
123 Appazov (n 122).
numerous, even if finding them may be challenging.\textsuperscript{125} Unfortunately, the electronic nature of the evidence allows for swift destruction, hiding, obfuscation and counterfeiting of available evidence.\textsuperscript{126} Further, there is no starting point for criminal investigation and no immediately identifiable suspect, as the hacker can be anywhere in the world clicking through a device. Potential electronic evidence is often spread over large geographical areas and across jurisdictional borders, and held or controlled by a number of different, sometimes not easily recognisable parties,\textsuperscript{127} even in fortunate situations that all of these digital crime scenes are located inside the jurisdiction in which the investigation is pursued, they may be difficult to find. Investigators may not be able to identify a natural starting place for their investigation, especially if they have no identifiable suspect.\textsuperscript{128} In the age before computers and computer networks, the most central coercive measures for the purposes of evidence collection were those of search and seizure.\textsuperscript{129} While, this intrusive and coercive method is still relevant, its translation into the online environment has not gone unproblematic.\textsuperscript{130} The demand for new measures, together with the emphasis on the rights of the individual, has resulted in considerable increases in the volume and complexity of regulation on coercive measures.\textsuperscript{131} Unfortunately, are not sufficient available tools to take resolve these challenges and the resultant effect is an increasing number of unresolved cases of illegal data access.\textsuperscript{132}

\section*{2.5 CONCLUSION}

Electronic commerce is reliant on the proper functioning of the information system and any attempt to illegal access data made available within the electronic commerce economy which is needed for the successful running of the electronic commerce is viewed as a criminal offence under Cybercrime Directive. Unfortunately, the territorial nature of criminal law and the criminal justice system challenges the enforcement of the Cybercrime Directive and this exposes the electronic commerce economy to abuse and attacks undermines the effectiveness of the Cybercrime Directive. With the states focussed on sovereignty and territoriality, jurisdiction would continue to affect the successful implementation of the Cybercrime Directive, especially in situations when the hacker is from a third country. Along with jurisdictional challenge is the anonymity and evidence-gathering. Anonymity raises because of the architecture of the internet while evidence-gathering from both the architecture and the territoriality of states.

\begin{thebibliography}{99}
\item Podgor (n 83) 730.
\item Brenner (n 121) 78.
\item Riekkinen (n 108) 49.
\item Riekkinen (n 108) 49.
\item Riekkinen (n 108) 50.
\item Riekkinen (n 108) 50.
\end{thebibliography}
CHAPTER 3

ILLEGAL DATA ACCESS AND THE NATIONAL INFORMATION SYSTEM
DIRECTIVE

3.1 INTRODUCTION

Having regards to the importance of networks and information systems; their reliability and security as essential to economic and societal activities, and in particular to the functioning of the internal market, the European Parliament and the Council of the European Union has enacted the 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. The essence of NIS Directive is to ensure a high common level of network and information security by extending required security measures to a broader set of private entities. The NIS Directive aims to ensure a culture of risk management is developed and that information is shared between private and public sectors. Companies are expected to outline the risk and ensure appropriate and proportionate measures to ensure the protection of their networks, further they are required to report to the competent authorities any serious compromise of their networks and information systems. Achieving a resilient and stable high common level of network and information security would guarantee the smooth functioning of the internal market as illegal access is usually the first point for the commission of most cybercrimes.

In order to ensure an adequate protection of data security within the European Union, the Directive creates both territorial and extra-territorial jurisdiction. The NIS Directive covers digital service providers who are established within the member states and those who are not established but transact within the member state. When a service provider is established across many Member States of the European Union, its jurisdiction shall be at the place of its main establishment. A main establishment shall for the purpose of the Directive be the location of the Head Office of the service provider within the Member State. As regards a service provider not located within the boundaries of the European Union but providing electronic commerce within the European Union, the service provider shall designate a representative within any of the Member State of the European Union, where the services are

133 NIS Directive, recital 1.
139 NIS Directive, art 18(1).
140 NIS Directive, art 18(1).
offered and the service provider shall be deemed to be within the jurisdiction of where the representative was established.\textsuperscript{141}

### 3.2.1 SCOPE OF THE NETWORK INFORMATION SYSTEM DIRECTIVE

The scope of the NIS Directive covers operators of essential services and digital service providers,\textsuperscript{142} making use of networks and information systems. Networks and information systems means an electronic communications network;\textsuperscript{143} any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;\textsuperscript{144} and/or digital data stored, processed, retrieved or transmitted by an electronic communication network and by any device which automatically processes any digital data for the purpose of protection, use, protection and maintenance.\textsuperscript{145} Operators of essential services are public and private entities providing services which are essential for the maintenance of critical societal and/or economic activities;\textsuperscript{146} whose provisions depends on networks and information systems and;\textsuperscript{147} upon whom should an incident happen, it would have significant disruptive effects on the provision of that service,\textsuperscript{148} and are referred to in the non-exhaustive list of Annex II of the NIS Directive.\textsuperscript{149} In particular circumstances when an essential service operator provides both non-essential and essential services, member states shall list the essential and non-essential services using the prescribed criteria above.\textsuperscript{150} Notably, the NIS Directive does not define non-essential services. On the other hand, a digital service provider is defined as any legal person that provides a digital service.\textsuperscript{151} A digital service is a service offered at a distance by electronic means at the request of an individual recipient of service\textsuperscript{152} or of businesses at large, meaning online marketplaces, online search engines or cloud computing services.\textsuperscript{153} An online marketplace is a platform which allows consumers and traders to conclude online sales or service contracts with traders, and is the final destination for the conclusion of those contracts either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace,\textsuperscript{154} with the exclusion of online services that serve only as intermediary to third-party services through which a contract can be ultimately be concluded,\textsuperscript{155} as well as online services that compare the price of particular products or services from traders, and then

\textsuperscript{141}NIS Directive, art 18(2).
\textsuperscript{142}NIS Directive, art 4(4),(6).
\textsuperscript{143}NIS Directive, art 4(1)(a).
\textsuperscript{144}NIS Directive, art 4(1)(b).
\textsuperscript{145}NIS Directive, art 4(1)(c).
\textsuperscript{146}NIS Directive, art 5(2)(a).
\textsuperscript{147}NIS Directive, art 5(2)(b).
\textsuperscript{148}NIS Directive, art 5(2)(c).
\textsuperscript{149}NIS Directive, art 4(5).
\textsuperscript{150}NIS Directive, recital 22.
\textsuperscript{151}NIS Directive, art 4(6).
\textsuperscript{152}Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) (Text with EEA relevance), art 1(B).
\textsuperscript{153}NIS Directive, art 4(5).
\textsuperscript{154}NIS Directive, art 4(17).
\textsuperscript{155}NIS Directive, recital 15.
redirect the user to the preferred trader to purchase the product.\textsuperscript{156} Cloud computing services are application stores, which operate as online stores enabling the digital distribution of applications or software programmes from third parties,\textsuperscript{157} with access to a scalable and elastic pool of shareable resources;\textsuperscript{158} while online search engine allows users to perform searches.\textsuperscript{159} However, the NIS Directive excludes small or micro-enterprises from the scope of service providers to be covered under the framework.\textsuperscript{160} Without the definition of “small or micro-enterprises” in the NIS Directive, recourse is made to Commission Recommendation of Micro, Small and Medium-sized Enterprises (SMEs).\textsuperscript{161} SMEs are enterprises which employ fewer than 250 persons and with an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million,\textsuperscript{162} while a small enterprise employs fewer than 50 persons and with an annual turnover and/or annual balance sheet total not exceeding EUR 10 million;\textsuperscript{163} and microenterprises are fewer than 10 employees and with annual turnover and/or annual balance sheet total not exceeding EUR 2 million.\textsuperscript{164} Further excluded from the scope of the NIS Directive, are service providers in sectors that are already regulated or may be regulated in the future by sector-specific EU legal acts that include rules related to the security of networks and information systems.\textsuperscript{165} While, future sector-specific regulations cannot be presumed, the NIS Directive already excluded public communication networks of publicly available electronic services within the meaning of Directive 2002/21/EC, since they are already subject to specific security and integrity requirements laid down in that Directive, as well as trust service providers within the meaning of Regulation (EU) No 910/2014 which are subject to the security requirements laid down in that Regulation.\textsuperscript{166} Electronic service are services normally provided for remuneration, which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society

\begin{flushleft}
\textsuperscript{156} NIS Directive, recital 15.  \\
\textsuperscript{157} NIS Directive, recital 15.  \\
\textsuperscript{158} NIS Directive, art 4(19).  \\
\textsuperscript{159} NIS Directive, art 4(18).  \\
\textsuperscript{160} NIS Directive, recital 53.  \\
\textsuperscript{165} NIS Directive, recital 9.  \\
\textsuperscript{166} NIS Directive, recital 7.
\end{flushleft}
services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.\textsuperscript{167} A combined reading of the NIS Directive, the Framework Directive and the Accompanying Directive would be that the exclusion afforded to public undertaking providing public communication networks or publicly available electronic services\textsuperscript{168} would only apply when they are providing electronic services only\textsuperscript{169} and does not include content of services delivered over electronic over electronic communications networks using electronic communications services, such as broadcasting content, financial services and information society services.\textsuperscript{170}

A further reading of the Art. 2(a) e-Commerce Directive;\textsuperscript{171} Art. 2(a) of Directive 98/48/EC\textsuperscript{172} and Art. 4(5) NIS Directive clearly demonstrates that the provisions of the NIS Directive does apply to service providers within the e-commerce economy. E-commerce service provided under the NIS Directive are referred to as “digital services”\textsuperscript{173} while service providers are referred to “digital service providers”.\textsuperscript{174} While the NIS Directive excludes small and micro-enterprises within the e-commerce sector,\textsuperscript{175} the exclusion does not apply to public communication networks of publicly available electronic services within the meaning of Directive 2002/21/EC when providing e-commerce services.\textsuperscript{176}

3.2.2 DATA SECURITY REQUIREMENT UNDER THE NETWORK INFORMATION SYSTEM DIRECTIVE

The data security requirement of the NIS Directive mandates service providers to ensure an appropriate technical and organisational measure to manage the risks posed to the security of network and information systems having regard to the state of the art technology,\textsuperscript{177} while taking into account the security of systems and facilities,\textsuperscript{178} incident handling,\textsuperscript{179} business

\textsuperscript{168} NIS Directive, recital 7.
\textsuperscript{169} Framework Directive, art 3 (C).
\textsuperscript{173} NIS Directive art 4(5).
\textsuperscript{174} NIS Directive, art 4(6).
\textsuperscript{175} NIS Directive, recital 53.
\textsuperscript{177} NIS Directive, art 16 (1).
\textsuperscript{178} NIS Directive, art 16 (1)(a).
\textsuperscript{179} NIS Directive, art 16 (1)(b).
continuity management;\textsuperscript{180} monitoring, auditing and testing;\textsuperscript{181} and compliance with international standards.\textsuperscript{182} Imperatively the keyword “appropriate and proportionate” was not defined in the Directive but a further reading of Article 16 (1) of the Directive suggests that the interpretation of the keyword “appropriate and proportionate” would have to be interpreted alongside with the phrase “state of the art technology” and “risk” involved, therefore an appropriate and proportionate technical and organisational measure would ensure a level of security commensurate with the degree of risk posed to the security of the digital services being provided.\textsuperscript{183} Risk is any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems.\textsuperscript{184} In implementing a “state of art technology” which is an appropriate and proportionate, technical and organisational measure commensurate with the risk, a service provider is not expected to implement a “state of the art technology” which is financial disproportionate and an administrative burden.\textsuperscript{185} Further, the Directive requires service providers to take measures to prevent and minimise the impact of security incidents within the network and information society in order to ensure continuity of services.\textsuperscript{186}

For the purpose of effective monitoring and supervision, the Directive mandates a service provider to immediately notify the competent authority of any security breach having substantial impact upon the services of the service providers.\textsuperscript{187} Notifications shall include information to enable the competent authority determine the significance of any cross-border impact, but does not subject the notifying party to increased liability.\textsuperscript{188} In determining “substantial impact” the service provider shall take into account the number of users affected by the incident, particularly users relying on the service for the provision of their own services;\textsuperscript{189} the duration of the incident;\textsuperscript{190} the geographical spread with regard to the area affected by the incident;\textsuperscript{191} the extent of the disruption of the functioning of the service;\textsuperscript{192} the extent of the impact on economic and societal activities.\textsuperscript{193} However, the obligation to notify an incident shall only apply where the service provider has access to the information needed to assess the impact of an incident against the parameters referred above.\textsuperscript{194} Where a cross-border incidence occurs, the competent authority in the service provider’s main establishment shall inform other involved member state, who shall in compliance with Union law, or national legislation preserve the service provider’s security and commercial interests as well as the

\begin{flushright}
\textsuperscript{180} NIS Directive, art 16 (1)(c).
\textsuperscript{181} NIS Directive, art 16 (1)(d).
\textsuperscript{182} NIS Directive, art 16 (1)(e).
\textsuperscript{183} NIS Directive, recital 49.
\textsuperscript{184} NIS Directive, art 4(9).
\textsuperscript{185} NIS Directive, recital 53.
\textsuperscript{186} NIS Directive, art 16 (2).
\textsuperscript{187} NIS Directive, art 16 (3).
\textsuperscript{188} NIS Directive, art 16 (3).
\textsuperscript{189} NIS Directive, art 16 (4) (a).
\textsuperscript{190} NIS Directive, art 16 (4) (b).
\textsuperscript{191} NIS Directive, art 16 (4) (c).
\textsuperscript{192} NIS Directive, art 16 (4) (d).
\textsuperscript{193} NIS Directive, art 16 (4) (e).
\textsuperscript{194} NIS Directive, art 16 (4).
\end{flushright}
confidentiality of the information provided. Competent authorities in the main establishment or of the representative and the competent authorities of those other Member States are obliged to cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between the competent authorities concerned and requests to take the supervisory measures. In necessary circumstances and upon consultation with the service provider, the competent authority may inform the public about individual incidents, where the awareness is necessary in order to prevent an incident or to deal with an ongoing incidence. In deciding whether a disclosure should be made, the underlining consideration would be public interest.

The Directive also mandates competent authorities take necessary actions only when they are provided with evidence that the service provider has failed to meet the requirement that was laid down in Article 16 of the Directive. Upon receiving of such evidence, the competent authorities shall request and assess the security of networks and information systems of the service providers inclusive of their documented security policies as well as order a remedy of any failure to comply to meet the requirements laid down in Article 16. Competent authorities are also empowered to take ex-post supervisory measures against the service providers. While, the supervisory role of the competent authorities are outlined in the Directive, the determination for penalties for infringement cases as well as the applicable liability regime, (strict liability or best effort) is to be determined by member states upon adoption of the Directive.

3.4 ILLEGAL DATA ACCESS UNDER THE CYBERCRIME DIRECTIVE AND THE NETWORK AND INFORMATION SECURITY DIRECTIVE

The initial step to correcting the information security crisis is simultaneously securing the most vulnerable points in the electronic commerce economy while raising the average level of security throughout the economy as a whole. While both the Cybercrime Directive and the NIS Directive are relevant for the protection of data against illegal access in the e-commerce economy, there nature and objectives are fundamentally different, so also is the implementation and the addressee for whom the law was enacted. In preventing illegal data access, the Cybercrime Directive established minimum rules concerning the definition of criminal

195 NIS Directive, art 16(6).
197 NIS Directive, art 17(3).
198 NIS Directive, art 16(7).
199 NIS Directive, recital 60; art 17 (1).
201 NIS Directive, art 17 (2)(b).
202 NIS Directive, art 17 (1).
203 NIS Directive, art 17 (1).
offences and introduces tougher sanctions, whereas the NIS Directive prescribes obligations on service providers, and competent authorities.

Illegal data access is a growing problem that must be effectively addressed in the e-commerce economy. Unfortunately, the Cybercrime Directive does not adequately address illegal data access as a result of the hampered enforcement and its reactive approach to data security. Under the Cybercrime Directive, service providers evaluate vulnerabilities and damages after an attack. With the addition of the NIS Directive, service providers would have to take a proactive approach to data security to ensure the security of their networks against illegal access through the implementation of an appropriate and proportionate security measure, which is inclusive of identification and fixing of data security and vulnerabilities before the hacker locates the security holes.

The Network and Information Security Directive, provides a clear and enforceable mechanism for dealing with the issue of extra-territorial jurisdiction than the Cybercrime Directive. The Cybercrime Directive clearly establishes an extra-territorial jurisdiction when there are sufficient facts to assume personal and subject matter jurisdiction. In circumstances where the hacker is domiciled outside the territorial borders of the member state where the effect of the illegal access is felt, the member states are to assume jurisdiction for prosecuting such an offence. However, the same technology that gives global consumers access to a virtual Nordstrom’s shoe department also allows hackers to illegal access data across international borders that are difficult to successfully prosecute as a result of state sovereignty. This form of jurisdiction is not effective in regulating the illegal data access. Whereas with the NIS Directive, the extra-territoriality jurisdiction requires that service providers ensure the

---


207 N Sukhai, ‘Hacking And Cybercrime’ <http://delivery.acm.org/10.1145/1060000/1059553/p128-sukhai.pdf?ip=137.56.80.216&id=1059553&acc=ACTIVE%20SERVICE&key=0C390721DC021FF%2E8E8A7FC83EB1C6A0%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFTOKEN=55588862&__acm_=1482500490_8a757b4f3a22a4ba2be952533c01901e> accessed 13 January 2017.


211 NIS Directive, art 16.


215 E Schneiderman and R Kornreich, ‘Personal Jurisdiction and Internet Commerce’ (1997) N.Y.L.J.
appointment of a representative within the Union in any or one of the member states where its services are being offered.\textsuperscript{216} With the appointment of representatives by service providers, member states need not worry about enforcing the NIS Directive in circumstances where service providers are not within the territorial borders of the Union, as their representative must be located within the Union.\textsuperscript{217} An effective enforcement of the extra-territoriality provision of the NIS Directive would cumulate in the provision of security for data and stem down illegal data access by hackers within the electronic commerce economy. Unfortunately, while this sounds interesting, the lapse occasioned by the exclusion of small and micro-enterprises may be the Achilles’ heel of the legislation, as interconnectivity of the information system is massive and an information system is as strong as its weakest point.\textsuperscript{218} In this way, the NIS Directive can aptly supplement the extra-territorial jurisdiction arising from the implementation of the Cybercrime Directive.

Under the Cybercrime Directive, evidence-gathering is a responsibility that solely resides with the investigating and prosecutorial authorities of each member state of the Union.\textsuperscript{219} The competent authority under the Cybercrime Directive has to gather sufficient evidence against the hacker in order to enforce the criminal sanctions against the hackers.\textsuperscript{220} Under the NIS Directive there is a paradigm shift in evidence-gathering. The NIS Directive scaffolds\textsuperscript{221} entities into developing a responsible security risk management, thereby holding them accountable for the security of their networks and information systems.\textsuperscript{222} In order to guarantee accountability, the Directive requires Member States to designate one or more national competent authority on the security of network and information systems to monitor compliance of service providers at the national level.\textsuperscript{223} While the NIS Directive does not expressly provide for a documentation requirement of compliance by service providers, except for a reference to documented security policies made in Article 17(2) the Directive, there were references notification obligation to the competent authority which can only be complied with by having a well-documented security process and procedures.\textsuperscript{224} Service providers are required to send the receipt of incident notification to competent authority of the Computer Security Incident Response Teams (CSIRTs).\textsuperscript{225} In case a Member State decides that CSIRTs shall not receive notifications, the CSIRTs shall, to the extent necessary to fulfil their tasks, be granted access to data on incidents notified by service providers pursuant to Article 16(3) and (6) of the NIS

\textsuperscript{216} NIS Directive, art 18(2).
\textsuperscript{217} NIS Directive, art 18(2).
\textsuperscript{218} Miguel and Others (n 15) 58.
\textsuperscript{219} Brenner (n 121) 78.
\textsuperscript{220} Riekkinen (n 108).
\textsuperscript{221} Scaffolding is an education theory term which involves facilitating an individual’s learning by giving them as little assistance as possible while at the same time ensuring their success. Therefore, the key is to let the learner teach herself while monitoring her progress and providing only as much redirection and correction as needed to keep the learner’s progress on target. See I Verenikina, ‘Understanding Scaffolding and the ZPD in Education Theory’ (2003) \url{http://aare.edu.au/03pap/ver03682.pdf} accessed 16 January 2017. In effect, traditional Socratic teaching methodology, if used correctly, is an example of scaffolding in action—a professor assists the student in teaching herself.
\textsuperscript{222} NIS Directive, art 17.
\textsuperscript{223} NIS Directive, art 8(1)(2).
\textsuperscript{224} NIS Directive, art 1(d).
\textsuperscript{225} NIS Directive, recital 32.
Directive. Upon the provision of such notification, the competent authority can request conduct an assessment of the security of the service providers. By the notification obligations under the Directive, a service provider would have to document evidential proofs of compliance with the security requirement of the Directive. This documented evidence is then gathered by competent authorities or handed over by the service provider to the competent authority if need arises to assess the liability or otherwise of the service providers.

In the implementation of the Cybercrime Directive, the anonymity of the offender hampers the enforcement of criminal sanctions against a hacker. Under the NIS Directive, addressees are clearly identifiable and their roles are clearly spelt out in the Directive. The service providers as primary parties upon whom the burden to ensure the protection of the networks and information systems are clearly identifiable and ascertainable. In particular to the protection of the e-commerce economy, the NIS Directive clearly identifies the addressee as digital service providers which comprises of online marketplaces; online search engine and cloud computing services excluding small and micro-enterprises. This clarity provides a certainty of persons who can be held accountable for non-compliance. Even for overseas service providers located outside the territory of the Union, the requirement for appointing a representative to be domiciled within any of the Member State would compel the overseas service providers to comply with the provisions of the Member State’s national law implementing the Directive through their designated representatives. However, the status of the designated representative is unclear, especially as to whether it should be a subsidiary of the service provider or whether a separate and independent entity, that would be determined by National Laws.

Unfortunately, the NIS Directive lost the opportunity to create a union level of security requirement by the exclusion of the small and micro-enterprises from the requirement. The internet is an inter-connected global system and the transfer of data within the electronic commerce economy defies the classification of the small or micro-enterprises especially because the data required by the included organisations under the NIS Directive is usually same required by excluded organisations in an e-commerce transaction. A breach into the network

226 NIS Directive, art 10 (2).
227 NIS Directive, art 17(2).
228 NIS Directive, art 16(3); 17(2).
229 Buono (n 205) 103.
231 NIS Directive, art 1(d) 32.
234 NIS Directive, art 18(2).
235 The determination of the status would be up to the Member State when transposing the Directive into National Law. It would seem that the legislators intended that the representative has an obligation and this is best fulfilled by ensuring that the representatives are subsidiaries rather than independent entities.
237 In an e-commerce transaction, usually there is the request for financial information, personal information and location information. Irrespective of the type of service provider in question, the same information is usually required and should a hacker access the information from the excluded class, the fruit of the efforts of the included class of service providers is watered down by such, as the hacker can already cause damage to the consumers and users of within the electronic commerce sector.
and information system of a small or micro-enterprise which is excluded under the directive can still cause damage to the users and consumers within the electronic commerce.

3.5 CONCLUSION

The electronic commerce economy is undoubtedly reliant on the network and information system and a failure of the system would definitely have an impact on the transactions and the services that are carried out through e-commerce platforms. Illegal access is also a breach of the network and security information system, hence once this breach occurs through illegal access, there is an inevitably intrusion into the data of persons. The security of networks is therefore crucial to the protection of the electronic commerce economy in order to ensure its continuous performance. The Network and Information System Directive is therefore a welcome addition to the protection against the illegal access of data by hackers and nefarious persons who are interested in committing crimes by accessing the data of innocent persons within the e-commerce economy. While, it is quite true that no security system is perfect, the need to stay up to date with protection is a sure a great addition to protecting the e-commerce economy as a network security is as strong as its weakest point as the NIS Directive assumes that hackers would always keep at developing strategies to illegally access data. Also with the shift from the legislative approach hinged on “security through obscurity” by creation of public awareness in cases of continuous breach of the information system, assurance and trust is created within the e-commerce economy, especially for the consumer of goods and services who often express concern about illegal data access and data security breaches. This would also serve as an incentive to service providers to take necessary cautionary measures against security breaches, since most Service Providers are keen on their public perception.

---

239 Miguel and Others (n 15) 61.
241 “Security through obscurity” is the idea that adequate security should be driven by the subjective beliefs of the owners of a system regarding the security of that system. Therefore, if the owners believe that particular security flaws of the system are not widely known or inconsequential, then attackers are unlikely to find and exploit them as long as the owners keep information about the vulnerabilities secret. See Matwyshyn (n 204) <http://poseidon01.ssrn.com/delivery.php?ID=930086105106031122021010068001096029046084048036031020026006114111020029024096116023032062030033112029051065099024001111090118082049003029117095112120116125126084010056000085092004090125111106017006115082007118089080121005085108067006101013003002&EXT=pdf> accessed 18 January 2017.
242 NIS Directive, art 16(7).
CHAPTER FOUR
ILLEGAL DATA ACCESS AND GENERAL DATA PROTECTION REGULATION

4.1 INTRODUCTION

A right to protection of an individual’s private sphere against intrusion from others, especially from the state, was laid down in an international legal instrument for the first time in Article 12 of the United Nations (UN) Universal Declaration of Human Rights (UDHR) of 1948 on respect for private and family life.\(^{243}\) Subsequently, the European Convention on Human Rights (ECHR) was enacted in 1950, which entered into force in 1953 as a legislation to guarantee the rights and freedom of citizens and residents of the Members States who are members of the Council of Europe.\(^{244}\) Member States of the European Union are also members of the Council of Europe,\(^{245}\) hence they are saddled with the responsibility of complying with the obligations under the ECHR. Under the ECHR the right to protection of personal data forms part of the rights protected under Article 8 of the ECHR, which guarantees the right to respect for private and family life, home and correspondence and lays down the conditions under which restrictions of this right are permitted.\(^{246}\) However, in order to deepen the rights of Article 8 as enshrined the ECHR, the European Union further enacted the Data Protection Directive\(^ {247}\). The Directive was enacted upon the premise that the free movement of goods, capital, services and people within the internal market required the free flow of data which could not be realised unless the Member States could rely on a uniform high level of data protection.\(^ {248}\) As the aim of adopting the Data Protection Directive was harmonisation\(^ {249}\) of data protection law at the national level, the directive afforded a degree of specificity comparable to that of the then existing national data protection laws.\(^ {250}\)

However, measured against the innovation cycle of the modern information society, the Data Protection Directive appears to be an ancient regulatory instrument\(^ {251}\) and it was therefore against this background that the Commission took the initiative that led to the enactment of the General Data Protection Regulation (GDPR).\(^ {252}\) With the passage of the GDPR by the

---


\(^{247}\) Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

\(^{248}\) European Union Agency for Fundamental Rights, (n 244).

\(^{249}\) Data Protection Directive, recitals 1, 4, 7 and 8.

\(^{250}\) European Union Agency for Fundamental Rights (n 244).


\(^{252}\) General Data Protection Regulation.
European Parliament, it becomes essential to consider data protection in the e-commerce economy in light of the new Regulation since the Directive would soon be repealed upon the commencement of the Regulation in May 2018. Under European Union law, a "Regulation" is directly binding upon Member States\(^{253}\) and thus have direct effect in all Member States upon the commencement date.\(^{254}\)

The GDPR is vital legal instrument in the protection of personal data of consumers and users within the electronic commerce sector, since it also applies to service providers in the electronic commerce sector.\(^{255}\) The GDPR provides for rules relating to the protection of natural persons with regard to the processing of personal data and free movement of personal data\(^{256}\) in order to safeguard against threats to the proper functioning of the internal market by putting in place appropriate safeguards against such threats through the imposing of responsibilities and sanctions on controllers and processors.\(^{257}\) This perspective shift is quite instrumental to the protection of the e-commerce economy against hackers, as the various challenges arising from the prescription and enforcement of the Cybercrime Directive could be circumvented by GDPR.

4.2.1 SCOPE OF THE GENERAL DATA PROTECTION REGULATION

The GDPR is intended to address the protection of natural persons\(^{258}\) in regards to the processing of personal data,\(^{259}\) having taken into consideration, the rapid technological developments and globalisation and the need to create trust\(^{260}\) which is essential to the development of the digital economy\(^{261}\) while harmonizing data protection among member states.\(^{262}\)

The GDPR relates to personal data of natural persons. "Personal data" is any information relating to an identified or identifiable natural person who is referred to as data subject; an identifiable natural person is one who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person.\(^{263}\) It also refers to the means of identifying individuals on the basis of an identification number, location data, and online identifier.\(^{264}\) An identifier must be associated with a 'lookup identifiers' (L-identifiers) that is, a register, directory, or table in which the connection between the identifier

\(^{254}\) Treaty of the Functioning of the European Union, art 288 (2).
\(^{255}\) General Data Protection Regulation, would easily suggest that service providers within the electronic commerce are included for the purpose of conforming with the Regulation, recital 6, 7; art 1(1); 2(1), (2).
\(^{256}\) General Data Protection Regulation, art 1(1).
\(^{257}\) General Data Protection Regulation, recital 13.
\(^{258}\) General Data Protection Regulation, recital 14.
\(^{259}\) General Data Protection Regulation, art 1(1) & (2).
\(^{260}\) General Data Protection Regulation, recital 6.
\(^{261}\) General Data Protection Regulation, recital 7.
\(^{262}\) General Data Protection Regulation, recital 3.
\(^{263}\) General Data Protection Regulation art 4 (1).
and a named individual can be looked up,\textsuperscript{265} as well as ‘recognition identifiers’ (R-identifiers), that is, data that allow an individual to be recognised as a previously known individual, without (necessarily) being able to associate the identifier with a named individual.\textsuperscript{266} Such R-identifiers can be combined with other data to identify the individual by name (or otherwise uniquely pinpoint the individual), in which case the R-identifier also counts as personal data.\textsuperscript{267} Further, the protection afforded by the GDPR is extends to the processing of personal data wholly or partly by automated means or non-automated means which form part of a relevant filing system.\textsuperscript{268}

The personal scope of the GDPR includes, the data subject, who is the natural person, who is identified or identifiable;\textsuperscript{269} the controller and the processor. The “Controller” could be a natural person or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;\textsuperscript{270} while the Processor is natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.\textsuperscript{271} Notably, the definition of natural persons does not apply to deceased persons and member states are at liberty to regulate the processing of data as regards deceased persons.\textsuperscript{272} Irrespective of the nationality or place of residence of the natural person, controllers and processors are bound to apply the provisions of the GDPR.\textsuperscript{273} Importantly, the GDPR does not apply to legal persons and controllers and processors are not bound to apply the GDPR in the handling of data belonging to legal persons.\textsuperscript{274}

As regards the territorial scope, the GDPR applies to processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.\textsuperscript{275} This expands the scope to include the activities of the processor that processes personal data on behalf of the data controller within the Union.\textsuperscript{276} Establishment implies the effective and real exercise of activity through stable arrangements,\textsuperscript{277} specifically for the controller, the main establishment of a controller in the Union should be the place of its central administration in the Union, unless decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment.\textsuperscript{278} Further, the territorial scope is extended to controllers and

\begin{itemize}
  \item \textsuperscript{265} R Leenes, ‘Do They Know Me? Deconstructing Identifiability’ (2008) 4 University of Ottawa Law Technology Journal 135.
  \item \textsuperscript{266} Koops (n 264) 258.
  \item \textsuperscript{267} Koops (n 264) 260.
  \item \textsuperscript{268} General Data Protection Regulation, art 2(1).
  \item \textsuperscript{269} General Data Protection Regulation, art 4 (1).
  \item \textsuperscript{270} General Data Protection Regulation, art 4(7).
  \item \textsuperscript{271} General Data Protection Regulation, art 4(8).
  \item \textsuperscript{272} General Data Protection Regulation, recital 27.
  \item \textsuperscript{273} General Data Protection Regulation, recital 14.
  \item \textsuperscript{274} General Date Protection Regulation, recital 36.
  \item \textsuperscript{275} Voss and W Gregory, ‘European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting’ (2017) 72 Business Lawyer 221.
  \item \textsuperscript{276} General Data Protection Regulation, recital 22.
  \item \textsuperscript{277} General Data Protection Regulation, recital 27.
  \item \textsuperscript{278} General Data Protection Regulation, recital 36.
\end{itemize}
processors not established in the Union but whose processing activities are related to data subjects in the Union, for the purpose of offering of goods and services, irrespective of the payment status of the data subject or monitoring behaviours of data subjects taking place within the Union. In such circumstances, the controller or processor shall appoint a representative within the Union.

Undoubtedly, the GDPR applies to the e-commerce economy since the e-commerce economy processes personal data of its various consumers. However, since the exchange of goods the within the e-commerce sector is not limited to natural persons but inclusive of legal persons, the protection afforded to natural persons by the GDPR would not be applicable to legal persons, especially in cases of business to business transactions where the consumer and the service providers are legal persons. Also, included as the objective of the GDPR is the need for a strong and more coherent data protection framework in the Union, backed by strong enforcement as a result of the need to create trust that enhance the growth of the digital economy.

4.2.2 DATA SECURITY REQUIREMENT UNDER THE GENERAL DATA PROTECTION REGULATION

The data security requirement under the GDPR requires the controller and the processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to risk. In putting in place the required technical and organisational security measures, both the controller and the processor must consider the state of art, the cost of implementation, the nature, scope context and purpose of processing as well as risk of varying

---

279 General Data Protection Regulation, art 3(2) (a).
280 General Data Protection Regulation, art 3(2) (b).
Recital 24 of the Regulation further explains monitoring for the purpose of Article 3(2)(b) thus: “The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.”
281 General Data Protection Regulation, art 27.
284 General Data Protection Regulation, recital 14.
286 Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced, recital 7 (7).
287 General Data Protection Regulation, art 32.
likelihood and severity for the rights and freedoms of natural persons.\textsuperscript{288} For the purpose of clarity, the GDPR provides appropriate and specific standards as to security actions which might be considered as appropriate to the risk, which includes; the pseudonymisation and encryption of personal data;\textsuperscript{289} the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;\textsuperscript{290} the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;\textsuperscript{291} a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.\textsuperscript{292} In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.\textsuperscript{293} However, controllers and processors may also show compliance with the above provisions by adhering to prescribed code of conducts\textsuperscript{294} and/or an approved certification\textsuperscript{295} described in the GDPR.\textsuperscript{296}

In order to ensure compliance and supervision, the GDPR further requires the Member States to establish a supervisory authority which shall be saddled with the responsibility of ensuring compliance with the provisions of the GDPR.\textsuperscript{297} With the establishment of a competent authority, the GDPR requires that a controller shall notify both the supervisory authority and the data affected subject on an occasion of a personal data breach\textsuperscript{298} upon receiving such a notification from the processor.\textsuperscript{299} A “personal data breach” is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.\textsuperscript{300} Such notification shall be by the controller, without undue delay and not exceeding 72 hours upon being aware of the personal data breach.\textsuperscript{301} In circumstances where the notification to the supervisory authority is made after 72 hours, it shall be accompanied by reasons for the delay.\textsuperscript{302} Since the GDPR provides for a layered notification system\textsuperscript{303} a controller may not notify the supervisory in circumstances where the personal data breach is unlikely to result in risk to the rights and freedoms of natural persons.\textsuperscript{304} “Risk to the rights and freedoms of natural persons” is described as any breach that

\textsuperscript{288} General Data Protection Regulation, art 32.
\textsuperscript{289} General Data Protection Regulation, art 32 (1)(a).
\textsuperscript{290} General Data Protection Regulation, art 32 (1)(b).
\textsuperscript{291} General Data Protection Regulation, art 32 (1)(c).
\textsuperscript{292} General Data Protection Regulation, art 32 (1)(d).
\textsuperscript{293} General Data Protection Regulation, art 32 (2).
\textsuperscript{294} General Data Protection Regulation, art 40.
\textsuperscript{295} General Data Protection Regulation, art 42.
\textsuperscript{296} General Data Protection Regulation, art 32 (3).
\textsuperscript{297} General Data Protection Regulation, art 51 (1).
\textsuperscript{298} General Data Protection Regulation, art 33(1).
\textsuperscript{299} General Data Protection Regulation, art 33(2).
\textsuperscript{300} General Data Protection Regulation, art 4 (12).
\textsuperscript{301} General Data Protection Regulation, art 33(1).
\textsuperscript{302} General Data Protection Regulation, art 33 (1).
\textsuperscript{304} General Data Protection Regulation, art 33(1).
may lead to physical, material or non-material damage and inclusive of circumstances where the processing may give rise to theft or fraud, financial loss, damage to the reputation, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage. Minimally, the notification to the supervisory authority must include a description of the nature of the personal data breach, including the number and categories of data subjects and personal data records affected; provide the data protection officer’s contact information; description of the likely consequences of the personal data breach; and describe how the controller proposes to address the breach, including any mitigation efforts.

If not all information is available at once, it may be provided in phases, while also documenting the personal data breach, its effect and remedial action taken. When a data processor experiences a personal data breach, it must notify the controller. Further to the notification of the supervisory authority, a controller would still have to inform the data subjects in circumstances where the breach is likely to result in high risk for the rights and freedoms of natural persons, such communication shall be without undue delay.

In line with the principle of transparency, notification to the data subject must be in a clear and plain language and must contain all information as required by the GDPR in Article 33(3) (b); (c) and (d). Importantly, the GDPR created exceptions to the additional and obligatory duty of notifying the data subjects in circumstances where the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise. Where notification would involve disproportionate effort, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. In circumstances where the controller has notified the supervisory authority of the breach but not the data subjects, the supervisory authority shall determine whether the data subjects be informed based on the assessment of high risk to the rights and freedom of the natural persons. Assuming the controller has notified the appropriate supervisory authority of a personal data breach, its discretion to notify data subjects is limited by the DPA’s ability, under Article 34(4), to require notification or conversely to determine it is unnecessary under the circumstances.

---

305 General Data Protection Regulation, recital 75.
306 General Data Protection Regulation, art 33 (3)(a).
307 General Data Protection Regulation, art 33 (3)(b).
308 General Data Protection Regulation, art 33 (3)(c).
309 General Data Protection Regulation, art 33 (3)(d).
310 General Data Protection Regulation, art 33 (4).
311 General Data Protection Regulation, art 33 (5).
312 General Data Protection Regulation, art 34 (1).
313 General Data Protection Regulation, recital 39.
314 General Data Protection Regulation, art 34 (2).
315 General Data Protection Regulation, art 34 (3) (a).
316 General Data Protection Regulation, art 34 (3) (b).
317 General Data Protection Regulation, art 34 (3) (c).
318 General Data Protection Regulation, art 34 (4).
The establishment of an extra-territorial jurisdiction of the GDPR is similar to that of the NIS Directive which requires the appointment of the representatives for service providers who are not established but transact within the member state. In cases where both the data controller and processor are not within the union but services are directed towards the members states of the Union, they are required to appoint representatives; this would definitely ensure the effectiveness of the extra-territorial jurisdiction and ensure compliance with the data security and enforcement by the competent authorities. In circumstances, where the processor is located outside of the Union, the data controller is still obliged to ensure that the security requirement is complied with, as the GDPR mandates that controllers only engage processors who have ensured compliance with the data security requirement. Such appointment by the controller shall be a written contract and shall also include the implementation of the data security requirement. Hence, a processor who does not direct services towards the Union but is employed by a controller within the Union is still bound by the written contract reflecting the data security provision of the GDPR. While, the GDPR is still awaiting commencement, the exclusion of legal persons within the e-commerce economy when transacting with other legal persons may hinder the effectiveness of the GDPR as controllers or processors are not obliged to ensure data security. This is particularly of concern to business-business (B2B) e-commerce transactions as there are no determinants that the data exchange between legal persons differ from those collected in a business-consumer (B2C) transaction. Unlike the Cybercrime Directive, the GDPR extra-territorial arrangement is better organised to enhance the resilience of data security against illegal data access than the Cybercrime Directive in prosecuting hackers as a means of ensuring data security against illegal access and with no world court to prosecute illegal access, the extra-territorial effect of the Cybercrime Directive is still subject to sovereignty of third countries.

Prosecuting illegal data access as a crime requires the availability of evidence by the prosecuting authority. In order to secure conviction, which is the desired outcome of the Cybercrime Directive, the prosecuting authority must have sufficient evidence against the hacker, as the presumption of innocence is applicable to every criminal trial in spite of the difficulties of prosecutorial authorities face in evidence gathering. Conviction can only be secured by evidence-gathering which leads to provenance of guilt of the accused, for which a
conviction is handed down. With the GDPR, the approach is fundamentally different, as there is a strong emphasis on accountability by the controller and the processor.\textsuperscript{328} This accountability requirement is a presumption of guilt, until the controller or processor can prove innocence. The GDPR requires an evidentiary proof of compliance which is inclusive of data security measures,\textsuperscript{329} privacy impact assessments,\textsuperscript{330} audits,\textsuperscript{331} policy reviews,\textsuperscript{332} book-keeping and appointment of data protection officer.\textsuperscript{333} Further, there must be proper documentation of the technical and organisational security measures undertaken by the controller and processor in compliance with the data security requirement,\textsuperscript{334} which are also inclusive of keeping of an internal register documenting such personal data breaches, its effects and remedial action taken.\textsuperscript{335} Non-compliance with the record-keeping obligation can lead to sanctions on controllers and processors.\textsuperscript{336} In order to ascertain whether there has been a breach or compliance with the GDPR the supervisory authority is empowered to request for evidentiary proof which shall be supplied by the controller or processor and/or any of whom was addressed by the supervisory authority.\textsuperscript{337} The effect of this record-keeping obligations under the GDPR is the availability of evidence such that the supervisory authority can effectively administer the GDPR while also being furnished with enough evidence to sanction a non-compliant service provider.\textsuperscript{338} This various record-keeping obligations on the service providers and the accessibility of supervisory authorities to those evidence ensures that the GDPR can be enforced with fair judgment. Also the record-keeping obligation is of strict liability, such that non-compliance with this obligation is subject to administrative fines.\textsuperscript{339}

Enforcing criminal sanctions requires the apprehension of the offender;\textsuperscript{340} under the Cybercrime Directive, like every other criminal statute the offender is usually unknown but the nature of illegal access as an internationalized crime which can occur over multiple jurisdiction and without a natural crime scene makes it more complex and demanding. Under the GDPR, all persons are ascertainable and identifiable with roles clearly defined.\textsuperscript{341} The controller and the processor upon whom the duty lies to ensure the security of data is clearly spelt out. Admittedly, developing technology can lead to intricacies in the identification of controllers and processors. Again the GDPR tries to objectively balance such circumstances, by providing for joint controllers,\textsuperscript{342} who shall ensure compliance with the data security requirement. At other times, when circumstantial evidence proves that certain authorities allowed the

\textsuperscript{328} General Data Protection Regulation, recital 74.
\textsuperscript{329} General Data Protection Regulation, recital 74, 78, 82; art 25.
\textsuperscript{330} General Data Protection Regulation, art 35.
\textsuperscript{331} General Data Protection Regulation, art 28 (3) (h); 39.
\textsuperscript{332} General Data Protection Regulation, art 24 (1); 35(11).
\textsuperscript{333} General Data Protection Regulation, art 37.
\textsuperscript{334} General Data Protection Regulation, art 30.
\textsuperscript{335} General Data Protection Regulation, art 33 (5).
\textsuperscript{336} General Data Protection Regulation, art 83.
\textsuperscript{337} General Data Protection Regulation, recital 82.
\textsuperscript{338} General Data Protection Regulation, art 83.
\textsuperscript{339} General Data Protection Regulation, art 83.
\textsuperscript{340} Riekkinen (n 108) 52.
\textsuperscript{341} General Data Protection Regulation, art 4.
\textsuperscript{342} General Data Protection Regulation, art 26.
processing operation without the instructions from the initial controller, such authorities shall be deemed as factual controller.\textsuperscript{343} This distinction of persons is essential to enforcement as competent authorities can fully hold an erring party accountable for a breach of the data security requirement under the GDPR, whether they expressly signed up as a controller and/or processor or not.

While the GDPR and NIS Directive both create data security obligations, the purpose of each legislation is fundamental different. The NIS Directive was enacted to improve security of the internet and make private networks and information systems on which the digital society relies\textsuperscript{344} as well as to make the online environment more trustworthy,\textsuperscript{345} explicating stating that there is a need to ensure the ability of networks and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by or accessible via that network and information systems.\textsuperscript{346} The GDPR on the other hand was enacted to protect individuals, that is, natural persons and not legal entities, with respect to their personal data processing.\textsuperscript{347} Interestingly, the security obligation under both legislations do not differ. A perusal of the both legislations reveals that the security obligations do not differ from each, however, the yardstick for arriving at compliance does differ. Under the NIS Directive service providers are to take into consideration the security of facilities; incident handling; business continuity management; monitoring, auditing and testing; compliance with international standards,\textsuperscript{348} while the GDPR requires consideration of the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.\textsuperscript{349} However the difference in the yardstick to be considered does not lead to a lesser requirement for data security.

Notwithstanding the similarity of the data security requirement and the applicability to e-commerce players, both the NIS Directive and the GDPR made fundamental exemptions of different applicable players. The NIS Directive left a significant gap by the exclusion of small and micro-enterprises.\textsuperscript{350} In the e-commerce economy, the use of personal data for electronic transaction is generally same irrespective of the type of service provider, hence same protection against an unlawful intrusion should be required of all service providers. Excluding service providers who have been categorized into small and micro-enterprises is a gap that can be exploited by hackers, as failure to provide adequate security could be an invitation to hacking.\textsuperscript{351} However, the GDPR does not take this approach as it requires all service providers

\textsuperscript{343} European Union Agency for Fundamental Rights (n 244).
\textsuperscript{346} Weber and Studer (n 344) 720. See also NIS Directive, art 4(2).
\textsuperscript{347} Voss and Gregory (n 276) 225.
\textsuperscript{348} NIS Directive, art 16.
\textsuperscript{349} General Data Protection Regulation, art 32.
\textsuperscript{350} General Data Protection Regulation, recital 53.
to ensure compliance with the data security requirement.\textsuperscript{352} As regards the GDPR, the scope of protection afforded to natural persons does not apply to legal persons.\textsuperscript{353} The exclusion of legal persons from the scope of persons who are excluded from having the assurance of a secured data, is particularly troubling for the e-commerce because of its ability to facility B2B transactions which sometimes require the use of personal data.\textsuperscript{354} The exclusion of legal persons is also from the GDPR does not however exist under NIS Directive and this is particularly crucial for the e-commerce economy since both the GDPR and the NIS Directive are applicable. A B2B transaction though exempted from the GDPR data security requirement is still covered by the NIS Directive. With the difference in personal scope, both the GDPR and NIS Directive enhances the resilience of security systems in the e-commerce economy.

The NIS Directive does not expressly provide for a documentation requirement of compliance by service providers, except for a reference to documented security policies.\textsuperscript{355} However, there were several references to the notification requirement to the competent authority which can only be complied with by having a well-documented security process and procedures.\textsuperscript{356} While the inferences under NIS Directive may leave room for doubts as to when the service providers should keep-record and what type of liability the regime does apply,\textsuperscript{357} the GDPR provides an explicit documentation requirement.\textsuperscript{358} Unfortunately, the record-keeping obligation does not apply to enterprises organisations employing fewer than two hundred and fifty persons unless the processing is not occasional.\textsuperscript{359} With the ability to fuse the responsibilities of the supervisory authority under the GDPR and the NIS Directive;\textsuperscript{360} this fusion can effectively cover the gaps in the NIS Directive as supervisory authorities would be able to require compliance with the strict liability procedure under the GDPR, since the NIS Directive is a minimal provision and does not stop member states from enacting stricter provision.\textsuperscript{361} The exclusion from the record-keeping requirement is however undesirable as a large number of e-commerce services would fall into this category,\textsuperscript{362} but with caveat of “continuous processing” many service providers may still have an obligation to compile with the record-keeping requirement.

Further to the record-keeping requirement, there is a notification duty under the GDPR and the NIS Directive in cases of data breaches. The data breach notification under the GDPR is a layered system that provides for many instances in which the controller may avoid such notification.\textsuperscript{363} This is in contrast to the NIS Directive which requires a service provider to

\textsuperscript{352} General Data Protection Regulation, recital 13.
\textsuperscript{353} General Data Protection Regulation, art 4 (1).
\textsuperscript{354} Bhalekar and Others (n 238) 25.
\textsuperscript{355} NIS Directive, art 17(2).
\textsuperscript{356} General Data Protection Regulation, recital 32; art 1(d).
\textsuperscript{357} Weber and Studer (n 344) 722.
\textsuperscript{358} General Data Protection Regulation, art 1(d); recital 82.
\textsuperscript{359} General Data Protection Regulation, art 1(d), 30(5).
\textsuperscript{360} NIS Directive, recital 6.
\textsuperscript{361} Weber and Studer (n 344) 718.
\textsuperscript{362} De Hert and Papakonstantinou (n 303).
immediately notify the competent authority without undue delay of any incident having substantial impact.\textsuperscript{364}

Another striking distinction is that while the NIS Directive does lay down obligations as to data security implementation like the GDPR, the NIS Directive lacks an administrative sanction procedure, which is important to compelling of the obedience of service providers. Under the GDPR, in circumstances where the service provider has failed to implement an appropriate technical and organisational measure in accordance with the provisions of the GDPR, there would liabilities on such a service provider. The supervisory authority shall impose and administrative fine up to 10,000,000 Euros or in case of an undertaking 2\% of the total worldwide annual turnover of the preceding financial year, whichever is higher.\textsuperscript{365} Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, a consumer has a right to an effective judicial remedy when there has been a breach of this duty by the service provider;\textsuperscript{366} and is also entitled to compensation from the controller or processor when such breach leads to either a material or non-material damage.\textsuperscript{367} Such proceedings can be brought before the courts of the member state where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject resides unless the controller or processor is a public authority of Member State acting in the exercise of its public powers.\textsuperscript{368} The determination of non-compliance with the data security requirement is an objective test, as the supervisory authority would be expected to consider the parameters stated in the GDPR.\textsuperscript{369}

4.4 CONCLUSION

Evidently, the GDPR is a great addition in the protection against illegal data access, however, it should be noted that the GDPR is not just a compendium for rights and obligations but also imposes sanctions and penalties which of course has penal effect on service providers. Unlike the Cybercrime Directive, that seeks to punish the intruder, the GDPR seeks to penalise the controller and processor who has failed in its obligations to prevent illegal access data. This is essential in order to strengthen the enforcement. Under the GDPR, penalties could be inclusive of administrative fines, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this GDPR.\textsuperscript{370} Further, the GDPR also allows member states to lay down the rules on criminal penalties for infringements of the GDPR, inclusive of infringements of national rules adopted pursuant to and within the limits of this GDPR. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this GDPR.\textsuperscript{371} While the phrase “criminal penalties” have been used by the draftsmen of the GDPR, it does not seem that the reference is in terms of the machinery of the

\begin{footnotesize}
\begin{enumerate}
\item NIS Directive, art 16(3).
\item General Data Protection Regulation art 83(4)(a).
\item General Data Protection Regulation, art 79 (1).
\item General Data Protection Regulation, art 82(1).
\item General Data Protection Regulation, art 79 (2).
\item General Data Protection Regulation, recital 87; art 32(1).
\item General Data Protection Regulation, recital 148.
\item General Data Protection Regulation, recital 149.
\end{enumerate}
\end{footnotesize}
criminal justice system which requires prosecutions and trials but that the supervisory authority would have capacity to issue effective, proportionate and dissuasive sanctions\(^{372}\) which would be of penal effect such as is been meted out under the criminal justice system.\(^{373}\) Further with the GDPR operates as an administrative law which need does not operate under the criminal justice system for sanctioning of non-compliant service providers within the e-commerce economy and should not be challenged by the jurisdiction, anonymity and evidence gathering.

Notwithstanding the effectiveness of the GDPR in protecting the e-commerce economy better than the Cybercrime Directive, the GDPR does also create certain vacuums, especially in the data notification, applicability to natural persons to the exclusion of legal persons and record-keeping. However, with the introduction of the NIS Directive, those vacuums are adequately covered; unfortunately the exclusion organization which employs two hundred and fifty persons from the record-keeping obligation cannot be expressly remedied by the NIS Directive as there was no express record-keeping obligation under the NIS Directive. This does not mean that the NIS Directive can replace the GDPR as the scope and purpose of each legislation is fundamentally different.

---

\(^{372}\) General Data Protection Regulation, art 84.

\(^{373}\) General Data Protection Regulation, art 84.
CHAPTER 5

5.1 CONCLUSION

With continuous revolution of the information society, the e-commerce economy would continue to penetrate into our everyday lives, and the continuous functioning is dependent on the continuous trust of consumers and safety of personal data. While, criminal legislations does have its place in ensuring the proper functioning of the society, its effectiveness towards the protection of the e-commerce economy is severely limited. Hackers, as individuals are also knowledgeable of legal frameworks in states and for those whose motive is to cause real damage, they sure exploit the gaps in enforcement procedures. Until there is the eradication of territorial jurisdiction, emphasis on securing the e-commerce economy through criminal legislations is sure not going to heed the desired result.

From the comparative study conducted in this paper, the NIS Directive and the GDPR does offer a great alternative to the protection of the e-commerce economy by strengthening the resilience of security systems. Since the both laws can be effectively enforced without the machinery of the criminal justice system, its enforcement would not be hampered by jurisdiction, anonymity and evidence-gathering. With both legislations as administrative legislations which are internally organised, sanctions for defaulting service providers can be easily effected. The NIS Directive and the GDPR should therefore be the focus of the data security within the e-commerce economy by the Union.

Unfortunately, exclusion of small and micro-enterprises from the scope of the NIS Directive is a fundamental gap that need be addressed as most quite a number of e-commerce service provider does fall into that category. In a period where computing power is getting cheaper, with reduced cost of starting an e-commerce platform, many more service providers would fall into that classification than reasonably expected. Invariably, the expected level of protection being envisaged by the Union may not be achieved as a network is as strong as its weakest link. Thankfully, the GDPR does not create for the exemptions as the NIS Directive, hence all service providers whether classified as small or micro-enterprise would have to comply with the data security requirement under the GDPR. Further, the lack of a specified liability regime and omnibus sanction clause under the NIS Directive has capacity to create differences between member states and in the face of low penalties, service providers may become less willing to comply with directive. Again, the GDPR comes to the rescue and provides a strict liability regime as well as hefty sanctions for non-compliance with the security requirement.

While the GDPR covers for loopholes which could lead to less compliance under the NIS Directive, the layered data breach notification is a weakness as service providers are provided with alternatives for escape, especially from declarations to consumers. The NIS Directive data breach notification should have been the minimum requirement and not the layered pattern under the GDPR.

With regards to extra-territorial jurisdiction for service providers established outside the jurisdiction, it is laudable that the NIS Directive and GDPR does establish the appointment of a representative. However, there has to be an established legal relationship between the representative and service provider. Establishing a legal relationship between both parties would ensure that sanctions can be meted out. This is important, because the NIS Directive nor the GDPR made representative liable for the acts or omission of the service provider and unless
there is a sort of legal relationship between both parties, it may be difficult to sanction a service provider who has breached the data security requirement.

From the discussions in this paper, it would be beneficial if the competent authority under the NIS Directive and the GDPR are fused for ease of administration, and in order to ensure proper monitoring. Also competent authorities must be strict in the application of the NIS Directive and especially the GDPR in order to establish trust within the economy and give guarantees for the safety of personal data. However, it is critical to say that the administration of NIS Directive and the GDPR should not stop the continuous effort of investigators and prosecutors, but that members states through their competent authorities under the NIS Directive and the GDPR should be proactive in ensuring that data security is high rather than reliance on the reactive work of the investigators and prosecutors. The NIS Directive and the GDPR if properly enforced serves as better legal framework for the data security against illegal data access in the e-commerce economy.
BIBLIOGRAPHY

Official Documents and Opinions:

- Charter of Fundamental Rights of the European Union (2000/C 364/01)
- CoE ‘European Convention on Human Rights’ (1950) CETS No. 005, 1950
- Computer Misuse Act 1990
- Dutch Criminal Code II (Wetboek van Strafvordering) art 4a


German Criminal Code (Strafgesetzbuches durch) s7


NIS Directive 2016/1148/EU 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 [2016]


UK: Serious Crime Act, s 43
Books, Articles and Websites:


  <http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf> accessed 13 January 2017


  <http://semanticscholar.org/f953/2157d7c9cce42d44f6b4eb42479d6bf6a.pdf> accessed 6 January 2017


Charbon F and Kaspersen H, Computer/Law Institute, Free University, Amsterdam, accessed 5 January 2017

Clough J, ‘Principles of Cybercrime’ (Cambridge University Press 2012) 114


• Jones A and Doobay A, Extradition and Mutual Assistance (4th edn, Sweet & Maxwell, 2014)


• Podgor E, ‘Cybercrime: Discretionary Jurisdiction’ (2009) 47 University of Louisville Law Review 727


• Riekkinen J, ‘Evidence of Cybercrime and Coercive Measures in Finland’ (2016) 13 Digital Evidence and Electronic Signature Law Review 49


• Salane DE and Misshula E, Legislative and Regulatory Attempts to Address Cybercrime: The Good, the Bad and the Ugly (John Jay College of Criminal Justice Center for Cybercrime Studies Mathematics and Computer Science Department 2012)


• Schneiderman E and Kornreich R, ‘Personal Jurisdiction and Internet Commerce’ (1997) N.Y.L.J


• Soukieh K, ‘Cybercrime Shifting Doctrine of Jurisdiction’ (2011) 10 Canberra Law Review 221


• Sukhai N, ‘Hacking And Cybercrime’ <http://delivery.acm.org/10.1145/1060000/1059553/p128-sukhai.pdf?ip=137.56.80.216&id=1059553&acc=ACTIVE%20SERVICE&key=0C390721DC3021FF%2E8E8A7FC83EB1C6A0%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=878681869&CFTOKEN=55588862&__acm__=1482500490_8a757b4f3a22a4ba2be952533c01901e> accessed 13 January 2017


• ———, ‘Manual on Mutual Legal Assistance and Extradition’ (2012) 9

